16°EnGiTEC

Governança x Shadow IT/AI

Wagner Miranda Costa

TRIBUNAL DE CONTAS DA UNIÃO

80%

das organizações com plataformas low-code/no-code não possuem uma política de governança formal (2024).

Fonte: Forrester Research.

4x mais

A proporção de **Citizen Developers** para **desenvolvedores profissionais** até 2026.

Fonte: Gartner.

O Acelerador Inevitável: Adoção de GenAI

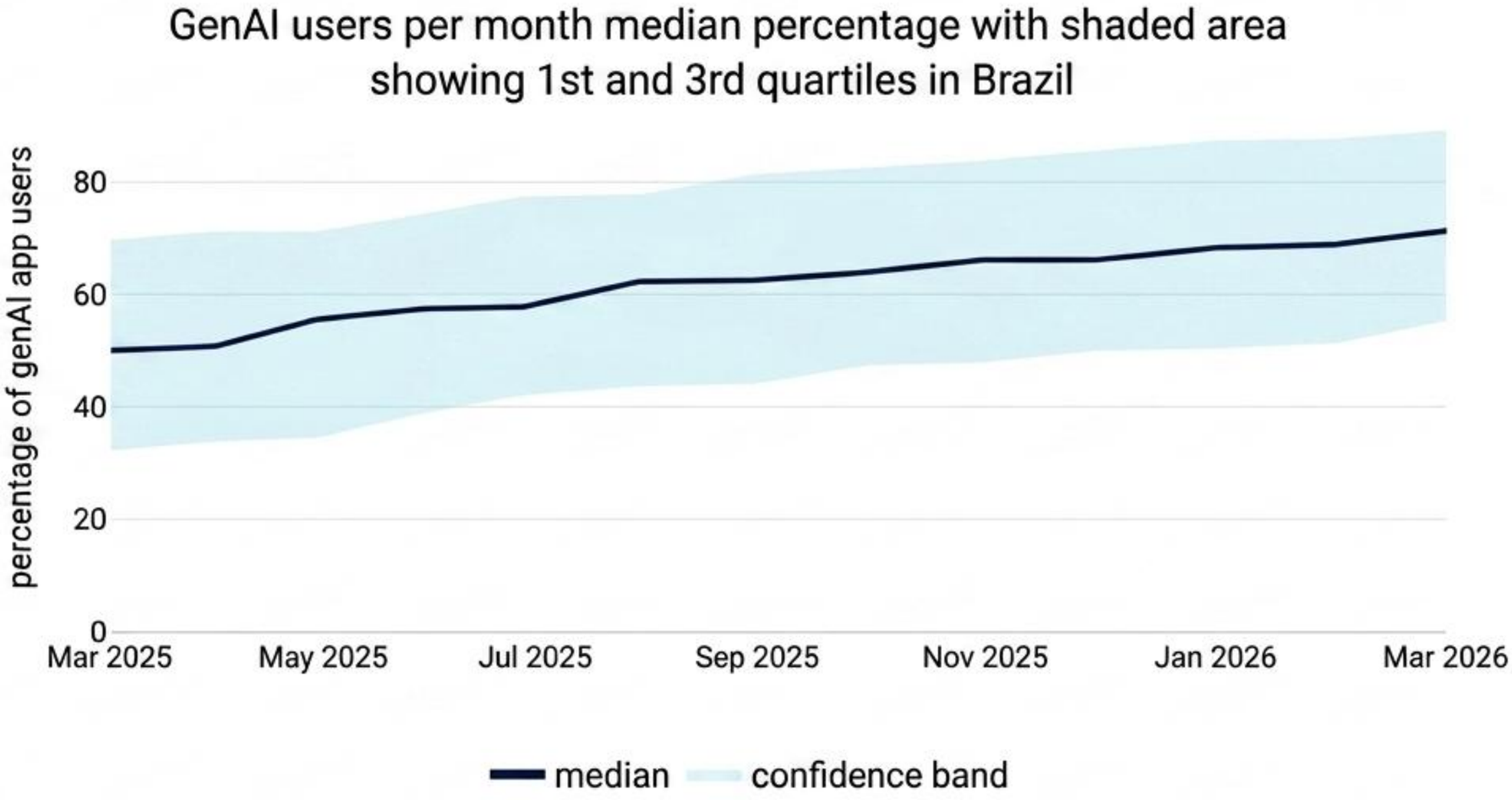
netskope

Threat Labs Report:

Brazil 2026

Risco Exponencial

Sem letramento (**AI Literacy**) e canais oficiais estabelecidos, o uso de IA com dados da Organização cresce rapidamente à sombra da governança institucional.



IA no Desenvolvimento

Até 2028, a IA Generativa permitirá que **40%** dos membros de equipes de software venham de formações **formações não técnicas tradicionais** (contra 20% em 2025).

Até 2027, o desenvolvimento auxiliado por IA trará **produtividade**, mas apenas **8%** de **melhoria média** nos resultados de negócio.

Fonte: Gartner.

15 a 20 vezes

As empresas subestimam o uso de SaaS em 15 a 20 vezes. Onde a TI vê 50 aplicações, o real costuma superar 700.

Fonte: Cisco.

30% a 50%

dos gastos de TI ocorrem fora do orçamento oficial (Shadow IT).

Fonte: Gartner e Everest Group.

Quando a ferramenta vira o limite

65.536

Limite de linhas em uma planilha .xls antiga.

15.841

Casos de Covid-19 perdidos no rastreamento.

No Reino Unido, o uso de planilhas locais para gestão de dados críticos de saúde pública colapsou o sistema. A ferramenta inadequada não suportou o volume de dados, silenciando infecções reais durante a pandemia.

Fonte: BBC. | **Caso:** Pandemia Reino Unido.

A porta aberta para o mundo

38 Milhões

Registros confidenciais expostos publicamente.

O uso do Microsoft Power Apps por usuários de negócio (Citizen Developers) focados em agilidade resultou na **inadequada configuração de permissões padrão** (APIs OData). Sem governança, dados corporativos ficaram abertos para a internet.

Fonte: ZDNet e Dark Reading. | Caso: Microsoft Power Apps.

Ataques de Injeção via Shadow AI

Ação do Usuário

Conector de Terceiros (ex: Zapier)

GenAI

O Atacante

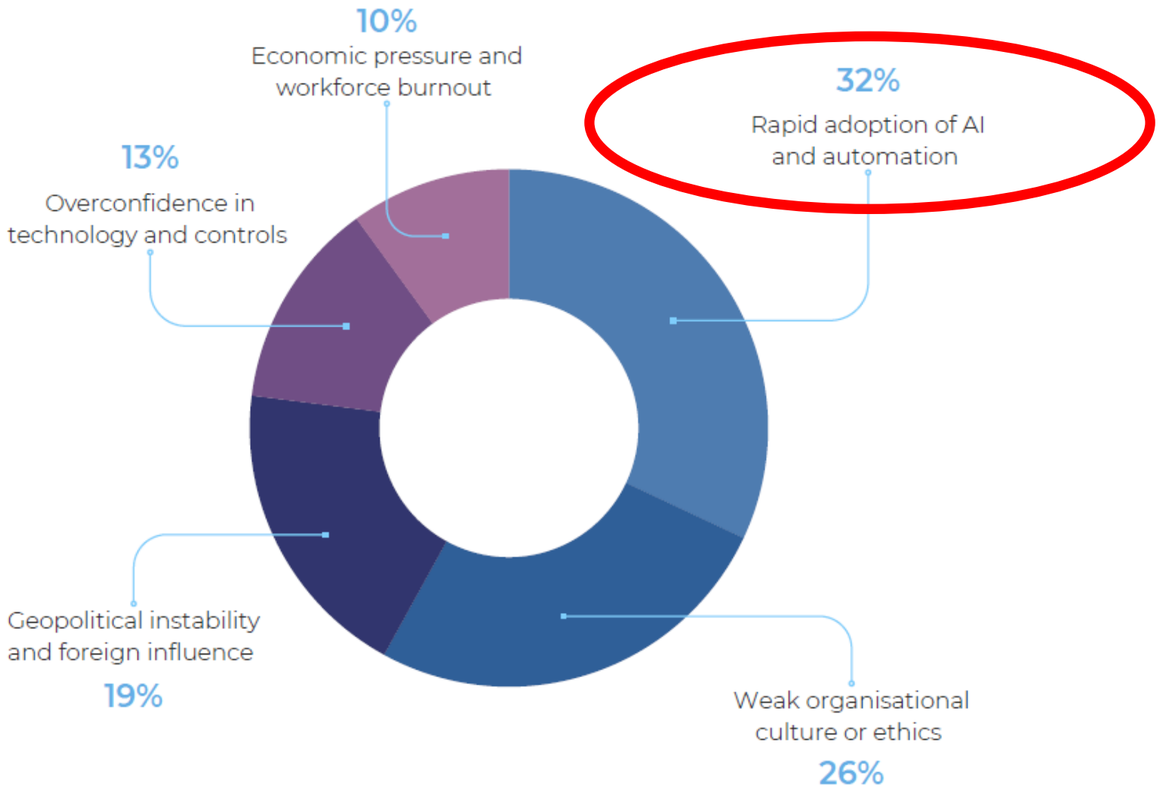
Ação do Usuário: Criação de “chatbots” caseiros integrando Zapier + GenAI para produtividade sem revisão de arquitetura.

A Vulnerabilidade: Prompt Injection. A IA recebe comandos maliciosos disfarçados em texto comum.

O Dano: Conectores de terceiros atuam como pontes cegas, permitindo o desvio e exfiltração de dados corporativos sem acionar alarmes convencionais.

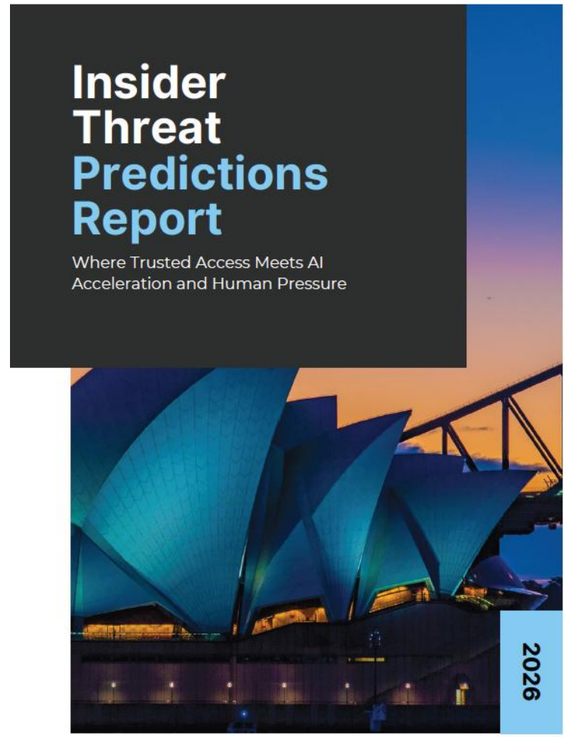
Ameaça: Uso não gerenciado de IA + Automação.

What's driving insider threats heading into 2026



Taken together, these drivers point to a combined reality: AI is accelerating behaviour and decision-making faster than governance and shared norms can keep pace, while cultural and geopolitical pressures continue to shape intent, opportunity, and harm.

Australian Institute of Insider Threats



The 2026 Insider Threat Predictions Report

Ranking #	Insider Threat Type	Why It Matters In 2026
1	Accidental Data Exposure via AI Tools	Routine AI use can expose sensitive information instantly and irreversibly beyond organisational control.
2	Supply-Chain Insider Compromise	Third-party access expands the insider perimeter while reducing visibility and accountability.
3	Spy Recruitment	State-aligned actors exploit trusted access for long-term strategic damage and intellectual property loss.
4	Ransomware-Recruited Insiders	Criminal groups incentivise insiders to enable rapid, high-impact ransomware activity from within.
5	Psychological Fatigue & Negligence	Sustained pressure and disengagement increase errors that can cascade into major incidents.
6	Shadow AI Deployments	Unapproved AI use moves data outside governance boundaries without leadership visibility.
7	AI-Powered Phishing & Deepfakes	Convincing impersonation exploits trust to trigger fraud, access

Australian Institute of Insider Threats

Insider Threat Predictions Report

Where Trusted Access Meets AI Acceleration and Human Pressure

2026

The 2026 Insider Threat Predictions Report

52%

dos funcionários admitem usar ferramentas de IA generativa no trabalho sem o conhecimento da organização.

Fonte: Salesforce.

Shadow IT

Qualquer hardware, software ou serviço de TI utilizado sem aprovação ou registro formal, fora da visibilidade da governança corporativa.

Shadow AI

Uso, desenvolvimento ou treinamento de sistemas de IA com dados institucionais sem a devida avaliação de risco, conformidade e registro.

Os Riscos do Provimento Descentralizado sem Governança

Segurança

Exposição de Dados Pessoais. Risco de vazamentos, não conformidade com a LGPD e violação de sigilo institucional.

Estratégia

Desalinhamento. Iniciativas (“Seleção Adversa”) que não geram valor público ou ignoram o Planejamento Estratégico.

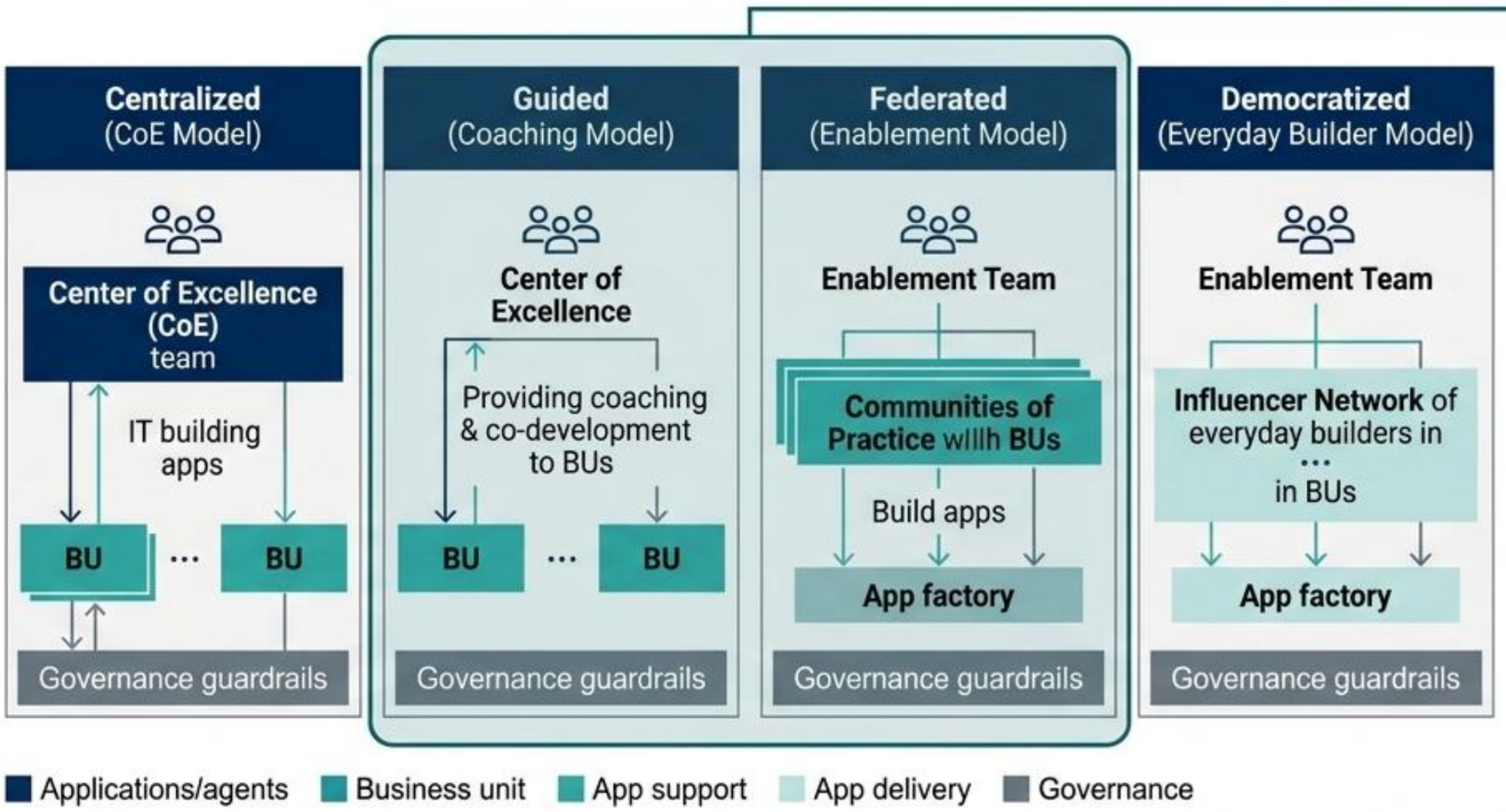
Custos

Desperdício e Redundância. Multiplicação de licenças SaaS ocultas e silos tecnológicos sem interoperabilidade.

Operação

Fragilidade (“Risco Moral”). Soluções sem continuidade, sem documentação e dependentes de um único servidor.

Modelos de Sucesso para Citizen Development



Os modelos Guiado e Federado representam o alvo estratégico da estrutura de governança do TCU, garantindo o equilíbrio ~~perfeito~~ entre Guardrails corporativos e Comunidades de Prática.

Fonte: Gartner (Adaptado).

Estruturas Organizacionais de TI: O Equilíbrio

Modelo de TI	Ideal Para	Ponto Forte	Fraqueza Principal
Centralizada	Negócios regulados e focados em custo	Forte governança e controle	Resposta excessivamente lenta ao negócio (O passado)
Descentralizada	Empresas ágeis guiadas pelo mercado	Resposta rápida	Alta redundância e riscos severos de segurança **(O perigo atual / Shadow IT)**
Federada	**Organizações complexas e globais**	**Combina controle central (Setid/Assip) com flexibilidade na ponta (O alvo do TCU)**	**Desafios de coordenação**

A estrutura Federada reflete exatamente a premissa de 'Autonomia com Responsabilidade' do novo modelo.

O Modelo do TCU: Motivações e Propósito

O Problema: Repressão gera “TI Sombra”

Bloquear o conhecimento especializado das unidades de negócio resulta inevitavelmente em inovações ocultas, fragmentadas e altamente arriscadas.

O Propósito: Habilitar com Responsabilidade

Transformar o Shadow IT em ativo estratégico gerenciado. Garantir autonomia mitigando ativamente o Risco Moral e a Seleção Adversa.

O objetivo não é controlar a inovação, mas prover canais oficiais (Catálogos e Sandboxes) para que o Citizen Developer atue com segurança estruturada.

O Propósito da Política: Transformar o Risco

Modelo de Governança TCU: Habilitar, Não Bloquear

Trazer o “Shadow IT” para a luz. Substituir o risco oculto por um regime de Autonomia com Responsabilidade e Resultado Institucional.

Fonte: TCU (elaboração própria).

Princípios Orientadores do Modelo

Alinhamento Estratégico

Vinculação obrigatória à geração de valor público.

Responsabilidade

A unidade proponente é dona do ciclo de vida da solução.

Proporcionalidade

O rigor dos controles varia conforme o risco da solução.

Conformidade by Design

Segurança e LGPD desde a concepção inicial.

Interoperabilidade

Uso de APIs oficiais e não redundância de sistemas.

Transparência em IA

Revisão humana e explicabilidade dos resultados probabilísticos.

O Ecossistema de Governança: Papéis e Responsabilidades

Atores da Inovação

Unidades de Negócio & Gestoras. Identificam oportunidades, desenvolvem e garantem o suporte Nível 1.

A Habilitadora

Setid. Mantém o catálogo oficial, provê plataformas (Sandbox), suporte Nível 2 e avalia arquitetura.

A Guardiã

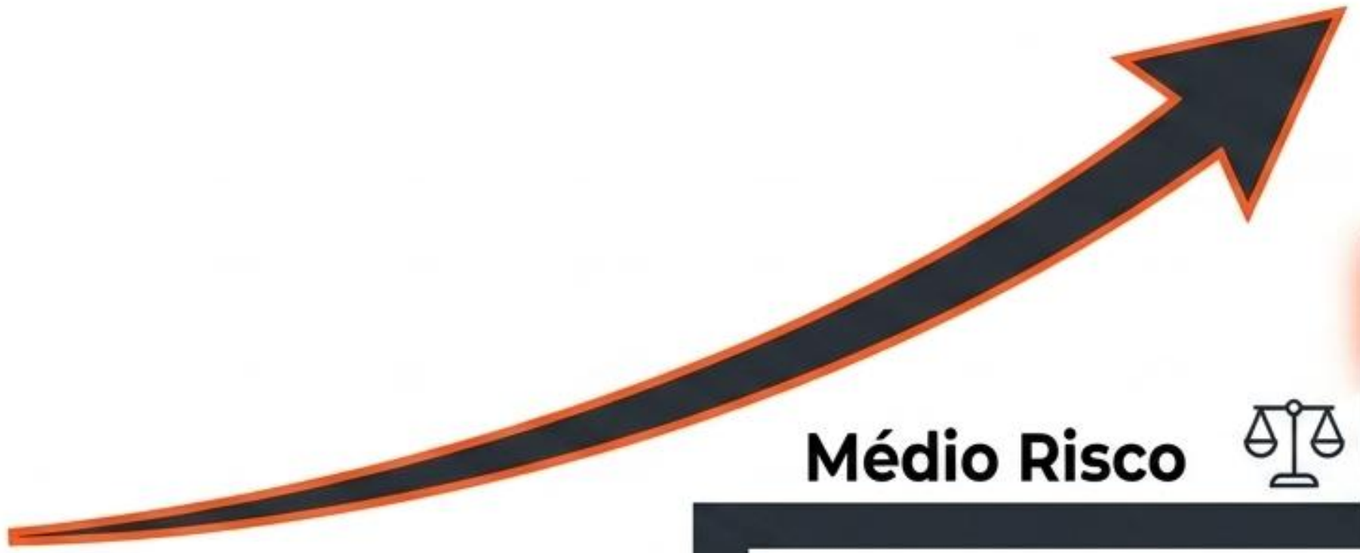
Assip. Avalia riscos, atua como DPO e garante o “Security & Privacy by Design”.

A Instância Máxima

CGTI. Delibera sobre projetos de alto risco, dirime conflitos e monitora o portfólio estratégico.

Fonte: TCU (elaboração própria).

Governança Proporcional ao Risco



Baixo Risco

Automações Pessoais. Dados públicos.
Rito: Registro simples, validação no catálogo, aprovação interna.

Médio Risco

Aplicativos de Negócio. Dados restritos/pessoais não sensíveis ou decisões com supervisão.
Rito: Análise técnica Setid + avaliação Assip.

Alto Risco

IA Autônoma / Ambientes Corporativos. Dados sigilosos, alcance externo ou IA sem supervisão.
Rito: Análise completa + deliberação formal do CGTI.

A Mudança de Paradigma na Governança

Dimensão	TI Centralizada Tradicional	Governança Habilitadora
Papel da TI Central	Gargalo executor e controlador rígido	Curadora, habilitadora e fornecedora de infraestrutura
Papel do Negócio	Solicitante passivo (ou criador de Shadow IT)	Protagonista com responsabilidade total pelo ciclo de vida
Postura perante a Inovação	Tudo que não é aprovado é proibido	Canais de “anistia”, experimentação segura (Sandbox) e catálogo oficial
Gestão de Risco	Baseada em bloqueios de rede e permissões	Baseada em autodeclaração, transparência e observabilidade

Checklist de Governança e Sustentabilidade:

- **Inventário:** Catálogo centralizado das soluções criadas pelas áreas.
- **Segurança:** Revisão de permissões e presença de autoridade de proteção de dados (DPO) formal.
- **Continuidade:** Plano de contingência e responsável pelo ciclo de vida designado.
- **Qualidade:** Testes formais e requisitos de engenharia em processos críticos.
- **Evolução:** Soluções descentralizadas e corporativas seguem jornadas distintas (sem promoção automática no TCU).

Arquitetura de governança de provimento descentralizado no TCU

PILARES DE ESPECIALIZAÇÃO

- **IA Generativa & Agentes**
- **Painéis BI**
- **Plataforma de Dados**
- **Sistemas de Informação**

Extensão do modelo fundamental:
normas específicas que adaptam a governança às particularidades de cada tecnologia

MODELO DE GOVERNANÇA

Premissas e Diretrizes

- Alinhamento Estratégico
- Responsabilidade Integral
- Segurança by Design
- Governança Proporcional ao Risco

Papéis e Responsabilidades

- **Setid** (Habilitadora)
- **UN** (Autora)
- **Assip** (Segurança)

Ciclo de Vida

Do registro e operação até a desativação.

Plataforma Corporativa

Uso de tecnologias e catálogo pré-aprovados.

Matriz de Risco

Avaliação de sensibilidade, criticidade e alcance.

Obrigado!

Wagner Miranda Costa
Tribunal de Contas da União - TCU
Setid - Secretaria de Tecnologia da Informação e Evolução Digital
Secretário Adjunto
e-mail: wagnermc@tcu.gov.br