AFRIKA

TECNOLOGIA E NEGÓCIO

EXECUTIVE GUIDE AI SECURITY

O Novo Perímetro da Segurança.

COMO PROTEGER APLICAÇÕES E AGENTES DE IA NA ERA DA INTELIGÊNCIA ARTIFICIAL.

afrikatec.com.br

@afrikatec

Contexto

A Inteligência Artificial já faz parte da operação das empresas. Modelos de linguagem, agentes inteligentes e automações estão acelerando processos, apoiando decisões e transformando a forma como organizações trabalham.

Essa evolução traz enormes oportunidades, mas também cria uma nova superfície de risco. Surge uma disciplina que tende a ocupar um papel semelhante ao desempenhado por Cloud Security e Gestão de Identidades: AI Security.

Este Executive Guide reúne conceitos, tendências, riscos e recomendações práticas para apoiar líderes de tecnologia na construção de uma estratégia segura para adoção da IA.

Afrika Insights

AI Security

Cada grande evolução tecnológica exigiu uma nova disciplina de segurança. A IA é o próximo capítulo dessa história.

índice

A IA criou um novo perímetro de segurança.

Redes exigiram Firewalls. Aplicações impulsionaram Application Security. A nuvem trouxe Cloud Security. A identidade consolidou IAM, PAM e Zero Trust.

Agora aplicações de IA acessam dados, utilizam ferramentas, executam tarefas e tomam decisões. Proteger apenas infraestrutura e usuários já não é suficiente.

Novo perímetro, novas responsabilidades
A segurança precisa evoluir na mesma velocidade da tecnologia

Como mudou a superfície de ataque.

Aplicações baseadas em IA possuem novos componentes críticos: modelos, agentes, memória, RAG, APIs, ferramentas e integrações. Cada elemento amplia a superfície de exposição.

Visibilidade, controles e governança são essenciais em cada etapa da jornada da IA

A IA já transformou o negócio.

A governança ainda tenta acompanhar.

Os indicadores mostram que a adoção da Inteligência Artificial avança em ritmo acelerado, enquanto políticas, controles e mecanismos de governança evoluem de forma mais gradual. Esse descompasso amplia a exposição das organizações e reforça a necessidade de uma estratégia estruturada de AI Security.

A EVOLUÇÃO DO PERÍMETRO DE SEGURANÇA

INDICADORES QUE MOSTRAM A NOVA REALIDADE DA INTELIGÊNCIA ARTIFICIAL NAS ORGANIZAÇÕES.

56%

Aumento dos incidentes relacionados à Inteligência Artificial no último ano.

US$ 4,44MI

Custo médio global de um incidente de segurança de dados.

97%

Das organizações afetadas não possuíam controles de específicos de acesso para sistema de IA

61%

Das empresas não possuem políticas formais de governança para o uso de Inteligência Artificial

A IA já é realidade nas empresas, e os riscos evoluem na mesma velocidade.
Sem governança, visibilidade e controles adequados, os impactos financeiros operacionais e reputacionais tendem a aumentar

Os cinco riscos que atualmente merecem maior atenção.

A evolução da IA também amplia sua superfície de risco. Entre as diferentes ameaças já identificadas, cinco pontos merecem atenção especial das organizações que utilizam aplicações e agentes de Inteligência Artificial.

PROMPT INJECTION

Manipulação do comportamento do modelo por linguagem natural.

VAZAMENTO DE DADOS

Exposição de informações sensíveis.

PERMISSÕES EXCESSIVAS

Agentes com autonomia além do necessário.

CADEIA DE SUPRIMENTOS

Modelos, plugins e integrações vulneráveis.

MEMÓRIA E CONTEXTO

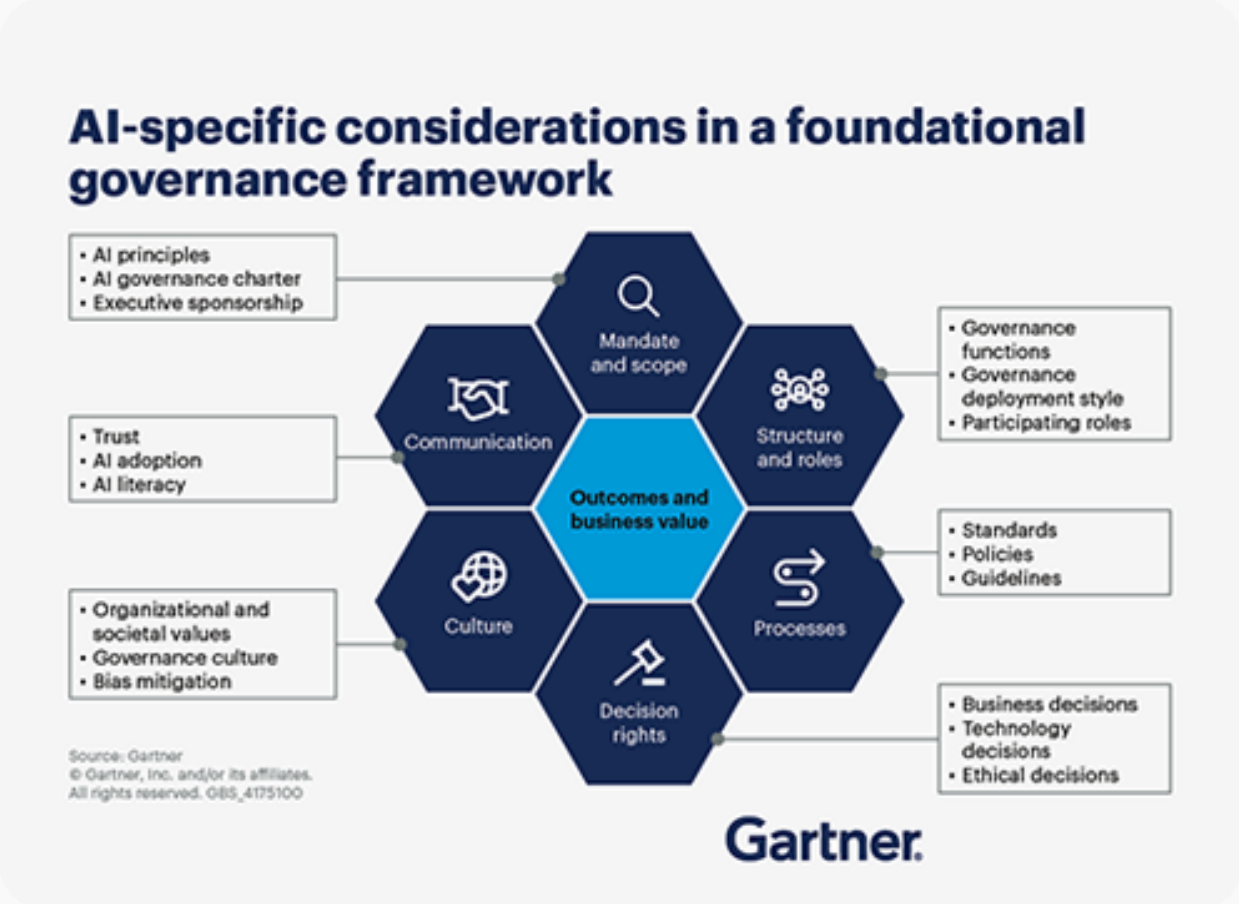
Informações incorretas influenciando decisões futuras.

Governança é a base para escalar a IA com segurança

À medida que a Inteligência Artificial passa a integrar processos, decisões e operações críticas, sua governança não pode depender apenas de controles tecnológicos isolados.

Uma abordagem estruturada exige clareza sobre **responsabilidades, processos, critérios de decisão, cultura e comunicação,** sempre conectando a adoção da IA aos objetivos e resultados do negócio.

O modelo de governança apresentado pelo Gartner reforça essa visão ao posicionar **resultados e valor para o negócio no centro da estratégia**, sustentados por seis dimensões fundamentais.



O futuro da AI Security

A maturidade em AI Security não será definida apenas pelas tecnologias adotadas, mas pela capacidade das organizações de estabelecer governança, acompanhar riscos e evoluir seus controles à medida que a Inteligência Artificial também evolui.

Mais do que uma iniciativa pontual, AI Security deve ser entendida como uma jornada contínua. Um processo de aprendizado, adaptação e melhoria que permita às empresas ampliar o uso da IA com mais segurança, visibilidade e confiança.

Porque a tecnologia continuará mudando. E a forma de protegê-la também precisará evoluir.

AI Security Quick Check.

Quanto sua organização está preparada para adotar IA com segurança?

Marque os itens que já fazem parte da realidade da sua organização.

Não é necessário atender a todos os critérios. O objetivo é identificar oportunidades para fortalecer sua estratégia de AI Security.

	PERGUNTA	O QUE SIGNIFICA?
☐	**Existe uma política corporativa para IA?**	A organização possui diretrizes claras para o uso da IA, compartilhamento de dados e responsabilidades das equipes.
☐	**Há inventário das aplicações com IA?**	A empresa sabe quais aplicações, agentes, copilots ou modelos de IA estão em uso, sejam eles desenvolvidos internamente ou contratados de terceiros.
☐	**Os agentes possuem identidade própria?**	Cada agente ou aplicação de IA possui credenciais individuais, permitindo identificar quem executou cada ação e evitando acessos compartilhados.
☐	**Existe menor privilégio?**	Agentes e aplicações acessam apenas os sistemas e informações estritamente necessários para executar suas funções, reduzindo o impacto de falhas ou abusos.
☐	**Há proteção contra Prompt Injection?**	Existem mecanismos para detectar ou reduzir o risco de instruções maliciosas alterarem o comportamento da IA ou permitirem acessos indevidos.
☐	**Existe auditoria?**	Todas as interações, decisões e ações executadas por aplicações ou agentes de IA podem ser registradas, rastreadas e auditadas quando necessário.
☐	**Há monitoramento contínuo?**	A organização acompanha continuamente o comportamento das aplicações de IA, identificando desvios, riscos e incidentes em tempo hábil.
☐	**São realizados testes periódicos?**	Aplicações de IA passam por avaliações regulares de segurança, validação de controles e revisão de configurações antes e durante a operação.

Afrika Insights

AI Security

Empresas maduras em AI Security não se diferenciam apenas pelas tecnologias que utilizam, mas pela capacidade de governar continuamente o uso da Inteligência Artificial.

Glossário Executivo.

- **AI Security**

  Disciplina da cibersegurança voltada à proteção de aplicações, modelos e agentes de Inteligência Artificial durante todo o seu ciclo de vida, garantindo governança, segurança e conformidade.

- **Agentic AI**

  Sistemas de IA capazes de executar tarefas de forma autônoma, utilizando ferramentas, acessando sistemas e tomando decisões com base em objetivos previamente definidos.

- **LLM (Large Language Model)**

  Modelo de linguagem treinado com grandes volumes de dados para compreender, interpretar e gerar texto em linguagem natural. Exemplos incluem GPT, Claude, Gemini e Llama.

- **Prompt**

  Instrução ou pergunta enviada ao modelo de IA para solicitar uma resposta, executar uma tarefa ou iniciar uma interação.

- **Prompt Injection**

  Técnica que busca manipular o comportamento da IA por meio de instruções maliciosas inseridas em prompts, documentos, páginas web ou outras fontes de informação consumidas pelo modelo.

- **RAG (Retrieval-Augmented Generation)**

  Arquitetura que permite ao modelo consultar bases de conhecimento externas antes de gerar uma resposta, tornando as informações mais atualizadas e contextualizadas.

- **MCP (Model Context Protocol)**

  Protocolo que padroniza a comunicação entre modelos de IA, agentes, ferramentas e sistemas externos, facilitando integrações de forma estruturada.

AFRIKA

TECNOLOGIA E NEGÓCIO

Sobre a Afrika

A Afrika apoia organizações na construção de jornadas de AI Security por meio de assessment, estratégia, implementação de controles e evolução contínua.

O próximo passo começa com uma conversa.

A Inteligência Artificial está transformando a forma como as empresas desenvolvem software, automatizam processos e tomam decisões.

Construir uma estratégia de AI Security significa equilibrar inovação, governança e proteção, respeitando a realidade e o nível de maturidade de cada organização.

A Afrika apoia empresas nessa jornada, ajudando líderes de tecnologia a identificar riscos, estruturar controles e adotar práticas que permitam evoluir o uso da IA com mais segurança e confiança.

Vamos conversar sobre como preparar sua organização para essa nova realidade.

+55 11 99193-9451

comercial@afrikatec.com.br

afrikatec.com.br