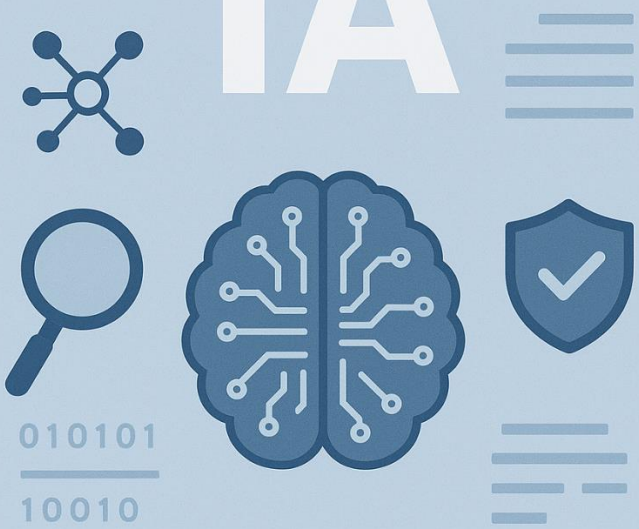
ESTRATÉGIA DE IA



SECRETARIA DE CONTROLE
E TRANSPARÊNCIA

GOVERNO DO ESTADO
DO ESPÍRITO SANTO

SECRETÁRIO
Edmar Moreira Camata

SUBSECRETÁRIO DE TRANSPARÊNCIA
Fabiano da Rocha Louzada

SUBSECRETÁRIO DE CONTROLE
Artur Antônio Moraes Marques

SUBSECRETÁRIO DE INTEGRIDADE
Alexandre Del Santo Falcão

CORREGEDOR GERAL DO ESTADO
Marcello Paiva de Mello

Equipe de Elaboração:

Emerson Couto de Moura

Fabricio Massariol

Leandro Cesana Machado

Luciano Lovate Fardin

Versão 1.1
Outubro de 2025

Documento elaborado com auxílio de Inteligência Artificial.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

SUMÁRIO

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

1. INTRODUÇÃO.

A Secretaria de Controle e Transparência (SECONT), em seu contínuo compromisso com a modernização e a eficiência dos serviços públicos, reconhece o potencial transformador da Inteligência Artificial (IA) como ferramenta estratégica para aprimorar suas atividades finalísticas e de apoio.

Este documento estabelece a **Estratégia de Inteligência Artificial da SECONT**, delineando as diretrizes, objetivos, pilares de atuação e planos de ação para a adoção e o desenvolvimento de soluções de Inteligência Artificial, buscando otimizar processos, qualificar análises e fortalecer a atuação do seu corpo técnico e administrativo.

2. VISÃO INSTITUCIONAL.

Ser uma instituição reconhecida pela qualidade no controle interno da Administração Pública.

A visão institucional da SECONT é um pilar fundamental para a boa gestão dos recursos públicos e a promoção da integridade no Poder Executivo Estadual. Em um cenário onde a complexidade dos dados governamentais cresce exponencialmente, a capacidade de examinar, entender e agir sobre essas informações de forma eficiente se torna um diferencial crucial.

É nesse contexto que a Inteligência Artificial (IA) emerge não apenas como uma ferramenta tecnológica, mas como um **imperativo estratégico para a SECONT**. A IA oferece o poder de transcender os métodos tradicionais de auditoria e controle, permitindo uma análise proativa, a identificação ágil de riscos e a otimização de processos.

Ao integrar a IA em suas operações, a SECONT poderá aprimorar sua capacidade de fiscalização, garantir a transparência e, em última instância, fortalecer a confiança da sociedade na administração pública, consolidando-se como referência em controle interno.

Para apoiar essa visão, a estratégia proposta fornece objetivos e diretrizes claras com abrangência sobre todas as áreas de atuação da SECONT.

3. OBJETIVOS.

A Estratégia de IA da SECONT visa alcançar os seguintes objetivos:

Objetivo	Ação
A. Aumento da eficiência nas auditorias e inspeções.	▪ **A1** – Utilizar algoritmos de IA para prever onde há maior probabilidade de ocorrência de irregularidades, permitindo o uso mais estratégico dos recursos do órgão. ▪ **A2** – Utilizar os recursos de IA no processamento de documentos, planilhas, contratos e registros financeiros para identificar inconsistências, fraudes ou padrões suspeitos.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Objetivo	Ação
B. Melhoria na transparência e no acesso à informação.	▪ **B1** – Criar assistentes virtuais inteligentes capazes de auxiliar cidadãos, servidores e gestores com dúvidas sobre processos, normas e procedimentos, fortalecendo a transparência ativa. ▪ **B2** – Criar assistentes virtuais inteligentes para auxiliar a navegação no Portal da Transparência, extraindo e consolidando informações através de uma interface em linguagem natural.
C. Apoio à tomada de decisão baseada em dados.	▪ **C1** – Criar localmente agentes de IA conversacionais capazes de apoiar as equipes da SECONT consultando bases de documentos, bancos de dados e sistemas corporativos. ▪ **C2** – Contratar serviços de IA para apoio em pesquisas, análises de documentos e criação de conteúdo relacionadas às diversas atividades das áreas fim e meio da SECONT.
D. Fortalecimento da cultura de integridade.	▪ **D1** – Utilizar a IA para identificar conflitos de interesse através do cruzamento de bases de dados heterogêneas (como diários oficiais, portais de transparência e dados de vínculos familiares). ▪ **D2** – Utilizar a IA para ampliar a análise de redes de relacionamento e ajudar a mapear conexões que possam indicar favorecimentos e conluios em licitações e investigações.
E. Monitoramento contínuo e proativo.	▪ **E1** – Utilizar a IA na detecção de anomalias em tempo real e criar as condições para monitoramento contínuo de sistemas com o objetivo de sinalizar desvios fora do padrão esperado. ▪ **E2** – Utilizar a IA na monitoria de riscos em tempo real e na geração de alertas e recomendações automatizadas capazes de orientar os gestores e demais responsáveis.
F. Melhorar a eficiência operacional.	▪ **F1** – Capacitar os servidores da SECONT no uso e conhecimento geral das soluções de IA com foco na compreensão básica do que é IA, como funciona e suas aplicações no setor público. ▪ **F2** – Capacitar os servidores da SECONT no uso das soluções e recursos da IA nas atividades específicas do órgão, tais como: auditoria, fiscalização, investigação e monitoramento.

4. DIRETRIZES GERAIS.

As diretrizes gerais que nortearão a implementação desta estratégia são:

a. **Foco na Eficiência e Qualidade**: A adoção da IA deve resultar em ganhos comprovados de eficiência operacional e na melhoria da qualidade dos serviços prestados.

b. **Segurança e Privacidade dos Dados**: Todas as iniciativas de IA deverão estar em conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais regulamentações pertinentes, garantindo a proteção e o uso ético das informações.

c. **Transparência e Explicabilidade**: Buscar soluções de IA que permitam a compreensão de seus processos e resultados, fomentando a confiança e a rastreabilidade.

d. **Colaboração e Interoperabilidade**: Promover a integração das soluções de IA com os sistemas existentes e estimular a colaboração entre as diferentes áreas da SECONT.

e. **Desenvolvimento Contínuo e Inovação**: Incentivar a experimentação, o aprendizado contínuo e a busca por novas tecnologias e abordagens em IA.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

f. **Capacitação e Desenvolvimento de Pessoas**: Investir na qualificação dos servidores para a utilização e o desenvolvimento de soluções de IA.

5. GOVERNANÇA.

A adoção de sistemas de Inteligência Artificial (IA) pela SECONT, embora promissora para otimizar processos e aprimorar sua atividade fim, introduz uma complexidade sem precedentes que demanda uma governança robusta e bem definida.

Sem diretrizes claras e mecanismos de supervisão, os riscos associados à IA – como vieses algorítmicos, questões de privacidade e segurança de dados, opacidade nas tomadas de decisão e a própria responsabilidade legal em caso de erros – podem comprometer a credibilidade e a eficiência das iniciativas.

A governança da IA na SECONT, portanto, não é um mero acessório, mas um pilar fundamental para garantir que a implementação da inteligência artificial ocorra de forma ética, transparente, responsável e alinhada aos objetivos estratégicos da Secretaria, maximizando seus benefícios e mitigando potenciais danos.

A presente estratégia estabelece a seguinte estrutura de governança:

a. Governança Estratégica e Ética.

Será exercida pelo **Comitê Gestor de Tecnologia, Segurança da Informação e Proteção de Dados Pessoais** (**CTSP**). Ele define o "porquê" e o "o quê" da IA na SECONT, garantindo que a tecnologia esteja alinhada aos valores e objetivos da Secretaria.

Responsabilidades:

- Definição e revisão dos princípios éticos e diretrizes gerais de IA.
- Estabelecimento da política de uso de IA na SECONT.
- Avaliação de impacto social e ético de novas aplicações de IA.
- Definição de limites e áreas de automação permitidas.
- Promoção da cultura de IA responsável em toda a Secretaria.
- Engajamento com partes interessadas (cidadãos, academia, outras instituições).
- Monitoramento das tendências regulatórias e tecnológicas em IA.

b. Governança de Dados e Privacidade.

Será exercida pela **Coordenação de Informações Estratégicas e Inteligência de Dados** (**CIED**). Ela deve garantir que a matéria-prima da IA (os dados) seja tratada com a máxima segurança, privacidade e qualidade.

Responsabilidades:

- Definição de políticas para coleta, armazenamento, processamento e descarte de dados para IA.
- Garantia de conformidade com a LGPD e outras regulamentações de privacidade.
- Estabelecimento de padrões de qualidade e integridade dos dados.
- Auditoria de bases de dados para identificação e mitigação de vieses.
- Gestão do consentimento e do acesso aos dados.
- Implementação de técnicas de anonimização e pseudonimização, quando pertinente.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

c. Governança de Desenvolvimento e Operações (DevOps de IA).

Será exercida pela **Gerência de Tecnologia da Informação e Comunicação** (**GTIC**). Ela será responsável pela implementação técnica, segurança e performance dos sistemas de IA, desde o desenvolvimento e/ou contratação até a operação contínua.

Responsabilidades:

- Estabelecimento de padrões para o desenvolvimento de modelos de IA (metodologias, ferramentas).
- Definição de requisitos de segurança cibernética para sistemas de IA.
- Criação de protocolos para testes, validação e implantação de modelos.
- Implementação de sistemas de monitoramento contínuo de desempenho e segurança dos modelos em produção.
- Definição de procedimentos para manutenção, atualização e retreinamento de modelos.
- Garantia de rastreabilidade e auditabilidade técnica dos sistemas de IA.
- Gestão de infraestrutura tecnológica para IA.

d. Governança de Riscos e Conformidade.

Será exercida pela **Coordenação de Consultoria em Governança, Gestão de Riscos e Controles Internos** (**CGRC**). Deve atuar com a função de fiscalização interna, identificando, avaliando e mitigando os riscos associados à IA, e garantindo que todas as atividades estejam em conformidade com as políticas e regulamentações.

Responsabilidades:

- Desenvolvimento de metodologias de avaliação de risco específicas para IA.
- Realização de auditorias regulares nos sistemas de IA.
- Gestão de incidentes relacionados à IA (falhas, vieses, violações de segurança).
- Verificação dos planos de contingência e recuperação.
- Garantia da conformidade legal e regulatória em todas as fases do ciclo de vida da IA.
- Criação de um canal para relato de denúncias (*whistleblowing*) relacionadas à IA.

6. CRONOGRAMA E ETAPAS DE IMPLEMENTAÇÃO.

A jornada de implementação da Inteligência Artificial na SECONT é um processo complexo, que exige planejamento detalhado, flexibilidade e um compromisso contínuo com a inovação responsável. Este capítulo detalha o cronograma proposto e as principais etapas que guiarão a SECONT na adoção estratégica e ética da IA.

É fundamental reconhecer, contudo, que projetos de alta complexidade e com o ineditismo que a IA representa no setor público podem enfrentar desafios imprevistos. Atrasos podem ocorrer devido à necessidade de validações adicionais, adaptações tecnológicas, evolução regulatória ou mesmo à maturação de novos conhecimentos.

Por isso, o cronograma aqui apresentado serve como um guia, uma referência que será monitorada e ajustada conforme o progresso e as contingências surgirem, sempre com o objetivo de garantir a segurança, a eficácia e a aderência aos princípios de governança estabelecidos.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Etapas previstas para conclusão em **2026**:

Ação	Objetivo	Etapas	Responsável
C1 – Criar localmente agentes de IA conversacionais capazes de apoiar as equipes da SECONT consultando bases de documentos, bancos de dados e sistemas corporativos via API.	Apoio à tomada de decisão baseada em dados.	• Definir escopo e áreas atendidas. • Definir infraestrutura e recursos necessários. • Construir os agentes. • Testar e homologar a solução. • Disponibilizar em produção.	GTIC e áreas técnicas
C2 – Contratar serviços de IA para apoio em pesquisas, análises de documentos e criação de conteúdo relacionadas às diversas atividades das áreas fim e meio da SECONT.	Apoio à tomada de decisão baseada em dados.	• Definir escopo, usuários e áreas atendidas. • Realizar análise comparativa entre as possíveis soluções. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	GTIC e áreas técnicas
F1 – Capacitar os servidores da SECONT no uso e conhecimento geral das soluções de IA com foco na compreensão básica do que é IA, como funciona e suas aplicações no setor público.	Melhorar a eficiência operacional.	• Definir o público alvo. • Definir a ementa. • Analisar as opções de contratação. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar o treinamento.	GTIC e áreas técnicas
F2 – Capacitar os servidores da SECONT no uso das soluções e recursos da IA nas atividades específicas do órgão, tais como: auditoria, fiscalização, investigação e monitoramento.	Melhorar a eficiência operacional.	• Definir o público alvo. • Definir a ementa. • Analisar as opções de contratação. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar o treinamento.	GTIC e áreas técnicas

Etapas previstas para conclusão em **2027**:

Ação	Objetivo	Etapas	Responsável
A1 – Utilizar algoritmos de IA para prever onde há maior probabilidade de ocorrência de irregularidades, permitindo o uso mais estratégico dos recursos do órgão.	Aumento da eficiência nas auditorias e inspeções.	• Definir escopo. • Definir disponibilidade e qualidade dos dados. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Ação	Objetivo	Etapas	Responsável
A2 – Utilizar os recursos de IA no processamento de documentos, planilhas, contratos e registros financeiros para identificar inconsistências, fraudes ou padrões suspeitos.	Aumento da eficiência nas auditorias e inspeções.	• Definir escopo. • Definir disponibilidade e qualidade dos dados. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED e GTIC
B1 – Criar assistentes virtuais inteligentes capazes de auxiliar cidadãos, servidores e gestores com dúvidas sobre processos, normas e procedimentos, fortalecendo a transparência ativa.	Melhoria na transparência e no acesso à informação.	• Definir escopo e áreas atendidas. • Definir disponibilidade e qualidade dos dados. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED, GETIC e SUBTRAN
B2 – Criar assistentes virtuais inteligentes para auxiliar a navegação no Portal da Transparência, extraindo e consolidando informações através de uma interface em linguagem natural.	Melhoria na transparência e no acesso à informação.	• Definir escopo e áreas atendidas. • Definir disponibilidade e qualidade dos dados. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED, GETIC e CTRA
D1 – Utilizar a IA para identificar conflitos de interesse através do cruzamento de bases de dados heterogêneas (como diários oficiais, portais de transparência e dados de vínculos familiares).	Fortalecimento da cultura de integridade.	• Considerar os projetos de Ciência de Dados existentes. • Definir escopo. • Definir disponibilidade e qualidade dos dados. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED e SUBINT
D2 – Utilizar a IA para ampliar a análise de redes de relacionamento e ajudar a mapear conexões que possam indicar favorecimentos e conluios em licitações e investigações.	Fortalecimento da cultura de integridade.	• Considerar os projetos de Ciência de Dados existentes. • Definir escopo. • Definir disponibilidade e qualidade dos dados. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED e SUBINT

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Etapas previstas para conclusão em **2028**:

Ação	Objetivo	Etapas	Responsável
E1 – Utilizar a IA na detecção de anomalias em tempo real e criar as condições para monitoramento contínuo de sistemas com o objetivo de sinalizar desvios fora do padrão esperado.	Monitoramento contínuo e proativo.	• Definir capacidade de integração com sistemas corporativos. • Definir escopo de detecção e monitoria. • Definir disponibilidade e qualidade de dados complementares. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED e SUBCONT
E2 – Utilizar a IA na monitoria de riscos em tempo real e na geração de alertas e recomendações automatizadas capazes de orientar os gestores e demais responsáveis.	Monitoramento contínuo e proativo.	• Definir capacidade de integração com sistemas corporativos. • Definir escopo de detecção e monitoria. • Definir disponibilidade e qualidade de dados complementares. • Definir arquitetura, recursos e integrações. • Elaborar o projeto de contratação (ETP/TR). • Fazer a contratação. • Disponibilizar serviços.	CIED e SUBCONT

7. MÉTRICAS DE AVALIAÇÃO.

Para medir o sucesso da Estratégia de IA na SECONT e garantir que os objetivos propostos sejam efetivamente alcançados, é crucial estabelecer métricas de avaliação claras e mensuráveis para cada um. Essas métricas permitirão à SECONT acompanhar o progresso, identificar áreas de melhoria e demonstrar o valor agregado pela inteligência artificial.

Objetivo	Ações	Métricas
A – Aumento da Eficiência nas Auditorias e Inspeções.	A1 – Utilizar algoritmos de IA para prever onde há maior probabilidade de ocorrência de irregularidades, permitindo o uso mais estratégico dos recursos do órgão.	• **Taxa de Acerto na Detecção de Irregularidades**: Percentual de irregularidades reais que foram corretamente identificadas pelos algoritmos de IA em relação ao total de irregularidades encontradas nas auditorias. • **Otimização de Recursos**: Percentual de redução nos custos operacionais (humanos e materiais) por auditoria ou inspeção, devido à alocação mais estratégica. • **Número de Irregularidades Identificadas**: Aumento no volume de irregularidades detectadas anualmente, especialmente aquelas que poderiam passar despercebidas sem a IA.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Objetivo	Ações	Métricas
	A2 – Utilizar os recursos de IA no processamento de documentos, planilhas, contratos e registros financeiros para identificar inconsistências, fraudes ou padrões suspeitos.	• **Volume de Documentos Processados pela IA**: Número de documentos, planilhas e contratos analisados pela IA em um período específico. • **Taxa de Falsos Positivos/Negativos**: Percentual de alertas de IA que não correspondem a uma irregularidade real (falso positivo) e de irregularidades reais não detectadas (falso negativo). O objetivo é reduzir ambos. • **Tempo para Identificação de Inconsistências**: Redução do tempo necessário para que a IA sinalize potenciais inconsistências ou fraudes em grandes volumes de dados, comparado à análise manual.
B – Melhoria na Transparência e no Acesso à Informação.	B1 – Criar assistentes virtuais inteligentes capazes de auxiliar cidadãos, servidores e gestores com dúvidas sobre processos, normas e procedimentos, fortalecendo a transparência ativa.	• **Taxa de Resolução de Perguntas**: Percentual de perguntas dos usuários respondidas com sucesso pelo assistente virtual sem intervenção humana. • **Volume de Atendimentos Automatizados**: Número de interações mensais/anuais com o assistente virtual. • **Satisfação do Usuário**: Pontuação média obtida em pesquisas de satisfação realizadas com os usuários dos assistentes virtuais (cidadãos, servidores, gestores).
	B2 – Criar assistentes virtuais inteligentes para auxiliar a navegação no Portal da Transparência, extraindo e consolidando informações através de uma interface em linguagem natural.	• **Número de Consultas ao Assistente do Portal da Transparência**: Volume de vezes que o assistente é utilizado para navegar e extrair informações. • **Complexidade das Consultas Atendidas**: Avaliação da capacidade do assistente em responder a perguntas mais complexas e multifacetadas. • **Tempo de Acesso à Informação**: Redução do tempo médio que um cidadão leva para encontrar uma informação específica no Portal da Transparência usando o assistente, comparado à navegação tradicional. • **Feedback Qualitativo de Cidadãos**: Análise de comentários e sugestões sobre a facilidade e eficácia do assistente.
C – Apoio à Tomada de Decisão Baseada em Dados.	C1 – Criar localmente agentes de IA conversacionais capazes de apoiar as equipes da SECONT consultando bases de documentos, bancos de dados e sistemas corporativos via API.	• **Número de Consultas Realizadas pelos Agentes de IA**: Volume de interações dos servidores com os agentes para obter informações. • **Acurácia das Respostas**: Avaliação da precisão e relevância das informações fornecidas pelos agentes. • **Produtividade das Equipes**: Aumento na capacidade de análise e no volume de trabalho realizado pelas equipes apoiadas pelos agentes de IA.
	C2 – Contratar serviços de IA para apoio em pesquisas, análises de documentos e criação de conteúdo relacionadas às diversas atividades das áreas fim e meio da SECONT.	• **Número de Relatórios/Análises Aceleradas**: Quantidade de documentos, pesquisas ou análises complexas que tiveram seu tempo de produção reduzido significativamente pelo uso de IA. • **Qualidade e Profundidade das Análises**: Avaliação subjetiva (por especialistas) da melhoria na qualidade e profundidade das análises geradas com apoio da IA. • **Retorno sobre o Investimento (ROI)**: Comparação entre o custo dos serviços de IA e os benefícios gerados (economia de tempo, melhoria de qualidade, etc.).

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Objetivo	Ações	Métricas
D – Fortalecimento da Cultura de Integridade.	D1 – Utilizar a IA para identificar conflitos de interesse através do cruzamento de bases de dados heterogêneas (como diários oficiais, portais de transparência e dados de vínculos familiares).	• **Número de Potenciais Conflitos de Interesse Identificados**: Volume de alertas gerados pela IA que indicam possíveis conflitos. • **Taxa de Validação dos Alertas**: Percentual de alertas de IA que, após investigação humana, são confirmados como conflitos de interesse reais. • **Impacto na Prevenção**: Redução no número de casos confirmados de conflito de interesse em determinado período, atribuível à capacidade preditiva da IA.
	D2 – Utilizar a IA para ampliar a análise de redes de relacionamento e ajudar a mapear conexões que possam indicar favorecimentos e conluios em licitações e investigações.	• **Detecção de Conluios**: Número de casos de conluio ou favorecimento identificados com o auxílio da IA. • **Tempo de Investigação**: Redução do tempo médio necessário para investigar casos complexos de corrupção ou fraude, devido à aceleração da análise de redes. • **Impacto em Processos**: Número de sanções aplicadas ou processos abertos a partir de evidências de conluio identificadas pela IA.
E – Monitoramento Contínuo e Proativo.	E1 – Utilizar a IA na detecção de anomalias em tempo real e criar as condições para monitoramento contínuo de sistemas com o objetivo de sinalizar desvios fora do padrão esperado.	• **Volume de Anomalias Detectadas**: Número de desvios significativos ou comportamentos incomuns sinalizados pela IA. • **Tempo de Resposta a Anomalias**: Diminuição do tempo entre a ocorrência de uma anomalia e o alerta gerado pela IA. • **Redução de Incidentes**: Diminuição do número de incidentes de segurança, fraude ou falhas operacionais graças à detecção proativa da IA. • **Falsos Positivos na Detecção de Anomalias**: Percentual de alertas de anomalia que não correspondem a um problema real.
	E2 – Utilizar a IA na monitoria de riscos em tempo real e na geração de alertas e recomendações automatizadas capazes de orientar os gestores e demais responsáveis.	• **Número de Alertas de Risco Gerados**: Volume de notificações de risco enviadas pela IA aos gestores. • **Relevância dos Alertas**: Avaliação da pertinência e da capacidade dos alertas em orientar decisões e ações corretivas. • **Implementação de Recomendações**: Percentual de recomendações da IA que foram efetivamente adotadas pelos gestores. • **Redução de Perdas/Danos**: Impacto financeiro ou operacional evitado devido à intervenção proativa baseada em alertas de risco da IA.
F – Melhorar a Eficiência Operacional.	F1 – Capacitar os servidores da SECONT no uso e conhecimento geral das soluções de IA com foco na compreensão básica do que é IA, como funciona e suas aplicações no setor público.	• **Número de Servidores Capacitados**: Contagem de servidores que concluíram os cursos de capacitação geral em IA. • **Nível de Compreensão**: Avaliação do conhecimento adquirido pelos servidores através de testes ou pesquisas de proficiência antes e depois do treinamento. • **Satisfação com o Treinamento**: Feedback dos participantes sobre a qualidade e relevância do conteúdo e da metodologia do curso. • **Aumento da Confiança na IA**: Pesquisas de percepção sobre a confiança e o conforto dos servidores em relação ao uso da IA em suas atividades.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Objetivo	Ações	Métricas
	F2 – Capacitar os servidores da SECONT no uso das soluções e recursos da IA nas atividades específicas do órgão, tais como: auditoria, fiscalização, investigação e monitoramento.	• **Número de Servidores Certificados em Ferramentas Específicas**: Contagem de servidores que demonstraram proficiência no uso de ferramentas de IA específicas para suas áreas. • **Aumento da Utilização das Ferramentas de IA**: Monitoramento da frequência e do escopo de uso das soluções de IA pelas equipes. • **Melhoria no Desempenho de Tarefas Específicas**: Avaliação do impacto da capacitação na performance dos servidores em suas atividades (ex: tempo para concluir uma análise, acurácia das identificações). • **Feedback dos Gestores**: Avaliação dos líderes de equipe sobre a melhoria na capacidade e produtividade de seus subordinados após a capacitação específica em IA.

8. RISCOS IDENTIFICADOS.

A implementação de uma estratégia de Inteligência Artificial (IA), apesar de seus múltiplos benefícios, não está isenta de riscos. Para cada objetivo existem desafios inerentes que precisam ser identificados e gerenciados proativamente. Conhecer esses riscos é o primeiro passo para desenvolver estratégias de mitigação eficazes, garantindo que o potencial da IA seja plenamente realizado sem comprometer a confiança pública ou a integridade das operações da Secretaria.

A seguir, estão os principais riscos associados a cada objetivo e suas respectivas ações:

Objetivo	Riscos
A – Aumento da Eficiência nas Auditorias e Inspeções.	Riscos Gerais: • **Vieses nos Dados ou Algoritmos**: A IA pode perpetuar ou amplificar vieses existentes nos dados de treinamento, levando a auditorias que focam desproporcionalmente em certos grupos ou setores, negligenciando outros. • **Falsos Positivos/Negativos Excessivos**: Muitos alertas irrelevantes (falsos positivos) podem sobrecarregar as equipes, enquanto a falha em identificar irregularidades reais (falsos negativos) pode comprometer a fiscalização. • **Dependência Excessiva da IA**: A confiança cega nos resultados da IA pode levar à diminuição do pensamento crítico e da expertise humana, resultando em falhas de fiscalização quando a IA não for precisa. • **Resistência à Mudança**: Servidores podem resistir à adoção de novas ferramentas que alterem seus métodos de trabalho tradicionais.
	Riscos Específicos: • **Complexidade dos Dados**: Dificuldade em integrar, padronizar e limpar grandes volumes de dados heterogêneos para treinamento da IA. • **Desatualização dos Modelos**: Modelos de IA podem perder eficácia com o tempo se os padrões de fraude ou irregularidade evoluírem e os modelos não forem retreinados. • **Custos de Manutenção**: Manter e atualizar os algoritmos e a infraestrutura de IA pode ser mais caro do que o previsto.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Objetivo	Riscos
B – Melhoria na Transparência e no Acesso à Informação.	Riscos Gerais: • **Imprecisão das Respostas**: Assistentes virtuais podem fornecer informações incorretas ou incompletas, gerando desinformação e frustração. • **Falta de Compreensão da Linguagem Natural**: Limitações da IA em entender nuances e intenções complexas nas perguntas dos usuários. • **Problemas de Privacidade**: O uso indevido de dados nas interações com os assistentes pode expor informações sensíveis.
	Riscos Específicos: • **Segurança de Dados**: Vulnerabilidades podem permitir acesso não autorizado a informações pessoais ou sensíveis através dos assistentes. • **Sobrecarga de Expectativas**: Usuários podem ter expectativas irrealistas sobre as capacidades do assistente, levando à insatisfação. • **Manutenção de Conteúdo**: Garantir que as informações fornecidas pelo assistente estejam sempre atualizadas com as últimas normas e procedimentos da SECONT.
C – Apoio à Tomada de Decisão Baseada em Dados.	Riscos Gerais: • **Confiança Excessiva**: Decisores podem se basear cegamente nas recomendações da IA sem o devido julgamento crítico. • **Opacidade dos Algoritmos**: Dificuldade em compreender como a IA chegou a certas recomendações, o que pode minar a confiança e a capacidade de contestação. • **Privacidade e Segurança dos Dados**: Acesso e manuseio de grandes volumes de dados sensíveis para análises.
	Riscos Específicos: • **Integração de Sistemas**: Dificuldade em conectar os agentes de IA com as diversas bases de dados e sistemas corporativos via API. • **Qualidade dos Dados de Entrada**: Dados de má qualidade ou incompletos podem levar a análises e recomendações falhas. • **Capacidade de Infraestrutura**: Agentes podem consumir recursos substanciais da infraestrutura existente.
D – Fortalecimento da Cultura de Integridade.	Riscos Gerais: • **Falsos Positivos**: Identificação errônea de conflitos de interesse ou redes suspeitas, levando a investigações desnecessárias e danos à reputação. • **Vieses nos Dados**: A IA pode aprender vieses nos dados históricos, resultando na perseguição de determinados grupos ou na negligência de outros. • **Invasão de Privacidade**: O cruzamento de dados sensíveis pode gerar preocupações com a privacidade dos indivíduos.
	Riscos Específicos: • **Complexidade do Cruzamento de Dados**: Dificuldade técnica em integrar e analisar dados de fontes muito distintas e não estruturadas. • **Limitações Legais/Éticas**: Restrições legais ou éticas para o acesso e cruzamento de determinados tipos de dados.
E – Monitoramento Contínuo e Proativo.	Riscos Gerais: • **Falsos Positivos**: Geração excessiva de alertas que não correspondem a anomalias reais, causando fadiga de alerta e perda de confiança nos resultados. • **Sensibilidade da IA**: A IA pode não ser sensível o suficiente para detectar desvios sutis ou novos tipos de anomalias. • **Segurança dos Dados Monitorados**: Vulnerabilidades no sistema de monitoramento podem expor dados sensíveis.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

	Riscos Específicos: • **Custo de Infraestrutura**: A necessidade de processamento em tempo real pode exigir uma infraestrutura tecnológica robusta e cara. • **Latência**: Atrasos na detecção de anomalias ou na geração de alertas podem comprometer a proatividade. • **Complexidade da Manutenção**: Modelos de detecção de anomalias precisam ser constantemente atualizados para se adaptarem a novos padrões de comportamento. • **Responsabilidade Legal**: Questões sobre a responsabilidade em caso de falha da IA em detectar um risco ou anomalia que cause algum tipo de dano.
F – Melhorar a Eficiência Operacional.	Riscos Gerais: • **Subutilização da Capacitação**: Servidores podem não aplicar o conhecimento adquirido, resultando em baixo retorno sobre o investimento em treinamento. • **Desengajamento**: Falta de interesse ou percepção de relevância dos treinamentos por parte dos servidores. • **Recursos Limitados**: Orçamento e tempo insuficientes para oferecer treinamento contínuo e de qualidade para todos os servidores.
	Riscos Específicos: • **Resistência à Mudança**: Servidores podem ter dificuldades em adaptar-se às novas ferramentas e metodologias baseadas em IA. • **Disparidade de Habilidades**: Diferentes níveis de aptidão e familiaridade com tecnologia entre os servidores podem dificultar a padronização da capacitação. • **Conteúdo Desatualizado**: A rápida evolução da IA exige que os materiais de treinamento sejam constantemente revisados e atualizados.

9. FATOR DE VIABILIDADE TÉCNICA DAS AÇÕES.

A ambição de integrar a Inteligência Artificial nas operações da SECONT é promissora, mas sua concretização depende de uma análise rigorosa da viabilidade técnica de cada ação proposta, com exceção das ações de capacitação. Este capítulo se dedica a examinar os requisitos tecnológicos, infraestruturais e de dados necessários para transformar os objetivos estratégicos em realidade.

Avaliar a viabilidade técnica não significa apenas identificar o que é possível, mas também o que é prático, sustentável e seguro dentro do contexto da SECONT. Consideraremos a disponibilidade de talentos e recursos, a compatibilidade com os sistemas existentes, a qualidade e acessibilidade dos dados, e a robustez da infraestrutura de TI.

Ação	Dados disponíveis?	Infraestrutura disponível?	Arquitetura definida?	Integração possível?	Pessoal capacitado?	Viabilidade técnica	Risco de execução
A1 – Utilizar algoritmos de IA para prever onde há maior probabilidade de ocorrência de irregularidades.	Não	Sim	Não	Talvez	Sim	5	Moderado
A2 – Utilizar recursos de IA no processamento de documentos, planilhas, contratos para identificar inconsistências, fraudes ou padrões suspeitos.	Não	Sim	Não	Talvez	Sim	5	Moderado

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Ação	Dados disponíveis?	Infraestrutura disponível?	Arquitetura definida?	Integração possível?	Pessoal capacitado?	Viabilidade técnica	Risco de execução
B1 – Criar assistentes virtuais inteligentes capazes de auxiliar cidadãos, servidores e gestores com dúvidas sobre processos, normas e procedimentos.	Não	Sim	Não	Talvez	Sim	5	Moderado
B2 – Criar assistentes virtuais inteligentes para auxiliar a navegação no Portal da Transparência, extraindo e consolidando informações através de uma interface em linguagem natural.	Sim	Sim	Não	Sim	Sim	8	Baixo
C1 – Criar localmente agentes de IA conversacionais capazes de apoiar as equipes da SECONT consultando bases de documentos, bancos de dados e sistemas corporativos via API.	Sim	Sim	Não	Sim	Sim	8	Baixo
C2 – Contratar serviços de IA para apoio em pesquisas, análises de documentos e criação de conteúdo relacionadas às diversas atividades das áreas fim e meio da SECONT.	Sim	Sim	Sim	Sim	Sim	10	Muito Baixo
D1 – Utilizar a IA para identificar conflitos de interesse através do cruzamento de bases de dados heterogêneas.	Não	Sim	Não	Talvez	Talvez	4	Alto
D2 – Utilizar a IA para ampliar a análise de redes de relacionamento e ajudar a mapear conexões que possam indicar favorecimentos e conluios em licitações e investigações.	Não	Sim	Não	Talvez	Talvez	4	Alto
E1 – Utilizar a IA na detecção de anomalias em tempo real e criar as condições para monitoramento contínuo de sistemas.	Não	Não	Não	Talvez	Talvez	2	Muito Alto
E2 – Utilizar a IA na monitoria de riscos em tempo real e na geração de alertas e recomendações automatizadas capazes de orientar os gestores e demais responsáveis.	Não	Não	Não	Talvez	Talvez	2	Muito Alto

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

10. OBSTÁCULOS ORGANIZACIONAIS.

A implementação da Inteligência Artificial na SECONT enfrentará uma série de obstáculos organizacionais. Tais desafios, muitas vezes não técnicos, podem ser tão ou mais complexos que os puramente tecnológicos, demandando uma abordagem estratégica para serem superados. Entender esses pontos críticos é essencial para planejar de forma eficaz, mitigando riscos e garantindo a adesão de todo o órgão ao projeto.

Os principais obstáculos podem ser formulados como questões estratégicas que devem ser tratadas ao longo de todo o ciclo de vida das soluções de IA propostas.

a. Cultura Organizacional e Resistência à Mudança.

Questão Estratégica: A cultura organizacional da SECONT pode ser resistente a inovações disruptivas. Servidores acostumados a processos manuais ou estabelecidos podem temer a substituição de suas funções pela IA, a necessidade de adquirir novas habilidades ou a simples mudança de rotina.

Solução	Responsáveis	O que deve ser feito
Fomentar uma cultura de inovação e experimentação.	Alta direção	• **Comunicação Transparente**: Explicar claramente os benefícios da IA para a organização e para os servidores, destacando que a IA é uma ferramenta de apoio, não de substituição. • **Programas de Conscientização**: Realizar workshops e seminários sobre o potencial da IA no setor público e como ela pode otimizar o trabalho.

b. Deficiência de Habilidades e Conhecimento.

Questão Estratégica: A SECONT pode não possuir internamente todas as habilidades necessárias em IA, ciência de dados, engenharia de dados, ou mesmo em alfabetização digital avançada. A falta de conhecimento pode dificultar a adoção, a gestão e a manutenção das soluções de IA.

Solução	Responsáveis	O que deve ser feito
Construir e/ou adquirir as competências necessárias.	Alta direção GTIC CIED	• **Capacitação Contínua**: Implementar um plano robusto de treinamentos para todos os níveis, desde a alfabetização digital básica até especializações em IA para equipes técnicas. • **Programas de Reciclagem/Reskilling**: Oferecer programas que permitam aos servidores existentes adquirir novas habilidades relevantes para o ambiente com IA. • **Parcerias Estratégicas**: Buscar colaboração com universidades, centros de pesquisa ou empresas especializadas para transferência de conhecimento e capacitação.

c. Questões Legais e Regulatórias.

Questão Estratégica: O uso de IA no setor público enfrenta desafios regulatórios e legais específicos, como a LGPD, a LAI e a necessidade de garantir a auditabilidade e a não-discriminação das decisões automatizadas.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Solução	Responsáveis	O que deve ser feito
Garantir a conformidade legal e ética.	Alta direção GTIC CIED	• **Assessoria Jurídica**: Contar com apoio especializado para garantir que todas as ações estejam em conformidade com a legislação vigente e futura. • **Avaliações de Impacto de Proteção de Dados**: Realizar avaliações para todos os projetos de IA que envolvam dados pessoais. • **Diretrizes Éticas Claras**: Desenvolver um código de conduta para o uso da IA na SECONT, alinhado aos princípios de transparência, equidade e responsabilidade.

d. Financiamento e Alocação de Recursos.

Questão Estratégica: A implementação da IA requer investimentos significativos em tecnologia, talentos e treinamento. A alocação orçamentária pode ser um obstáculo, especialmente em um contexto de restrições financeiras do setor público.

Solução	Responsáveis	O que deve ser feito
Garantir um orçamento adequado e sustentável.	Alta direção	• **Plano de Investimento**: Desenvolver um plano de investimento detalhado e justificado para a IA. • **Busca por Fontes de Financiamento**: Explorar parcerias com outras instituições ou financiamento externo, quando aplicável. • **Priorização de Projetos**: Priorizar os projetos de IA com maior potencial de impacto e viabilidade, começando com pilotos que demonstrem valor rapidamente.

11. CONCLUSÃO.

A Estratégia de Inteligência Artificial da SECONT representa um passo fundamental na modernização e no aprimoramento das capacidades do órgão. Ao abraçar o potencial da IA, a Secretaria reafirma seu compromisso com a eficiência, a transparência e a excelência na gestão pública, buscando otimizar recursos e fortalecer sua atuação em prol da sociedade.

A implementação bem-sucedida desta estratégia exigirá esforço colaborativo, investimento contínuo e uma governança robusta, consolidando a SECONT como um órgão inovador e referência na aplicação de tecnologias avançadas no setor público.

12. REFERÊNCIAS.

1. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais – LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018.

2. BRASIL. **Decreto nº 11.882, de 20 de dezembro de 2023**. Institui a Estratégia Nacional de Inteligência Artificial – ENIA. Diário Oficial da União, Brasília, DF, 21 dez. 2023.

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

3. OECD. **OECD Principles on Artificial Intelligence**. Paris: OECD Publishing, 2019. Disponível em: https://www.oecd.org/going-digital/ai/principles/. Acesso em: 6 jun. 2025.

4. CGU – Controladoria-Geral da União. **Referencial de Governança de Tecnologia da Informação e Comunicação do Poder Executivo Federal**. Brasília: CGU, 2022.

5. TCU – Tribunal de Contas da União. **Referencial Básico de Governança de Dados e Informação**. Brasília: TCU, 2021.

6. Gartner, Inc. – **Ferramenta de planejamento de IA generativa**. © 2023 Gartner.

7. IBM. **Como criar uma estratégia de IA bem-sucedida**. Disponível em: https://www.ibm.com/br-pt/think/insights/artificial-intelligence-strategy

Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700