GOVERNO DO
ESPÍRITO
SANTO

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Biênio 2026/2027
Revisão 1

SECRETARIA DE CONTROLE
E TRANSPARÊNCIA

Março 2026

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

MISSÃO
Contribuir para o aperfeiçoamento das políticas públicas e contribuir para a evolução da qualidade na aplicação dos recursos em benefício da sociedade.

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

VALORES
I. **Integridade**: Agir com ética, honestidade, imparcialidade, moralidade e legalidade.

II. **Autonomia Técnica**: Refere-se a autonomia e liberdade técnica que a equipe de auditoria interna tem para realizar seu trabalho de forma independente e objetiva.

III. **Zelo Profissional**: Trabalhar com excelência, produtividade, comprometimento, eficiência, agregação de valor e resultado na preservação dos bens e interesses da sociedade.

IV. **Melhoria Contínua**: Refere-se ao esforço contínuo na promoção da melhoria das atividades desenvolvidas de maneira a agregar valor nos serviços prestados à população.

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

Plano Diretor de Tecnologia da Informação e Comunicação Biênio 2026/2027

Elaboração: Emerson Couto de Moura

Vitória, Espírito Santo
30 de março de 2026
Revisão 1

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. CONTEXTUALIZAÇÃO.

Este documento apresenta o **Plano Diretor de Tecnologia da Informação e Comunicação** (**PDTIC**) da **Secretaria de Estado de Controle e Transparência** (**SECONT**) para o período de abril de 2026 a abril de 2028 (Biênio 2026/2027), em conformidade com o **Decreto 5871-R, de 18 de novembro de 2024**, que dispõe sobre as competências e obrigações da **Gerência de Tecnologia da Informação e Comunicação** (**GTIC**).

O PDTIC tem como finalidade definir as diretrizes e prioridades da área de Tecnologia da Informação e Comunicação (TIC) em alinhamento com os objetivos estratégicos da SECONT, conforme definido em seu Planejamento Estratégico para o período de 2023 a 2027. Trata-se de um instrumento tático fundamental para assegurar que a TIC contribua efetivamente para a modernização institucional, para a entrega de valor público e para o fortalecimento do controle interno.

Sua elaboração contou com participação das unidades finalísticas da SECONT, assegurando que as iniciativas tecnológicas estejam conectadas às necessidades operacionais e estratégicas das áreas de negócio. O processo colaborativo resultou em um plano orientado à entrega de resultados concretos, otimização de recursos e superação de desafios estruturais.

Adotando o *framework* de gestão por **Objetivos e Resultados Chave** (**OKRs**), o PDTIC organiza suas ações em **cinco temas estratégicos**, estruturados com escopos definidos, metas qualificadas e indicadores mensuráveis (**KRs**), além de mecanismos adequados para acompanhamento sistemático. Essa abordagem fortalece o alinhamento entre planejamento e execução, promove a integração entre áreas técnicas e finalísticas, bem como potencializa o impacto institucional das iniciativas de TI.

Além disso, o Plano integra os instrumentos de planejamento institucional ao posicionar a tecnologia como elemento estruturante para a geração de valor público. A TIC apoia decisões baseadas em evidências, viabiliza ações mais tempestivas e impulsiona a inovação em processos, produtos e serviços voltados à sociedade e ao público cliente da SECONT. Assim, consolida-se como alavanca estratégica para a execução das políticas institucionais, garantindo que os investimentos tecnológicos estejam alinhados aos resultados esperados pelas áreas de negócio.

O PDTIC 2026/2027 reconhece a importância de uma cultura institucional orientada por dados, da segurança da informação e do uso ético e eficiente da inteligência artificial. A atuação da TIC é transversal e estratégica, impulsionando a adoção de tecnologias relevantes para a atuação institucional da SECONT.

Dessa forma, o PDTIC reafirma o papel da Tecnologia da Informação e Comunicação como vetor de transformação institucional da SECONT. Ao conjugar visão de longo prazo com ações táticas bem definidas, consolida-se como ferramenta essencial para o aprimoramento da atuação do órgão e para a entrega sustentável de valor público à sociedade capixaba.

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

2. PRIORIDADES DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO.

A definição das prioridades da área de Tecnologia da Informação e Comunicação para o biênio 2026/2027 reflete o compromisso da SECONT em utilizar a TIC como vetor de transformação organizacional, integrando os objetivos do **Planejamento Estratégico Institucional 2023/2027** aos desafios e oportunidades identificados na construção do PDTIC.

Com base em levantamentos realizados nas unidades das áreas de negócio e nas orientações da direção da SECONT, foram priorizadas iniciativas voltadas ao atendimento dos objetivos estratégicos institucionais.

Dessa forma, no período de vigência indicado no PDTIC, a atuação da TIC será orientada por **duas** grandes frentes de contribuição estratégica, conforme as Perspectivas e Objetivos definidos no Planejamento Estratégico Institucional da SECONT para o período 2023/2027:

Frente	Perspectiva	Objetivo Estratégico
1	Orçamento e Infraestrutura	Promover infraestrutura adequada ao desempenho das atividades.
2	Processos Internos	Aperfeiçoar a legislação e os procedimentos internos.

Na **Frente 1** os esforços estarão concentrados na modernização do ecossistema de dados e IA, no fortalecimento da segurança cibernética e na criação de uma capacidade produtiva interna de software.

Principais áreas de atuação:

- **Ampliação do DataStack Institucional**: O foco será a evolução da arquitetura de dados e das ferramentas disponíveis para permitir o processamento de grandes volumes de dados e a melhor integração de bases heterogêneas.

- **Liberação de Ferramentas de IA e Produtividade**: A TIC disponibilizará um ambiente governado para o uso de IA, focado no aumento da produtividade dos auditores.

- **Implantação do Sistema de Gestão de Segurança da Informação (SGSI)**: Em conformidade com as normas ISO/IEC 27001 e 27002, a TIC formalizará o SGSI da SECONT para garantir a confidencialidade, integridade e disponibilidade dos sistemas, dados e informações custodiadas.

- **Melhoria da Infraestrutura de Publicação de Aplicações**: Inclui a transição para uma infraestrutura baseada em contêineres e orquestração, permitindo que as soluções sejam entregues com maior agilidade e estabilidade.

- **Montagem de Equipe de Desenvolvimento de Software**: Composição de uma equipe multidisciplinar (Desenvolvedores, Analistas de Requisito e Scrum Master) operando sob metodologias ágeis, focada no desenvolvimento de sistemas customizados que respondam rapidamente às demandas do órgão.

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

Já na **Frente 2** o foco deixa de ser apenas a "entrega de tecnologia" e passa a ser a "entrega de valor e continuidade", assegurando que a SECONT cumpra seu papel sem interrupções.

Principais áreas de atuação:

- **Estratégias de Atendimento e Experiência do Usuário**: A TIC estabelecerá um novo modelo de gestão de serviços baseado em *frameworks* de mercado, visando a padronização e a agilidade no suporte aos servidores da SECONT e aos usuários externos dos sistemas do órgão. Esta área de atuação irá permear todos os demais projetos planejados, isso ocorrerá através da incorporação das eventuais demandas de suporte à estrutura técnica e de atendimento existente.

- **Resiliência Operacional e Continuidade de Negócios**: Considerando a criticidade dos dados de controle e transparência, a TIC implementará uma estratégia robusta de resiliência, alinhada à norma ISO 22301.

- **Plano de Recuperação de Desastres**: Para assegurar a integridade do patrimônio informacional da SECONT frente a eventos catastróficos, será formalizado o Plano de Recuperação de Desastres.

- **Governança Normativa e Conformidade**: O aperfeiçoamento dos processos internos passará pela revisão e criação de normativas que deem suporte legal às operações de TIC na Secretaria.

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. DEFINIÇÕES, EXECUÇÃO, OBJETIVOS E ABRANGÊNCIA.

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da Secretaria de Estado de Controle e Transparência (SECONT) para o biênio 2026/027 (abril de 2026 a abril de 2028) é um instrumento tático que orienta o planejamento, a priorização e a execução das iniciativas de TIC, em complemento ao Planejamento Estratégico Institucional. Enquanto este define a direção estratégica da organização, o PDTIC detalha como a área de TIC contribuirá para o alcance das suas diretrizes e objetivos, por meio de ações estruturadas e alinhadas às necessidades das áreas de negócio.

No contexto da SECONT, o PDTIC reflete os compromissos da gestão com a entrega de valor, com a modernização dos serviços digitais disponíveis e com a segurança da informação. Sua construção ocorreu de forma colaborativa, com participação das unidades finalísticas, o que possibilitou a identificação de temas prioritários e o alinhamento às demandas reais e enfrentadas no cotidiano da Secretaria. O plano fornece, assim, uma visão clara das necessidades de negócio relacionadas à tecnologia, orientando a alocação de recursos e a priorização de iniciativas.

A metodologia utilizada parcialmente para a elaboração deste documento foi a definida pelo Guia de Elaboração de PDTIC do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação), versão 2.1, desenvolvida pela **Secretaria de Governo Digital** do governo federal através da sua **Coordenação-Geral de Governança de Tecnologia da Informação**, que tem como base as melhores práticas de gestão com foco na Administração Pública, combinada com outras metodologias de planejamento. A organização elaborada neste documento foi baseada no **Plano Diretor de Tecnologia da Informação (PDTI**) do **Tribunal de Contas da União (TCU**) para o período 2025/2027.

3.1. Unidades Executoras de Projetos de TIC.

A SECONT possui formalmente duas unidades técnicas e executoras de projetos de TIC, a **Coordenação de Informações Estratégicas e Análise de Dados** (**CIED**) e a **Gerência de Tecnologia da Informação e Comunicação** (**GTIC**). Também há, eventualmente, a execução descentralizada de projetos menores em outros setores.

De forma geral, os setores não ligados especificamente a uma das áreas de TIC desenvolvem apenas projetos sobre suas respectivas competências finalísticas. Já a GTIC e a CIED atuam de forma mais ampla, desenvolvendo projetos de TIC para todos os demais setores.

Em considerável parte dos projetos avulsos de TIC que gerenciam, esses setores atuam como clientes do **Instituto de Tecnologia da Informação e Comunicação do Estado do Espírito Santo – PRODEST**, não desenvolvendo ou executando eles mesmos qualquer atividade operacional ou contratação de bens e serviços de TIC.

Pelo exposto, convencionou-se que somente os projetos de TIC cujo planejamento, execução operacional, monitoramento e fiscalização estejam sob a responsabilidade direta da GTIC e da CIED são elegíveis para o portfólio deste PDTIC.

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

3.2. *Framework* e Temas Estratégicos.

As prioridades das áreas finalísticas estão organizadas conforme o proposto pelo *framework* de **Objetivos e Resultados Chave** (*Objectives and Key Results - OKR*), agrupadas em **cinco temas estratégicos** para a TIC. Cada tema representa um eixo de atuação relevante para a evolução da Tecnologia da Informação e Comunicação na SECONT, contendo metas claras, mensuráveis e orientadas a resultados.

Esses temas foram definidos com base nas diretrizes da gestão e nas contribuições das áreas usuárias, refletindo a ambição de consolidar uma TIC estratégica, proativa e integrada ao negócio institucional.

Os cinco temas que direcionarão os trabalhos da Gerência de Tecnologia da Informação e Comunicação (GTIC) no período coberto por este PDTIC são:

1. **Ampliação e universalização do uso da Inteligência Artificial Generativa.**
2. **Nuvem pública e serviços *online* – Transformação cultural e operacional.**
3. **Automação, desenvolvimento de *software* e serviços de dados.**
4. **Segurança da Informação.**
5. **Garantia de Continuidade do Negócio.**

Cada tema desdobra-se em objetivos e resultados-chave, compondo um mapa claro das entregas esperadas da TIC ao longo do período contemplado no PDTIC, de acordo com as frentes de contribuição estratégicas. O foco está em promover uma atuação cada vez mais integrada à estratégia institucional, com responsabilidade sobre a sustentação de serviços críticos, a segurança da informação, a inovação e o suporte à transformação digital da SECONT.

Além dos OKRs, o PDTIC contempla a **Estimativa do Portfólio Orçamentário**, que apresenta os recursos financeiros necessários à execução das iniciativas previstas para o biênio. Essa estimativa é fundamental para o planejamento financeiro e a alocação eficiente de recursos, assegurando a viabilidade técnica e orçamentária das ações. Os valores são atualizados de acordo com a evolução da programação orçamentária da SECONT e o ciclo de aprovação das Leis Orçamentárias Anuais.

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

4. OBJETIVOS E RESULTADOS CHAVE ORGANIZADOS POR TEMAS.

4.1. Tema 1: Ampliação e universalização do uso da Inteligência Artificial Generativa.

O objetivo central deste tema é transcender o uso experimental atual e consolidar a IA, em especial a IA Generativa, como um pilar fundamental e onipresente na cultura organizacional e nos processos de controle e transparência. A "Ampliação e Universalização" não se limita à aquisição de ferramentas, mas abrange uma transformação estrutural dividida em três camadas: **Infraestrutura**, **Capacitação** e **Aplicação Finalística**.

Sob a ótica do *framework* OKR (*Objectives and Key Results*) adotado neste PDTIC, o Objetivo Estratégico Geral da TIC para este tema é:

> *Converter a SECONT em uma organização orientada por dados e assistida por IA, bem como reduzir o tempo de resposta em auditorias, inspeções, investigações e aumentando a precisão das análises*.

Para viabilização deste tema, definimos as seguintes demandas de trabalho:

a) Infraestrutura e Ecossistema de IA.

- **Contratação Corporativa do Gemini via Google Workspace**: Implementação das ferramentas de IA generativa (Gemini) integradas ao cotidiano administrativo, permitindo automação de minutas, sumarização de reuniões e organização de fluxos de trabalho para todos os servidores.

- **Aquisição de Créditos de IA na Google Cloud (Vertex AI)**: Garantia de recursos computacionais para o treinamento de modelos específicos, uso de tokens para IA Generativa e o processamento de modelos diversos.

b) Capital Humano e Cultura.

- **Contratação de Capacitação Corporativa em IA**: Programa de letramento digital e treinamento avançado para auditores e demais servidores, focado em engenharia de prompts, análise de dados com IA e ética no uso de algoritmos no setor público.

c) Desenvolvimento de Agentes de IA Especializados.

- **Desenvolvimento de agentes conversacionais**: criação de "IA Workers" (agentes autônomos ou assistentes) para a Subsecretaria de Integridade, Subsecretaria de Transparência e Corregedoria. Todos com foco na interlocução com a massa documental produzida pelos setores e com bases de dados de sistemas.

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

A partir das contratações e demandas de trabalho definidas, os seguintes objetivos e resultados chave foram estabelecidos:

Objetivos	Resultados
O1: Transformar o Google Gemini no assistente onipresente da SECONT, automatizando tarefas burocráticas e elevando a qualidade técnica da produção documental.	**KR1: Adoção e engajamento em escala.** Alcançar 80% de usuários ativos mensais até dezembro de 2026. **KR2: Eficiência na produção de documentos.** Até junho de 2027 reduzir em 50% o tempo de redação e revisão de documentos, validado por amostragem de produtividade nas subsecretarias. **KR3: Padronização e qualidade de respostas (*Prompt Library*).** Até dezembro de 2026 implementar 15 "Prompts Corporativos Padrão" integrados ao fluxo de trabalho, garantindo que a IA mantenha um rigor técnico adequado.
O2: Promover o letramento em IA e a especialização técnica por meio de um programa de capacitação corporativa, visando transformar a SECONT em um ambiente de trabalho onde os servidores sejam capazes de utilizar, de forma ética e eficiente, ferramentas de IA generativa para otimizar suas entregas.	**KR1: Capacitação das equipes de trabalho.** Até dezembro de 2026, alcançar 80% de usuários capacitados na utilização adequada do Google Gemini.
O3: Potencializar a eficiência operacional da SUBINT, SUBTRAN e CORREGEDORIA mediante o desenvolvimento e integração de agentes de IA customizados.	**KR1: Agente conversacional da SUBINT.** Até dezembro de 2026, disponibilizar um agente de IA conversacional para interagir com a base documental da SUBINT. **KR2: Agente conversacional da CORREGEDORIA.** Até dezembro de 2026, disponibilizar um agente de IA conversacional para interagir com a base documental da CORREGEDORIA. **KR3: Agente de interação com a base de dados do sistema E-OUV**. Até março de 2027, disponibilizar um agente de IA conversacional para interagir, em tempo real, com a base de dados do sistema E-OUV e disponibilizá-lo online aos gestores da rede de Ouvidorias.

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

4.2. Tema 2: Nuvem pública e serviços online – Transformação cultural e operacional.

A adoção de uma nuvem pública pela SECONT não se limita à substituição de serviços locais ou mantidos pela PRODEST. Ela representa uma mudança na arquitetura de produtividade do órgão. A amplitude deste tema abrange três pilares fundamentais:

a) **Software como Serviço (SaaS)**: Implementação do Google Workspace como plataforma central de produtividade, garantindo que armazenamento, e-mail, agenda e ferramentas de edição existam em um ecossistema integrado e de alta disponibilidade, bem como mantendo compatibilidade com a base legada.

b) **Migração e Sustentação Especializada**: Contratação de consultoria técnica para garantir uma transição de dados "*zero loss*" (perda zero) e a configuração de políticas de segurança (DLP, criptografia e gestão de identidades) adequadas ao *compliance* do órgão.

c) **Letramento Digital e Gestão de Mudança**: Trata-se do reconhecimento de que a ferramenta, por si só, não gera valor. O tema engloba um plano robusto de capacitação para que os servidores deixem de usar a nuvem apenas como "disco virtual" e passem a utilizá-la como ambiente de colaboração em tempo real.

Sob a ótica do *framework* OKR (*Objectives and Key Results*) adotado neste PDTIC, o Objetivo Estratégico Geral da TIC para este tema é:

> *Consolidar a SECONT como um órgão de controle digitalmente nativo, transformando a colaboração em nuvem no alicerce de uma cultura organizacional ágil, segura e orientada a resultados.*

Para viabilização deste tema, definimos as seguintes demandas de trabalho:

a) **Infraestrutura e Ecossistema de Produtividade.**

- **Contratação Corporativa do Google Workspace e de Consultoria Técnica para Implantação**: Aquisição e integração das ferramentas do Google Workspace ao cotidiano operacional, permitindo colaboração, interatividade e comunicação institucional aprimoradas, bem como adoção de um plano de transição coerente com os fatores técnicos e culturais do órgão.

b) **Capital Humano e Cultura.**

- **Contratação de Capacitação Corporativa**: Elaboração e adoção de um programa de letramento digital e treinamento avançado no Google Workspace para auditores e demais servidores, com foco nas funcionalidades da plataforma e sua integração com os processos de trabalho, base documental, dados e políticas de utilização existentes no órgão.

A partir das contratações e demandas de trabalho definidas, os seguintes objetivos e resultados chave foram estabelecidos:

Objetivos	Resultados
O1: Modernizar o ambiente de colaboração para potencializar a produtividade.	**KR1: Criação de identidades corporativas.** Até dezembro de 2026 deve ser feita a criação de 100% das identidades corporativas da SECONT no Google Workspace, vinculadas ao serviço de diretório em uso. **KR2: Migração de e-mails e agendas.** Migração de 100% das contas de e-mail e agenda (Zimbra) para o Google Workspace até março de 2027. **KR3: Migração do serviço de vídeo conferência e reuniões online.** Migração de 100% dos serviços de conferência e reuniões online (Zoom) para o serviço Meet do Google Workspace até março de 2027. **KR4: Ambiente de armazenamento.** Até dezembro de 2026 deve ser feita a criação dos ambientes para armazenamento (Google Drive), conforme as políticas da SECONT.
O2: Fomentar a cultura digital e o uso pleno das ferramentas de nuvem.	**KR1: Capacitação corporativa.** Capacitar 80% dos usuários na utilização dos recursos colaborativos e de produtividade do Google Workspace até março de 2027. **KR2: Mudança cultural.** Alcançar 80% dos usuários usando plenamente os recursos colaborativos do Google Workspace até julho de 2027 (produção de documentos, comunicação instantânea, reuniões *onlines*, armazenamento, etc.).
O3: Estabelecer um ambiente de nuvem seguro.	**KR1: Políticas de proteção.** Proteger 100% dos dados críticos com políticas de DLP (*Data Loss Prevention*) até julho de 2027. **KR2: Autenticação.** Alcançar 100% de aplicação da autenticação multifator (MFA) nas contas de usuários até julho de 2027.

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

4.3. Tema 3: Automação, desenvolvimento de software e serviços de dados.

Este tema estabelece o compromisso da SECONT com a soberania tecnológica e a eficiência operacional. Em um cenário onde o controle governamental exige respostas em tempo quase real, a tecnologia deixa de ser um suporte para se tornar a própria viabilizadora das atividades finalísticas.

A amplitude deste tema abrange desde a mudança do modelo de força de trabalho — priorizando a retenção de conhecimento e a agilidade — até a modernização da base sobre a qual os sistemas operam. Não se trata apenas de "escrever código", mas de criar um ecossistema onde o dado flui com segurança e as aplicações são entregues com alta disponibilidade.

Os seguintes eixos de atuação se aplicam a este tema:

a) **Transição para Gestão Direta do Desenvolvimento de Softwares**: A substituição da Fábrica de Software tradicional por uma equipe de desenvolvedores sob gestão direta da SECONT marca uma mudança de paradigma. Espera-se maior agilidade na implementação de regras de negócio complexas e manutenção do conhecimento crítico dentro da instituição, evitando a dependência excessiva de fornecedores externos e fluxos burocráticos de ordens de serviço.

b) **Evolução do Ecossistema SIAC**: O Sistema Integrado de Atividades de Controle (SIAC) é o coração das atividades-fim da SECONT. Busca-se a centralização das informações de controle em uma plataforma única, garantindo a integridade dos dados e a automação de fluxos que antes eram manuais ou fragmentados.

c) **Modernização do Data Stack e Serviços de Dados**: Para que a SECONT seja verdadeiramente orientada a dados (*data-driven*), é necessária uma infraestrutura de dados moderna. Para isso, torna-se necessária a atualização das ferramentas de ingestão, processamento e visualização de dados presentes no Data Stack do órgão.

d) **Infraestrutura Automatizada (Kubernetes e OpenShift)**: Busca-se a migração das aplicações para uma arquitetura de microserviços altamente escalável, evitando os gargalos operacionais atuais. Da mesma forma, busca-se a automação da implantação de aplicações (CI/CD), garantindo que novas funcionalidades entrem em produção sem interrupções (*zero downtime*) e com resiliência a falhas.

Sob a ótica do *framework* OKR (*Objectives and Key Results*) adotado neste PDTIC, o Objetivo Estratégico Geral da TIC para este tema é:

> *Consolidar a soberania tecnológica e a excelência analítica da SECONT por meio de uma arquitetura de desenvolvimento ágil e serviços de dados de alto desempenho, transformando a TIC em um motor estratégico para a inovação no controle público.*

Para viabilização deste tema, definimos as seguintes demandas de trabalho:

a) **Infraestrutura de Publicação de Aplicações.**

- **Construção da Infraestrutura**: Disponibilização do OpenShift, das soluções de CI/CD e dos recursos de observalidade disponíveis no PRODEST em uma instância de uso exclusivo da SECONT, conforme a demanda de aplicações existente.

b) **Capital Humano.**

- **Contratação de Capacitação Corporativa Red Hat**: Contratação de capacitação técnica e consultoria da empresa Red Hat a partir de um Registro de Preços mantido pelo PRODEST. O propósito da capacitação e da consultoria será a operacionalização, configuração e personalização da infraestrutura e serviços providos pelo PRODEST conforme os interesses e necessidades da SECONT.

- **Contratação da Equipe de Desenvolvedores**: Contratação de 4 (quatro) desenvolvedores, um analista de requisitos e um Scrum Master para formar o time de desenvolvimento de software da SECONT.

c) **Atividades Técnicas da GTIC.**

- **Finalização de Módulos do SIAC**: Concluir os módulos do sistema SIAC em desenvolvimento pela empresa CAST e previstos no programa PROFISCO.

- **Atualizar e Ampliar o Data Stack**: Atualizar os serviços de dados existentes e ampliar a oferta de funcionalidades agregando uma camada de virtualização de dados e soluções de monitoria.

A partir das contratações e demandas de trabalho definidas, os seguintes objetivos e resultados chave foram estabelecidos:

Objetivos	Resultados
O1: Estabelecer uma infraestrutura de nuvem resiliente para a publicação de aplicações, garantindo autonomia operacional e agilidade no ciclo de vida das aplicações da SECONT.	**KR1: Prover infraestrutura.** Concluir o provisionamento e a configuração da instância exclusiva do Rede Hat OpenShift no PRODEST, com 100% dos recursos de rede e segurança homologados até julho de 2026. **KR2: Migração de aplicações.** Migrar 100% das aplicações em produção para o novo ambiente até dezembro de 2026. **KR3: Implantação CI/CD.** Implementar 100% das esteiras de CI/CD automatizadas (GitLab) até dezembro de 2026.

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

Objetivos	Resultados
O1: Estabelecer uma infraestrutura de nuvem resiliente para a publicação de aplicações, garantindo autonomia operacional e agilidade no ciclo de vida das aplicações da SECONT.	**KR4: Observabilidade.** Alcançar 100% de cobertura de observabilidade (*logs*, métricas e *traces*) em todos os serviços produtivos, permitindo a identificação de falhas em tempo real antes do impacto ao usuário final até dezembro de 2026.
O2: Elevar a maturidade técnica da equipe interna e assegurar a alta performance do ambiente Red Hat, transformando o conhecimento especializado em autonomia operacional para a SECONT.	**KR1: Adesão a Registro de Preços.** Concluir 100% do processo de adesão à Ata de Registro de Preços do PRODEST para serviços de consultoria e treinamento Red Hat até julho de 2026. **KR2: Capacitação da equipe.** Capacitar e certificar tecnicamente 100% dos servidores envolvidos nas trilhas oficiais de Administração do OpenShift e Automação, garantindo a retenção do conhecimento crítico até dezembro de 2026. **KR3: Consultoria técnica.** Até julho de 2027, executar 80% das horas de consultoria técnica previstas para "Fine-Tuning", resultando na aplicação de pelo menos 5 melhorias documentadas de arquitetura e segurança na instância exclusiva da SECONT. **KR4: Redução de chamados ao PRODEST.** Até julho de 2027, reduzir em 50% a dependência de chamados externos ao PRODEST para configurações avançadas de infraestrutura.
O3: Transformar a capacidade produtiva de software da SECONT em um ativo estratégico de alta agilidade, internalizando a inteligência de negócio e eliminando barreiras burocráticas entre a TIC e as áreas finalísticas.	**KR1: Processo licitatório.** Concluir 100% do processo licitatório para contratação da equipe de desenvolvedores, incluindo a disponibilização dos profissionais, até agosto de 2026. **KR2: Transição contratual.** Repassar 100% das atividades executadas no contrato atual para a nova equipe de desenvolvedores até março de 2027. **KR3: Redução do prazo de entregas.** Reduzir em 50% o tempo de entrega e homologação de funcionalidades complexas no SIAC até dezembro de 2027.

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

Objetivos	Resultados
O4: Consolidar o SIAC como o coração tecnológico e a fonte única de verdade para as atividades de controle, eliminando a fragmentação operacional e garantindo a integridade absoluta dos dados da SECONT.	**KR1: Conclusão de módulos previstos.** Até abril de 2027, concluir a homologação e entrada em produção de 100% dos módulos do SIAC previstos no escopo do programa PROFISCO II (CAST). **KR2: Integração do legado.** Integrar 50% dos sistemas legados ao SIAC até dezembro de 2027. **KR3: Documentação.** Até julho de 2027, homologar a documentação de 100% dos módulos do SIAC previstos no escopo do programa PROFISCO II (CAST). **KR4: Análise de requisitos de novos módulos.** Até dezembro de 2026, produzir os requisitos e histórias de usuários iniciais do módulo do Gabinete e de Outras Ações de Controle.
O5: Estabelecer uma infraestrutura de dados de alto desempenho, transformando grandes volumes de informações em ativos estratégicos para controle e tomada de decisão.	**KR1: Atualização de serviços.** Concluir a atualização e ampliação de recursos do Apache Spark, JupyterHub e Apache Airflow para as versões estáveis mais recentes até dezembro de 2026. **KR2: Camada de virtualização de dados.** Implementar e homologar o Trino como motor de consulta distribuída, integrando-o ao Data Lake até dezembro de 2026. **KR3: Framework de metadados.** Até março de 2027, implementar e homologar o Apache Iceberg como suporte a ACID aplicado a arquivos parquet no MinIO. **KR4: Camada de catálogo e versionamento.** Até março de 2027, implementar e homologar o Project Nessie e o GitLab para catálogo de metadados e versionamento dos códigos desenvolvidos pela CIED. **KR5: Camada de observalidade.** Até dezembro de 2027, implementar e homologar o Prometheus e Grafana para observabilidade do Stack. Considerar a adoção conjunta do OpenTelemetry para a coleta de logs, métricas e traces.

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

Objetivos	Resultados
O6: Estabelecer e consolidar os serviços de dados da SECONT.	**KR1: Serviços de dados desenvolvidos no SAS Viya / Visual Analytics.** Até dezembro de 2026 entregar e homologar o Painel investigativo da SUBINT, o Painel de Informações Gerenciais da SUBCONT e a Classificação de Demandas da Ouvidoria (SUBTRAN).

4.4. Tema 4: Segurança da Informação.

Este tema estabelece as diretrizes fundamentais para a proteção dos ativos de informação da SECONT. Em um cenário de crescente transformação digital e sofisticação de ameaças cibernéticas, a Segurança da Informação deixa de ser uma camada técnica para tornar-se um pilar estratégico de governança e continuidade institucional.

A abordagem adotada pela SECONT baseia-se na resiliência e na conformidade normativa, garantindo que a tecnologia impulsione as atividades finalísticas do órgão sem comprometer a confidencialidade, integridade e disponibilidade dos dados e informações.

A amplitude deste tema compreende a transição de uma segurança reativa para uma postura proativa e normativa. O escopo abrange desde a infraestrutura física e lógica até a camada humana e de processos, estruturando-se em três pilares normativos internacionais:

- **Sistemas de Gestão (SGSI)**: Implementação de controles baseados nas normas ISO/IEC 27001 (requisitos) e 27002 (boas práticas), definindo políticas, normas e procedimentos que padronizam a resposta a incidentes e a proteção de dados.

- **Gestão de Riscos**: Adoção das diretrizes da ISO/IEC 27005, permitindo que a SECONT identifique, analise e trate riscos de TI de forma sistemática, priorizando investimentos onde o impacto institucional é crítico.

- **Governança de Inteligência Artificial**: Antecipando os desafios da inovação, o tema incorpora a ISO/IEC 42001, estabelecendo controles específicos para que o uso de IA na SECONT seja ético, seguro e auditável.

Sob a ótica do *framework* OKR (*Objectives and Key Results*) adotado neste PDTIC, o Objetivo Estratégico Geral da TIC para este tema é:

> *Consolidar a SECONT como referência em resiliência digital e governança de dados, garantindo a integridade dos processos de controle e a inovação segura com Inteligência Artificial.*

Para viabilização deste tema, definimos as seguintes demandas de trabalho:

a) **Governança e Normatização (ISO/IEC 27001 e 27002)**.

- **Elaboração e Instituição do SGSI**: Definição do escopo, atualização da política de segurança (PSI) e reestruturação da governança (comitês).
- **Inventário e Classificação de Ativos**: Mapeamento dos ativos de informação da SECONT (dados, sistemas, hardware) e atribuição de níveis de criticidade.
- **Desenvolvimento de Normas Complementares**: Criação de normas específicas para controle de acesso, criptografia, dispositivos móveis e trabalho remoto.
- **Gestão de Vulnerabilidades**: Estabelecimento de um fluxo contínuo de varredura e correção de falhas em sistemas e servidores.

b) **Gestão de Riscos e Resiliência (ISO/IEC 27005)**.

- **Realização da Análise de Riscos de TI**: Identificação de ameaças e vulnerabilidades, calculando o impacto institucional de possíveis falhas.
- **Elaboração do Plano de Tratamento de Riscos (PTR)**: Definição de quais riscos serão aceitos, mitigados, transferidos ou evitados.

c) **Governança de Inteligência Artificial (ISO/IEC 42001)**.

- **Estabelecimento do Sistema de Gestão de IA**: Criação de diretrizes para o desenvolvimento de soluções com o uso de IA (incluindo LLMs).
- **Avaliação de Impacto Algorítmico**: Análise de riscos específicos de IA, como vazamento de dados via prompts, alucinações de modelos e vieses.
- **Controles de Segurança para IA**: Implementação de camadas de proteção para APIs de modelos de linguagem e monitoramento de outputs.

d) **Cultura e Conformidade.**

- **Programa de Conscientização em Segurança**: Campanhas de *phishing* simulado, treinamentos para servidores sobre a LGPD e boas práticas digitais.
- **Auditoria Interna de Segurança**: Verificação periódica para medir se o que foi escrito no SGSI está sendo praticado no dia a dia.

A partir das demandas de trabalho definidas, os seguintes objetivos e resultados chave foram 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

Objetivos	Resultados
O1: Estabelecer uma gestão da segurança da informação adequada, garantindo que os ativos da SECONT estejam mapeados, normatizados e protegidos contra ameaças emergentes.	**KR1: Institucionalização e conformidade normativa.** Desenvolver, publicar e disseminar a nova Política de Segurança da Informação (PSI) e o SGSI até julho de 2027. **KR2: Visibilidade e priorização de proteção baseada em risco.** Concluir o mapeamento e a classificação de criticidade de 100% dos ativos de informação críticos até julho de 2027.
O2: Estabelecer uma infraestrutura de governança e proteção de dados resiliente, garantindo que os ativos da SECONT estejam mapeados, normatizados e protegidos contra ameaças emergentes.	**KR1: Padronização de procedimentos e redução de brechas operacionais.** Instituir 04 Normas Complementares fundamentais (Controle de Acesso, Criptografia, Dispositivos Móveis e Trabalho Remoto) com seus respectivos fluxos operacionais validados até julho de 2027. **KR2: Resposta técnica e redução da superfície de ataque.** Até dezembro de 2027, implementar o fluxo de Gestão de Vulnerabilidades, garantindo a correção de 80% das falhas classificadas como "Críticas" ou "Altas" em até 30 dias.
O3: Reduzir a incerteza tecnológica e estabelecer uma visão clara do apetite a risco e da capacidade de resposta da SECONT ante ameaças críticas.	**KR1: Risco técnico.** Até dezembro de 2027, mapear e quantificar o impacto institucional (financeiro, reputacional e legal) de todas as vulnerabilidades classificadas como "Críticas" no ambiente de TIC. **KR2: Maturidade da tomada de decisão institucional.** Até dezembro de 2027, aprovar o Plano de Tratamento de Riscos (PTR) com estratégias de resposta (aceitar, mitigar, transferir ou evitar) para 100% dos riscos de nível "Alto".
O4: Liderar a transformação digital no controle público com o uso ético e seguro da Inteligência Artificial, assegurando a confiabilidade das soluções e a proteção do patrimônio informacional.	**KR1: Alicerce normativo.** Até julho de 2027, instituir o Sistema de Gestão de IA (SGIA) conforme a norma ISO/IEC 42001, com 100% dos novos projetos de TIC da SECONT seguindo as diretrizes propostas.

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

Objetivos	Resultados
O4: Liderar a transformação digital no controle público com o uso ético e seguro da Inteligência Artificial, assegurando a confiabilidade das soluções e a proteção do patrimônio informacional.	**KR2: Segurança técnica.** Até dezembro de 2027, implementar camadas de proteção e filtragem (exemplo: *AI Gateways* e *Guardrails*) para monitorar 100% das requisições via API das soluções em uso, bloqueando proativamente a inserção de dados sensíveis ou sigilosos em prompts de modelos de linguagem. **KR3: Avaliação de Impacto Algorítmico.** Até dezembro de 2027, realizar a Avaliação de Impacto Algorítmico (AIA) em 100% das soluções de IA e LLMs, identificando e mitigando riscos de vieses e alucinações.
O5: Fortalecer a cultura de resiliência digital da SECONT, assegurando que o fator humano e os processos institucionais estejam em total conformidade com os padrões de segurança e privacidade.	**KR1: Mudança comportamental.** Até dezembro de 2027, reduzir a taxa de sucesso de ataques de *phishing* simulado para menos de 5% entre todos os servidores da Secretaria. **KR2: Auditoria interna de segurança.** A partir de julho de 2027 e até dezembro de 2027, realizar um ciclo de Auditoria Interna de Segurança, cobrindo a totalidade dos controles críticos estabelecidos no SGSI.

4.5. Tema 5: Garantia de Continuidade do Negócio.

A continuidade do negócio na SECONT refere-se à capacidade estratégica e tática da Secretaria de se antecipar, resistir e recuperar-se de interrupções, sejam elas causadas por falhas técnicas, ataques cibernéticos ou desastres naturais. No contexto do PDTIC 2026/2027, este tema foca na proteção dos ativos críticos que sustentam as atividades finalísticas institucionais.

A amplitude deste tema transcende a simples realização de cópias de segurança (*backups*). Ela envolve uma visão holística organizada em três pilares:

- **Resiliência Tecnológica**: Alta disponibilidade de infraestrutura (servidores, nuvem e redes) para minimizar eventuais "*Single Point of Failure*" (Pontos Únicos de Falha).

- **Recuperação de Desastres (DR)**: Procedimentos técnicos e infraestrutura secundária para restaurar serviços em tempos aceitáveis (RTO - Recovery Time Objective).

- **Processos de Trabalho**: Planos de contingência que orientam os servidores sobre como proceder caso os sistemas principais fiquem inacessíveis.

Sob a ótica do framework OKR (*Objectives and Key Results*) adotado neste PDTIC, o Objetivo Estratégico Geral da TIC para este tema é:

> *Transformar a infraestrutura de TIC da SECONT em uma estrutura resiliente, assegurando a disponibilidade ininterrupta dos serviços oferecidos.*

Para viabilização deste tema, definimos as seguintes demandas de trabalho:

a) **Análise de Impacto de Negócio (BIA)**: Mapear quais processos da SECONT são vitais e qual o impacto de sua indisponibilidade.

b) **Atualização da Política de *Backup* e Replicação**: Implementação de estratégias imutáveis (proteção contra *Ransomware*) e armazenamento distribuído.

c) **Simulados de Crise**: Realização de testes controlados de interrupção de serviços para validar a eficácia dos planos de recuperação.

d) **Modernização da Infraestrutura**: Expansão do uso de arquitetura híbrida para garantir que serviços essenciais possuam redundância automática.

A partir das demandas de trabalho definidas, os seguintes objetivos e resultados chave foram estabelecidos:

Objetivos	Resultados
O1: Estabelecer a base de inteligência sobre a criticidade operacional da SECONT para direcionar com precisão os investimentos em resiliência e continuidade.	**KR1: Abrangência.** Até março de 2027, mapear 80% dos processos das áreas finalísticas e suas dependências diretas de ativos (software e hardware). **KR2: Parâmetros de Recuperação.** Até junho de 2027, definir os índices de RTO (*Recovery Time Objective*) e RPO (*Recovery Point Objective*) para cada um dos ativos identificados como vitais. **KR3: Alinhamento de Negócio.** Até agosto de 2027, obter a validação formal da matriz de prioridade de recuperação por 100% dos gestores das subsecretarias envolvidas. **KR4: Documentação Estratégica.** Até outubro de 2027, consolidar o relatório final da BIA 2026/2027, integrando os resultados como requisito obrigatório para o Plano de Recuperação de Desastres da Secretaria.

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

Objetivos	Resultados
O2: Consolidar uma infraestrutura tecnológica resiliente, garantindo a integridade dos dados institucionais contra desastres críticos.	**KR1: Imutabilidade.** Até dezembro de 2027, implementar tecnologia de armazenamento imutável (WORM - *Write Once, Read Many*) para 100% dos backups críticos. **KR2: Distribuição Geográfica.** Até dezembro de 2027, garantir que 100% das cópias de segurança possuam redundância em local geograficamente distinto (Site Secundário ou solução de Multi-Cloud), seguindo a regra 3-2-1 de backup. **KR3: Conformidade Normativa.** Até dezembro de 2027, desenvolver, publicar e treinar a equipe técnica do órgão na Normativa Interna de Backup e Replicação, alinhada às normas ISO/IEC 27001 e 27002. **KR4: Eficiência de Recuperação.** Até dezembro de 2027, validar através de testes de estresse, que o tempo de recuperação (RTO) de um ambiente seja inferior a 12 horas.
O3: Validar a prontidão e a eficácia da resposta a incidentes críticos, transformando os planos de continuidade de documentos estáticos em capacidades operacionais comprovadas.	**KR1: Testes e Simulações.** Até dezembro de 2027, definir as bases para a construção de um teste simulado para validação da resposta a incidentes, alternando entre cenários de falha total do Data Center e indisponibilidade de Cloud. **KR2: Previsibilidade das Ações.** Até dezembro de 2027, garantir que 100% dos serviços críticos testados sejam restaurados dentro dos limites de RTO (*Recovery Time Objective*) estabelecidos na BIA (*Business Impact Analysis*). **KR3: Pós-Crise.** Até dezembro de 2027, publicar o Relatório de Lições Aprendidas (*After Action Report*) em até 5 dias úteis após cada exercício, com 100% das falhas identificadas convertidas em chamados de melhoria. **KR4: Documentação.** Até março de 2028 documentar todos os procedimentos e definições criadas.

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

Objetivos	Resultados
O4: Consolidar uma infraestrutura de TIC de alta disponibilidade e performance, utilizando a agilidade da nuvem pública e a segurança do ambiente privado do Data Center governamental para tornar os serviços da SECONT resilientes.	**KR1: Disponibilidade Ativa.** Até dezembro de 2027, implementar arquitetura de redundância geográfica (*Hybrid Cloud*) para 100% dos serviços críticos elegíveis identificados na BIA (*Business Impact Analysis*). **KR2: Automação de Recuperação.** Até março de 2028, configurar mecanismos de *failover* automáticos que garantam o restabelecimento dos serviços essenciais elegíveis em até 5 minutos em caso de queda do provedor principal.

5. REFERENCIAL ESTRATÉGICO DA TIC.

O Referencial Estratégico de Tecnologia da Informação e Comunicação (TIC) constitui o alicerce sobre o qual se assentam as decisões tecnológicas e os investimentos da Secretaria de Estado de Controle e Transparência (SECONT) para o biênio 2026/2027. Este capítulo define as diretrizes que orientam a atuação da TIC, garantindo que cada iniciativa tecnológica esteja intrinsecamente conectada à missão institucional de promover a integridade, a eficiência da gestão pública e o controle social.

Para este ciclo, a estratégia de TIC da SECONT transcende o suporte operacional, posicionando-se como um agente transformador e estratégico. O foco reside na modernização da infraestrutura de dados, no fortalecimento da segurança da informação e na entrega de serviços digitais que ampliem a transparência governamental e a agilidade nas atividades de controle interno.

A construção deste referencial baseia-se no alinhamento vertical com o Planejamento Estratégico Institucional e as diretrizes de governo. Para assegurar a execução e o monitoramento contínuo das metas estabelecidas, a SECONT adota o framework de Objetivos e Resultados-Chave (OKRs). Esta abordagem permite uma gestão ágil e orientada a resultados, facilitando adaptações rápidas diante de novos desafios tecnológicos ou mudanças no cenário da administração pública.

Dessa forma, os elementos descritos a seguir — Missão, Visão e Valores — não são meras declarações formais, mas sim os vetores que garantem que a Tecnologia da Informação atue como o suporte essencial para uma gestão tática mais alinhada aos objetivos institucionais.

MISSÃO	**Prover e manter soluções tecnológicas com eficiência e segurança para sustentar as ações da SECONT.**
VISÃO	**Ser reconhecido como um setor essencial que apoia a SECONT no cumprimento da sua missão**
VALORES	**Transparência** **Ética** **Comprometimento** **Profissionalismo** **Conhecimento** **Qualidade** **Tempestividade** **Inovação** **Segurança**

Figura 1 - Referencial estratégico de TIC.

5.1. Análise SWOT.

A expressão **SWOT** é uma abreviação das palavras em inglês ***s**trengths*, ***w**eaknesses*, ***o**pportunities* e ***t**hreats*, que significam **forças**, **fraquezas**, **oportunidades** e **ameaças**, respectivamente. Trata-se de uma ferramenta utilizada para fazer análises de cenário ou ambiente, sendo usada como base para o planejamento e gestão de uma instituição.

Ambiente Interno	**FORÇAS (S)** ▪ Dedicação, formação e disponibilidade das equipes técnicas. ▪ Ambiente operacional estável e bem gerenciado. ▪ Disponibilidade de recursos financeiros para melhoria e ampliação dos serviços e equipamentos de TIC. ▪ Apoio técnico do PRODEST na solução de problemas e nas definições dos serviços. ▪ Disponibilidade de recursos técnicos no PRODEST para utilização nos projetos de TIC da SECONT.	**FRAQUEZAS (W)** ▪ A TIC ainda é vista como um apêndice operacional e não como um ativo estratégico. ▪ Baixo engajamento dos usuários nos processos de inovação. ▪ Pouca compreensão dos processos de gestão de TIC por parte da alta direção e da equipe gerencial. ▪ Pouco interesse em atualizações e inovações tecnológicas por parte dos usuários. ▪ Pouca compreensão da importância dos processos de segurança da informação por parte dos usuários e da alta direção. ▪ Processos operacionais não mapeados e não padronizados adequadamente. ▪ Visão excessivamente reativa por parte da alta direção do órgão.
Ambiente Externo	**OPORTUNIDADES (O)** ▪ Possibilidade de absorção de novas tecnologias por parte das equipes técnicas em treinamentos presenciais e remotos. ▪ Melhoria na qualificação dos servidores através de especializações específicas na área de atuação. ▪ Possibilidade de parcerias com outros órgãos públicos para troca de informações e experiências.	**AMEAÇAS (T)** ▪ Contingenciamento de recursos financeiros destinados aos projetos de TIC planejados. ▪ Perda de servidores qualificados atraídos por outras oportunidades de trabalho. ▪ Mudanças nas estratégias e políticas governamentais com descontinuidade de projetos. ▪ Vazamentos de informação, indisponibilidade de serviços provocado por *malwares* e ataques. ▪ Indisponibilidade provocada por falhas na infraestrutura física e lógica do ambiente de trabalho.

Tabela 1 - Matriz SWOT do ambiente de TIC da SECONT.

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

5.2. Fatores Críticos de Sucesso.

Os fatores levantados como críticos para o efetivo sucesso na execução e consequente alcance dos resultados previstos neste PDTIC são:

- ✓ Participação ativa do Comitê de Tecnologia na discussão, análise das necessidades, priorização dos projetos, bem como avaliação e monitoramento do PDTIC.
- ✓ Apoio e compromisso da alta direção, dos gestores e demais servidores da SECONT na execução do PDTIC.
- ✓ TODOS os projetos relacionados à TIC estarem alinhados ao PDTIC.
- ✓ Composição de um quadro de competências de TIC com as especialidades necessárias para atender às ações e aos projetos definidos no PDTIC.
- ✓ Disponibilidade de recursos humanos, orçamentários e financeiros para a execução das ações e dos projetos do PDTIC.

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

6. CONSIDERAÇÕES FINAIS E CONCLUSÃO.

A elaboração deste Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) para o biênio 2026/2027 representa um marco estratégico para a Secretaria de Estado de Controle e Transparência (SECONT). Mais do que um inventário de necessidades técnicas, este documento consolida a visão de que a TIC é o sistema nervoso central das atividades de controle, auditoria e transparência pública no Estado do Espírito Santo.

Ao longo deste planejamento, priorizou-se o alinhamento entre as demandas tecnológicas e os objetivos finalísticos da instituição, garantindo que cada investimento e esforço técnico contribua diretamente para uma gestão pública mais ética e eficiente.

6.1. Viabilização e Gestão por Resultados.

O sucesso deste PDTIC reside na transição do planejamento para a execução. Para tanto, a adoção do *framework* de Objetivos e Resultados-Chave (OKRs) será o diferencial competitivo desta gestão. Os OKRs permitirão:

- **Monitoramento Dinâmico**: Revisões periódicas que evitam o distanciamento entre a estratégia e a operação.
- **Foco e Priorização**: Concentração de esforços naquilo que realmente move os indicadores de resultados.
- **Engajamento de Equipes**: Uma linguagem comum que conecta o trabalho técnico dos analistas e auditores de TI aos impactos para o negócio.

6.2. Desafios e Próximos Passos.

O horizonte 2026/2027 apresenta desafios significativos, especialmente no que tange à segurança cibernética, à governança de dados e à integração de sistemas de inteligência aplicada ao controle interno. No entanto, as diretrizes aqui estabelecidas fornecem a segurança necessária para que a SECONT navegue por essas transformações com resiliência e inovação.

Em suma, este PDTIC reafirma o compromisso da SECONT com a excelência na governança de TIC. Ao concluir este ciclo de planejamento, a Secretaria posiciona-se de forma robusta para enfrentar as demandas do próximo biênio, assegurando que a transparência e o controle social sejam potencializados por uma infraestrutura tecnológica moderna, segura e, acima de tudo, estratégica.

APÊNDICE A – ESTIMATIVA DO PORTFÓLIO ORÇAMENTÁRIO.

Tema	Objetivos	Investimento Previsto
Tema 1: Ampliação e universalização do uso da Inteligência Artificial Generativa	**01**: Transformar o Google Gemini no assistente onipresente da SECONT, automatizando tarefas burocráticas e elevando a qualidade técnica da produção documental.	**R$ 320.000,00**
	02: Promover o letramento em IA e a especialização técnica por meio de um programa de capacitação corporativa, visando transformar a SECONT em um ambiente de trabalho onde os servidores sejam capazes de utilizar, de forma ética e eficiente, ferramentas de IA generativa para otimizar suas entregas.	**R$ 140.000,00**
	03: Potencializar a eficiência operacional da SUBINT, SUBTRAN e CORREGEDORIA mediante o desenvolvimento e integração de agentes de IA customizados.	**R$ 90.000,00**

Investimento previsto para o tema no período (abril de 2026 a abril de 2028): R$ 550.000,00

Tema	Objetivos	Investimento Previsto
Tema 2: Nuvem pública e serviços online –Transformação cultural e operacional	**01**: Modernizar o ambiente de colaboração para potencializar a produtividade.	**R$ 0,00** (Investimento previsto no Tema 1 – 01)
	02: Fomentar a cultura digital e o uso pleno das ferramentas de nuvem.	**R$ 180.000,00**
	03: Estabelecer um ambiente de nuvem pública seguro.	**R$ 0,00** (Investimento previsto no Tema 1 – 01)

Investimento previsto para o tema no período (abril de 2026 a abril de 2028): R$ 180.000,00

Tema	Objetivos	Investimento Previsto
Tema 3: Automação, desenvolvimento de software e serviços de dados	**01**: Estabelecer uma infraestrutura de nuvem resiliente para a publicação de aplicações, garantindo autonomia operacional e agilidade no ciclo de vida das aplicações da SECONT	**R$ 0,00** (Provido pelo PRODEST)
	02: Elevar a maturidade técnica da equipe interna e assegurar a alta performance do ambiente Red Hat, transformando o conhecimento especializado em autonomia operacional para a SECONT	**R$ 180.000,00**
	03: Transformar a capacidade produtiva de software da SECONT em um ativo estratégico de alta agilidade, internalizando a inteligência de negócio e eliminando barreiras burocráticas entre a TIC e as áreas finalísticas.	**R$ 3.200.00,00**
	04: Consolidar o SIAC como o coração tecnológico e a fonte única de verdade para as atividades de controle, eliminando a fragmentação operacional e garantindo a integridade absoluta dos dados da SECONT.	**R$ 1.600.00,00**
	05: Estabelecer uma infraestrutura de dados de alto desempenho, transformando grandes volumes de informações em ativos estratégicos para controle e tomada de decisão.	**R$ 0,00** (Desenvolvimento próprio)
	06: Estabelecer e consolidar os serviços de dados da SECONT.	**R$ 3.000.000,00**

Investimento previsto para o tema no período (abril de 2026 a abril de 2028): R$ 7.980.000,00

Tema	Objetivos	Investimento Previsto
Tema 4: Segurança da Informação	**01**: Estabelecer uma infraestrutura de governança e proteção de dados resiliente, garantindo que os ativos da SECONT estejam mapeados, normatizados e protegidos contra ameaças emergentes.	**R$ 0,00** (Desenvolvimento próprio)
	02: Reduzir a incerteza tecnológica e estabelecer uma visão clara do apetite a risco e da capacidade de resposta da SECONT ante ameaças críticas.	**R$ 0,00** (Desenvolvimento próprio)
	03: Liderar a transformação digital no controle público com o uso ético e seguro da Inteligência Artificial, assegurando a confiabilidade das soluções e a proteção do patrimônio informacional.	**R$ 0,00** (Desenvolvimento próprio)
	04: Fortalecer a cultura de resiliência digital da SECONT, assegurando que o fator humano e os processos institucionais estejam em total conformidade com os padrões de segurança e privacidade.	**R$ 0,00** (Desenvolvimento próprio)

Investimento previsto para o tema no período (abril de 2026 a abril de 2028): R$ 0,00

Tema	Objetivos	Investimento Previsto
Tema 5: Garantia de Continuidade do Negócio	**01**: Estabelecer a base de inteligência sobre a criticidade operacional da SECONT para direcionar com precisão os investimentos em resiliência e continuidade.	**R$ 0,00** (Desenvolvimento próprio)
	02: Consolidar uma infraestrutura tecnológica resiliente, garantindo a integridade dos dados institucionais contra desastres críticos	**R$ 240.000,00**
	03: Validar a prontidão e a eficácia da resposta a incidentes críticos, transformando os planos de continuidade de documentos estáticos em capacidades operacionais comprovadas	**R$ 0,00** (Desenvolvimento próprio)
	04: Consolidar uma infraestrutura de TIC de alta disponibilidade e performance, utilizando a agilidade da nuvem pública e a segurança do ambiente privado do Data Center governamental para tornar os serviços da SECONT resilientes.	**R$ 0,00** (Desenvolvimento próprio)

Investimento previsto para o tema no período (abril de 2026 a abril de 2028): R$ 240.000,00

Total de investimento previsto no período deste PDTIC (2026/2027):

R$ 8.950.000,00

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

APÊNDICE B – CRONOGRAMA PREVISTO.

Tema	Objetivos	Resultados	1º Semestre Abr/26 a Set/26	2º Semestre Out/26 a Mar/27	3º Semestre Abr/27 a Set/27	4º Semestre Out/27 a Mar/28
Tema 1: Ampliação e universalização do uso da Inteligência Artificial Generativa	**01**: Transformar o Google Gemini no assistente onipresente da SECONT.	**KR1**: Alcançar 80% de usuários ativos mensais até dezembro de 2026.				
		KR2: Até junho de 2027 reduzir em 50% o tempo de redação e revisão de documentos, validado por amostragem de produtividade nas subsecretarias.				
		KR3: Até dezembro de 2026 implementar 15 "Prompts Corporativos Padrão" integrados ao fluxo de trabalho.				
	02: Promover a especialização técnica por meio de um programa de capacitação corporativa.	**KR1**: Até dezembro de 2026, alcançar 80% de usuários capacitados na utilização adequada do Google Gemini.				
	03: Potencializar a eficiência operacional da SUBINT, SUBTRAN e CORREGEDORIA mediante o desenvolvimento e integração de agentes de IA customizados.	**KR1**: Até dezembro de 2026, disponibilizar um agente de IA conversacional para interagir com a base documental da SUBINT.				
		KR2: Até dezembro de 2026, disponibilizar um agente de IA conversacional para interagir com a base documental da CORREGEDORIA.				
		KR3: Até março de 2027, disponibilizar um agente de IA conversacional para interagir com a base de dados do sistema E-OUV e disponibilizá-lo aos gestores da rede de Ouvidorias.				

Tema	Objetivos	Resultados	1º Semestre Abr/26 a Set/26	2º Semestre Out/26 a Mar/27	3º Semestre Abr/27 a Set/27	4º Semestre Out/27 a Mar/28
Tema 2: Nuvem pública e serviços online. Transformação cultural e operacional	**01**: Modernizar o ambiente de colaboração para potencializar a produtividade.	**KR1**: Até dezembro de 2026 deve ser feita a criação de 100% das identidades corporativas da SECONT no Workspace.				
		KR2: Migração de 100% das contas de e-mail e agenda (Zimbra) para o Google Workspace até março de 2027				
		KR3: Migração de 100% dos serviços de do Zoom para o serviço Meet do Google Workspace até março de 2027.				
		KR4: Até dezembro de 2026 devem ser criados os ambientes para armazenamento no Google Drive.				
	02: Fomentar a cultura digital e o uso pleno das ferramentas de nuvem.	**KR1**: Capacitar 80% dos usuários na utilização dos recursos do Google Workspace até março de 2027.				
		KR2: Alcançar 80% dos usuários usando os recursos colaborativos do Google Workspace até julho de 2027.				
	03: Estabelecer um ambiente de nuvem seguro.	**KR1**: Proteger 100% dos dados críticos com políticas de DLP (Data Loss Prevention) até julho de 2027.				
		KR2: Alcançar 100% de aplicação da autenticação multifator (MFA) nas contas de usuários até julho de 2027.				

Tema	Objetivos	Resultados	1º Semestre Abr/26 a Set/26	2º Semestre Out/26 a Mar/27	3º Semestre Abr/27 a Set/27	4º Semestre Out/27 a Mar/28
Tema 3: Automação, desenvolvimento de software e serviços de dados	**01**: Estabelecer infraestrutura resiliente para a publicação de aplicações.	**KR1**: Concluir a instância exclusiva do OpenShift no PRODEST até julho de 2026.				
		KR2: Migrar 100% das aplicações em produção para o novo ambiente até dezembro de 2026.				
		KR3: Implementar 100% das esteiras de CI/CD automatizadas (GitLab) até dezembro de 2026.				
		KR4: Alcançar 100% de cobertura de observabilidade até dezembro de 2026.				
	02: Elevar a maturidade técnica da equipe interna.	**KR1**: Concluir O processo de adesão à ARP Red Hat do PRODEST até julho de 2026.				
		KR2: Capacitar servidores técnicos no Red Hat OpenShift até dezembro de 2026.				
		KR3: Até julho de 2027, executar 80% das horas de consultoria técnica previstas.				
		KR4: Até julho de 2027, reduzir em 50% a dependência de chamados externos ao PRODEST.				
	03: Transformar a capacidade produtiva de software da SECONT.	**KR1**: Concluir processo licitatório para contratação da equipe de desenvolvedores até agosto de 2026.				
		KR2: Repassar 100% das atividades executadas para a nova equipe de desenvolvedores até março de 2027.				
		KR3: Reduzir em 50% o tempo de entrega e homologação no SIAC até dezembro de 2027.				
	04: Consolidar o SIAC como o coração tecnológico e a fonte única de verdade para as atividades de controle.	**KR1**: Até abril de 2027, concluir 100% dos módulos do SIAC previstos no escopo do programa PROFISCO II.				
		KR2: Integração do legado. Integrar 50% dos sistemas legados ao SIAC até dezembro de 2027.				
		KR3: Até julho de 2027, documentar 100% dos módulos do SIAC previstos no escopo do programa PROFISCO II.				
		KR4: Até dezembro de 2026, produzir os requisitos dos módulos do Gabinete e de Outras Ações de Controle.				
	05: Estabelecer infraestrutura de dados de alto desempenho.	**KR1**: Atualizar Apache Spark, JupyterHub e Apache Airflow até dezembro de 2026.				
		KR2: Implementar e homologar o Trino como motor de consulta distribuída até dezembro de 2026.				
		KR3: Até março de 2027, implementar e homologar o Apache Iceberg como suporte a ACID no MinIO.				
		KR4: Até março de 2027, implementar e homologar o Project Nessie e o GitLab.				
		KR5: Até dezembro de 2027, implementar e homologar o Prometheus e Grafana.				
	06: Estabelecer os serviços de dados previstos.	**KR1**: Até dezembro de 2026 entregar e homologar os serviços de dados previstos pela 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

Tema	Objetivos	Resultados	1º Semestre Abr/26 a Set/26	2º Semestre Out/26 a Mar/27	3º Semestre Abr/27 a Set/27	4º Semestre Out/27 a Mar/28
Tema 4: Segurança da Informação	**01**: Estabelecer uma gestão da segurança da informação adequada.	**KR1**: Desenvolver, publicar e disseminar a nova PSI, o controles e o SGSI até julho de 2027.				
		KR2: Concluir o mapeamento e a classificação de criticidade de 100% dos ativos até julho de 2027.				
	02: Estabelecer infraestrutura de governança e proteção de dados resiliente.	**KR1**: Instituir 04 Normas Complementares fundamentais até julho de 2027.				
		KR2: Até dezembro de 2027, implementar o fluxo de Gestão de Vulnerabilidades.				
	03: Reduzir a incerteza tecnológica.	**KR1**: Até dezembro de 2027, mapear e quantificar o impacto institucional todas as vulnerabilidades críticas.				
		KR2: Até dezembro de 2027, aprovar o Plano de Tratamento de Riscos (PTR) com estratégias de resposta.				
	04: Liderar a transformação digital no uso ético e seguro da Inteligência Artificial.	**KR1**: Até julho de 2027, instituir o Sistema de Gestão de IA (SGIA) conforme a norma ISO/IEC 42001.				
		KR2: Até dezembro de 2027, implementar camadas de proteção e filtragem para IA.				
		KR3: Até dezembro de 2027, realizar a Avaliação de Impacto Algorítmico (AIA) em 100% das soluções de IA.				
	05: Fortalecer a cultura de resiliência digital da SECONT.	**KR1**: Até dezembro de 2027, reduzir a taxa de sucesso de ataques de phishing para menos de 5%.				
		KR2: A partir de julho de 2027 e até dezembro de 2027, realizar 01 ciclo de Auditoria Interna de Segurança.				

Tema	Objetivos	Resultados	1º Semestre Abr/26 a Set/26	2º Semestre Out/26 a Mar/27	3º Semestre Abr/27 a Set/27	4º Semestre Out/27 a Mar/28
Tema 5: Garantia de Continuidade do Negócio	**01**: Estabelecer a base de inteligência sobre a criticidade operacional da SECONT.	**KR1**: Até março de 2027, mapear 80% dos processos das áreas finalísticas e suas dependências diretas de ativos (software e hardware).				
		KR2: Até junho de 2027, definir os índices de RTO e RPO para ativos considerados vitais.				
		KR3: Até agosto de 2027, obter a validação formal da matriz de prioridade de recuperação.				
		KR4: Até outubro de 2027, consolidar o relatório final da BIA 2026/2027, integrando os resultados.				
	02: Consolidar infraestrutura tecnológica resiliente, garantindo a integridade dos dados contra desastres críticos.	**KR1**: Até dezembro de 2027, implementar tecnologia de armazenamento imutável.				
		KR2: Até dezembro de 2027, garantir que 100% das cópias de segurança possuam redundância.				
		KR3: Até dezembro de 2027, desenvolver e treinar a equipe do órgão na Normativa Interna de Backup.				
		KR4: Até dezembro de 2027, validar se o tempo de recuperação (RTO) dos ambientes seja inferior a 12 horas.				

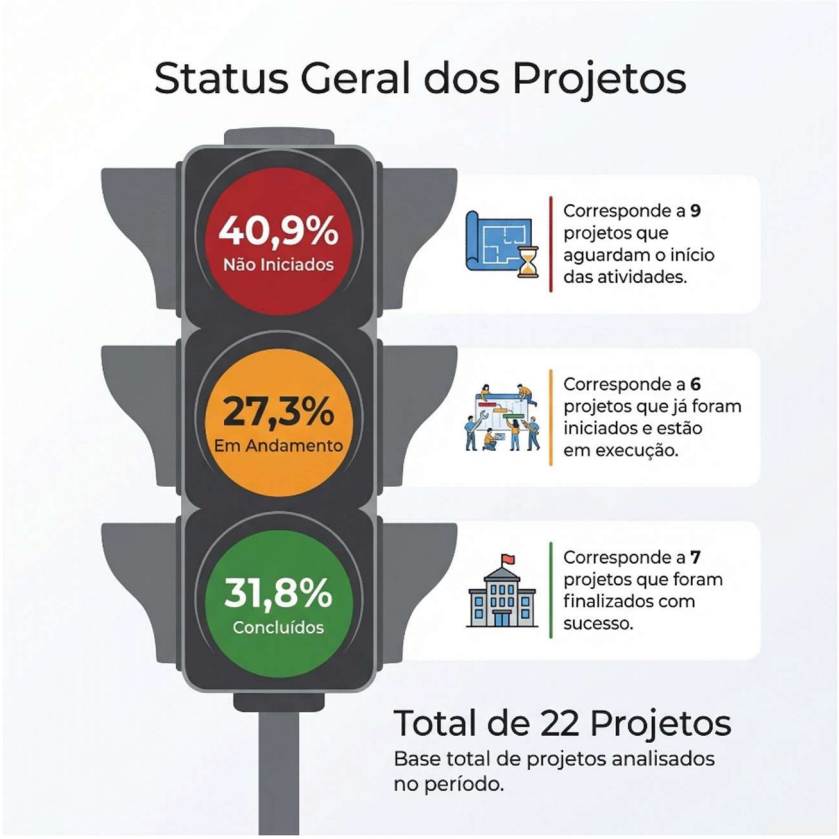
Av. João Batista Parra, 600 – Edifício Aureliano Hoffman – 10° Andar
Enseada do Suá – Vitória – Espírito Santo – CEP 29.050-375
Telefones (27) 3636-5369 – (27) 3636-0700

Tema	Objetivos	Resultados	1º Semestre Abr/26 a Set/26	2º Semestre Out/26 a Mar/27	3º Semestre Abr/27 a Set/27	4º Semestre Out/27 a Mar/28
Tema 5: Garantia de Continuidade do Negócio	**03**: Validar a prontidão e a eficácia da resposta a incidentes críticos.	**KR1**: Até dezembro de 2027, definir as bases para a construção de um teste para validação da resposta a incidentes.				
		KR2: Até dezembro de 2027, garantir que 100% dos serviços críticos testados sejam restaurados dentro dos limites.				
		KR3: Até dezembro de 2027, publicar o Relatório de Lições Aprendidas (After Action Report) em até 5 dias úteis				
		KR4: Até março de 2028 documentar todos os procedimentos e definições criadas.				
	04: Consolidar infraestrutura de TIC de alta disponibilidade e performance.	**KR1**: Até dezembro de 2027, implementar arquitetura de redundância geográfica (Hybrid Cloud).				
		KR2: Até março de 2028, configurar failover automático que garanta o restabelecimento dos serviços.				

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

APÊNDICE C – PRESTAÇÃO DE CONTAS DO PDTIC ANTERIOR.

O ciclo anterior do PDTIC da SECONT (2024/2025) não adotou o *framework* de gestão por **Objetivos e Resultados Chave** (**OKR**). Desta forma, a prestação de contas foi realizada com base nos projetos lançados.



Projeto	Forma de Execução	Responsável	Prazo Previsto	Situação
Desenvolvimento do módulo "3ª Linha" do sistema SIAC	Contrato CAST	SUBCONT	Fevereiro 2025	**Não concluído.** Projeto em finalização e remanejado para o PDTIC 2026/2027.
Desenvolvimento do Conselho de Usuários de Serviços Públicos	Contrato CAST	SUBTRAN	Outubro 2024	**Concluído.**
Desenvolvimento do módulo "Integridade" do sistema SIAC	Contrato CAST	SUBINT	Março 2026	**Não concluído.** Projeto iniciado e remanejado para o PDTIC 2026/2027.
Desenvolvimento do módulo "2ª Linha" do sistema SIAC	Contrato CAST	SUBCONT	Dezembro 2025	**Não concluído.** Projeto iniciado e remanejado para o PDTIC 2026/2027.
Desenvolvimento e implantação do SisPMPI e Portal PMPI	Contrato CAST	SUBINT	Março 2026	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.
Módulo "Gabinete" do sistema SIAC	Contrato CAST	GABINETE	Março 2026	**Não iniciado.** Projeto não iniciado, mas remanejado para o PDTIC 2026/2027.

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

Projeto	Forma de Execução	Responsável	Prazo Previsto	Situação
Análise e detecção de fraudes (Hunter)	Contrato VERT	SUBINT / CIED	Abril 2025	**Não concluído.** Projeto iniciado e remanejado para o PDTIC 2026/2027.
Painel de Obras Públicas	Contrato VERT	SUBCONT / CIED	Agosto 2025	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.
Automação dos Pontos de Controle da PCA	Contrato VERT	SUBCONT / CIED	Dezembro 2025	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.
Construção do Sistema de Desenvolvimento Profissional – 1ª versão	GTIC	SUBCONT	Abril 2024	**Concluído.**
Construção do Data Stack SECONT – 1ª versão	GTIC	CIED	Maio 2024	**Concluído.**
Sistema para Distribuição de processos CONSECOR.	GTIC	GABINETE	Julho 2024	**Concluído.**
Aquisição da solução para acompanhamento da implantação dos planos de integridade	GTIC	SUBINT	Julho 2024	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.
Aquisição de desktops, notebooks e workstations	GTIC	GTIC	Setembro 2024	**Concluído.**
Contratação técnicos de TI.	GTIC	GTIC	Novembro 2025	**Concluído.**
Apoio na implantação do sistema e-PAD.	GTIC	COGES	Dezembro 2024	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.
Solução para elevar a maturidade dos dados abertos do Portal da Transparência	SUBTRAN	SUBTRAN	Julho 2024	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.
Solução para facilitar e ampliar a compreensão das informações do Portal da Transparência	SUBTRAN	SUBTRAN	Outubro 2024	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.
Serviços para adequação operacional da SECONT à LGPD	SUBTRAN	SUBTRAN	Outubro 2024	**Não concluído.** Projeto em finalização, mas não remanejado para o PDTIC 2026/2027.
Aquisição de ferramenta de gestão de endpoints.	GTIC	GTIC	Junho 2025	**Concluído.**
Implantação da Recuperação de Desastres e da Resposta a Incidentes	GTIC	GTIC	Junho 2025	**Não concluído.** Projeto iniciado e remanejado para o PDTIC 2026/2027.
Adaptação do Portal dos Conselhos.	GTIC	SUBTRAN	Novembro 2024	**Não iniciado.** Projeto não iniciado e não relacionado no PDTIC 2026/2027.

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

Documento original assinado eletronicamente, conforme MP 2200-2/2001, art. 10, § 2º, por:

EMERSON COUTO DE MOURA
GERENTE QCE-03
GTIC - SECONT - GOVES
assinado em 30/03/2026 10:44:21 -03:00

INFORMAÇÕES DO DOCUMENTO
Documento capturado em 30/03/2026 10:44:21 (HORÁRIO DE BRASÍLIA - UTC-3)
por EMERSON COUTO DE MOURA (GERENTE QCE-03 - GTIC - SECONT - GOVES)
Valor Legal: ORIGINAL | Natureza: DOCUMENTO NATO-DIGITAL

A disponibilidade do documento pode ser conferida pelo link: https://e-docs.es.gov.br/d/2026-93NCGZ