ESTUDO TÉCNICO PRELIMINAR (ETP)

				Número do Processo - SISLOG ***117548***
				Número do Processo - SEI ***202500005038178***

001 - INTRODUÇÃO

Em conformidade com a Lei federal nº 14.133, de 01 de abril de 2021 e com o Decreto estadual n° 10.207, de 27 de janeiro de 2023, o Estudo Técnico Preliminar - ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação a fim de atender a uma necessidade administrativa, e tem por objetivo subsidiar a elaboração do Anteprojeto, Termo de Referência ou Projeto Básico, bem como do edital de licitação e da minuta contratual, quando aplicável.

Informamos que esta contratação sucede e substitui a Contratação 107135, de mesmo objeto, a qual por motivos técnicos não logrou sucesso na sessão do Pregão Eletrônico nº 79/22025.

Tópico 1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. O presente Estudo Técnico Preliminar apresenta os estudos técnicos realizados visando identificar e analisar as soluções disponíveis no mercado, em termos de requisitos, alternativas e justificativas para escolha da melhor solução para alcançar os resultados pretendidos.

1.2. Assim, a delimitação da solução nos termos e condições estipulados não é decisão de livre arbítrio desta equipe. Aqui estão pautados elementos que, fundamentadamente, têm a capacidade e potencial para, em tese, considerando o caso concreto, melhor atender ao interesse público.

1.3. Previsão no Plano de Contratações Anual:

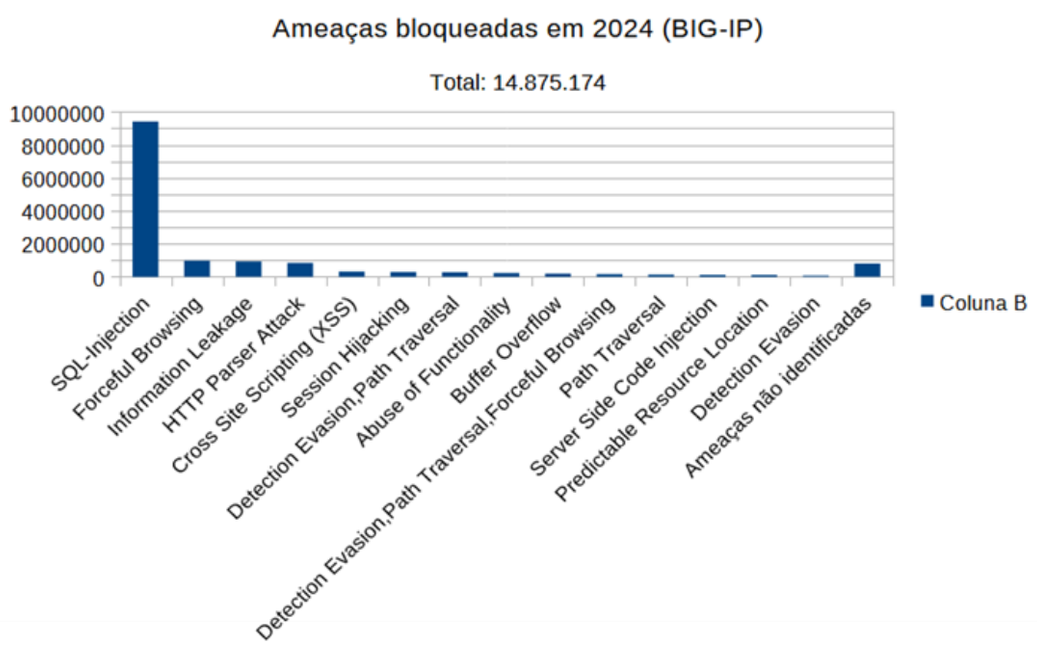
1.3.1. Esta contratação está incluida no planejamento efetuado pra inclusão no Plano Anual de Contratações quando formalizado.

1.4. Alinhamento Estratégico:

1.4.1. Esta pretendida contratação apresenta conformidade com os Programas e Ações do PPA 2024-2027 relacionados às atribuições desta Pasta, em conformidade com as suas competências, nos termos da Lei nº 22.317, 18 de outubro de 2023.

1.5. IDENTIFICAÇÃO DA DEMANDA OU DO PROBLEMA A SER SOLUCIONADO:

1.5.1. A Secretaria-Geral de Governo (SGG) enfrenta um cenário desafiador devido à ausência de um Sistema de Gestão de Segurança da Informação (SGSI) estruturado, o que pode comprometer a proteção de seus dados e sistemas diante do aumento exponencial de ameaças cibernéticas. Em 2024, os mecanismos de defesa existentes, como o firewall de borda, registraram mais de 14,8 milhões de tentativas de ataques, muitos deles focados em manipular informações por meio de técnicas como *SQL-Injection* ou obter acessos privilegiados, conforme gráfico abaixo:



Fonte: Dados do Firewall de borda, 2025.

1.5.1.1. A presente contratação está em consonância com o regime jurídico de responsabilidade previsto no art. 117 da Lei nº 14.133/2021, conforme estabelece a disposição normativa constante do do art. 7º do Decreto Estadual nº 10.680/2025, *in verbis:*

> ***Art. 7º.*** *Poderá ser objeto da contratação de terceiros a* ***prestação de serviços técnicos*** *para a realização de estudos, planejamentos, pareceres, perícias e* ***consultorias e para a avaliação da qualidade dos serviços de TIC****, desde que isso ocorra mediante a supervisão e a gestão do contrato realizadas por servidores do órgão ou da entidade da administração pública estadual, nos termos do art. 117 da Lei nº 14.133/2021****.*** *(destaque nosso)*

1.5.2. Além disso, entre agosto de 2024 e fevereiro de 2025, o software de proteção instalado nos computadores da rede local identificou e neutralizou mais de 1,2 milhão de incidentes, evidenciando a intensidade e a persistência das ameaças, conforme imagem abaixo:

Fonte: Dados do *Sentinel One*, 2025.

1.5.3. Esse contexto demonstra a necessidade urgente de uma abordagem mais robusta e sistemática para a segurança da informação, como a preconizada pela ISO/IEC 27005:2022, que oferece uma metodologia estruturada para o mapeamento e gerenciamento de riscos. Diferentemente das soluções isoladas atualmente em uso, como antivírus e *firewalls,* o mapeamento de riscos baseado nessa norma permite identificar vulnerabilidades de forma proativa, avaliar os impactos potenciais de incidentes e priorizar ações para mitigar ameaças. Isso é essencial em um ambiente onde os ataques estão cada vez mais sofisticados, explorando falhas em softwares desatualizados, configurações inadequadas e até mesmo comportamentos internos que podem expor a organização.

1.5.4. A ISO/IEC 27005:2022 (ISO 27005) é uma norma internacional que orienta a gestão de riscos de segurança da informação. Ela é aplicável a todas as organizações, independentemente do seu tamanho ou setor, fornecendo diretrizes para identificar, analisar, avaliar, tratar e monitorar riscos de segurança da informação. Entre seus principais objetivos, estão:

1.5.5. Identificar as necessidades da organização em relação aos requisitos de segurança da informação.

1.5.6. Criar um sistema de gerenciamento de segurança da informação eficaz.

1.5.7. Implementar a segurança da informação com base em uma abordagem de gerenciamento de risco.

1.5.8. Proteger os ativos de informação.

1.5.9. Atender aos requisitos da ISO/IEC 27001.

1.5.10. Sem uma gestão de riscos bem definida, a SGG/GO permanece suscetível a consequências graves, como o vazamento de dados sensíveis, a interrupção de serviços essenciais e a não conformidade com regulamentações de proteção de dados, o que pode gerar prejuízos financeiros e reputacionais. O mapeamento de riscos conforme a ISO/IEC 27005:2022 proporciona uma visão clara do ambiente de TI, permitindo a implementação de controles específicos para garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações. Além disso, ele suporta a integração de medidas de segurança em todas as plataformas utilizadas, independentemente do sistema operacional, atendendo à diversidade tecnológica da organização.

1.5.11. A justificativa para adotar essa abordagem está no fato de que as ameaças cibernéticas não apenas evoluem rapidamente, mas também se adaptam às defesas existentes, exigindo uma resposta dinâmica e contínua. Com o mapeamento de riscos, a SGG/GO pode antecipar cenários adversos, fortalecer sua resiliência e assegurar a proteção de seus ativos de informação, alinhando-se às melhores práticas internacionais e às demandas de um ambiente digital em constante transformação. A implementação dessa estratégia, apoiada por serviços especializados, é um passo fundamental para reduzir a exposição a ataques e garantir a continuidade das operações de forma segura e eficiente.

1.5.12. A importância do mapeamento de riscos baseado na ISO/IEC 27005:2022 também reside na capacidade de estabelecer uma governança sólida sobre a segurança da informação, algo que vai além da mera aplicação de tecnologias. Ele permite à SGG/GO criar um inventário detalhado de seus ativos digitais, compreender os processos críticos que dependem dessas informações e mapear as interdependências entre sistemas. Essa visão holística é indispensável para que a organização consiga alocar recursos de maneira estratégica, concentrando esforços nas áreas de maior vulnerabilidade e evitando desperdícios com medidas genéricas que não atendem às necessidades específicas do ambiente.

1.5.13. Outro aspecto crucial é a possibilidade de promover uma cultura de segurança dentro da instituição. O mapeamento de riscos não se limita a aspectos técnicos; ele também envolve a sensibilização dos colaboradores sobre os perigos de ações como o uso de senhas fracas ou o clique em links suspeitos, que frequentemente abrem brechas para ataques. Ao integrar essa metodologia, a SGG/GO pode capacitar sua equipe para reconhecer e reportar potenciais ameaças, transformando o fator humano de um ponto fraco em um elemento ativo de defesa, o que é especialmente relevante em um contexto de aumento de ataques de engenharia social.

1.5.14. Por fim, o mapeamento de riscos oferece uma base para a melhoria contínua, um princípio central da ISO/IEC 27005:2022. Ele não é um processo estático, mas sim um ciclo que permite à SGG/GO monitorar mudanças no cenário de ameaças, ajustar suas defesas conforme novas tecnologias são adotadas e responder rapidamente a incidentes emergentes. Essa adaptabilidade é vital em um órgão governamental, onde a confiança pública depende da capacidade de proteger informações sensíveis e manter serviços funcionando sem interrupções. Assim, investir nessa abordagem é tanto uma medida de proteção quanto um compromisso com a eficiência e a

responsabilidade no uso dos recursos públicos.

Tópico 2 - DESCRIÇÃO DA SOLUÇÃO

Definição da solução escolhida

2.1. Abaixo segue a descrição resumida do objeto a ser contratado, definido após a realização de estudo técnico preliminar: **Prestação de Serviços - Contratação de Consultoria de Risco em TI**

Tópico 2 - DESCRIÇÃO DA SOLUÇÃO

2.1. Definição da Solução

2.1.1. Abaixo segue a descrição resumida do objeto a ser contratado, definido após a realização de estudo técnico preliminar: **Prestação de Serviços - Contratação de Consultoria de Risco em TI.**

2.1.2. O objeto desta contratação é a prestação de serviços de consultoria em segurança de Tecnologia da Informação e Comunicação (TIC) para realização de um mapeamento de riscos de segurança da informação, com base na norma ISO/IEC 27005:2022.

2.1.2.1. O objeto da contratação é classificado como **serviço comum**, por apresentar, independentemente de sua complexidade, padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

2.1.2.2. Além disso, conforme exposto na justificativa da contratação, o objeto apresenta características técnicas e de qualidade passíveis de descrição clara e objetiva, com base em padrões amplamente consolidados, cujo mercado domina as técnicas de sua realização, de modo a permitir uma oferta segura em face das exigências previstas no edital. Há no setor inúmeras empresas e profissionais aptos a executar o serviço nos parâmetros definidos no edital, cuja execução não envolve tecnologias ou métodos complexos, tampouco exige soluções inovadoras ou desenvolvimento de projetos especiais.

2.1.3. A pretensão contratual envolve a realização de procedimento licitatório regular para a seleção de empresa especializada na prestação de serviços de consultoria em segurança de Tecnologia da Informação e Comunicação (TIC) para a execução de um mapeamento de riscos de segurança da informação, com base na norma ISO/IEC 27005:2022, atendendo às demandas da Gerência de Cibersegurança da Secretaria-Geral de Governo (GECIBER/SGG), de acordo com as especificações constantes neste Documento.

2.1.4. Metodologia de Trabalho: o mapeamento de riscos deverá ser conduzido em conformidade com as diretrizes da norma ISO/IEC 27005:2022, reconhecida como referência para a identificação, análise e avaliação de riscos de segurança da informação, alinhando-se às necessidades específicas da SGG/GO e considerando o contexto de ameaças cibernéticas identificadas no ambiente organizacional.

2.1.5. O escopo da consultoria deve abranger

2.1.5.1. Análise do cenário atual de segurança da informação na Subsecretaria de Tecnologia da Informação da SGG/GO, identificando ativos críticos, ameaças e vulnerabilidades existentes e propondo recomendações preliminares para adequação às práticas da ISO/IEC 27005:2022;

2.1.5.2. Definição de diretrizes iniciais para o planejamento de controles de segurança com base nos resultados do mapeamento;

2.1.5.3. Identificação, análise e avaliação de riscos de segurança da informação, com elaboração de matrizes detalhadas;

2.1.5.4. Documentação estruturada dos resultados e recomendações para subsidiar decisões estratégicas futuras;

2.1.5.5. A CONTRATADA deverá, para a realização do mapeamento de riscos, observar as etapas e entregas definidas neste documento, vinculadas às práticas recomendadas pela ISO/IEC 27005:2022, garantindo a precisão e a aplicabilidade dos resultados ao contexto da Secretaria.

2.1.5.6. Toda a documentação elaborada pela CONTRATADA deverá ser entregue ao CONTRATANTE em formato eletrônico editável, enviada ao endereço eletrônico da Secretaria a ser informado na reunião inicial do projeto.

2.1.6. Detalhamento das etapas a resultados:

2.1.6.1. Etapa 1 – Planejamento do Projeto:

2.1.6.1.1. Esta etapa consiste na estruturação do plano de trabalho, da Estrutura Analítica do Projeto (EAP) e na definição de um cronograma detalhado para a execução das atividades previstas neste Termo de Referência, alinhado às metodologias da ISO 27005:2022.

2.1.6.1.2. Entregas obrigatórias:

a. Plano de trabalho do projeto;

b. Estrutura Analítica do projeto;

c. Cronograma detalhado das atividades.

2.1.6.2. Etapa 2 – Diagnóstico do Cenário Atual:

2.1.6.2.1. Compreende a análise inicial do ambiente de TI da Subsecretaria de Tecnologia da Informação da SGG/GO, incluindo o levantamento preliminar de ativos de informação, o exame das práticas de segurança existentes e a identificação de lacunas em relação às diretrizes da ISO/IEC 27005:2022.

2.1.6.2.2. Entregas obrigatórias:

a. Relatório de análise do contexto atual de segurança da informação;

b. Inventário preliminar de ativos de informação;

c. Relatório de identificação de lacunas frente à ISO/IEC 27005:2022.

2.1.6.3. Etapa 3 – Identificação e Classificação de Ativos:

2.1.6.3.1. Envolve a identificação detalhada dos ativos de informação da SGG/GO, sua classificação com base em critérios de confidencialidade, integridade, disponibilidade e autenticidade, e o mapeamento de suas interdependências, conforme orientações da ISO/IEC 27005:2022.

2.1.6.3.2. Entregas obrigatórias

a. Inventário completo de ativos de informação;

b. Relatório de classificação dos ativos e suas interdependências;

c. Documento preliminar com recomendações para proteção dos ativos identificados.

2.1.6.4. Etapa 4 – Análise e Avaliação de Riscos

2.1.6.4.1. A CONTRATADA deverá realizar a análise de ameaças e vulnerabilidades, avaliar os impactos potenciais e elaborar uma matriz de riscos, utilizando a metodologia da ISO/IEC 27005:2022 adaptada ao contexto da Subsecretaria de Tecnologia da Informação da SGG/GO.

2.1.6.4.2 Entregas obrigatórias

a. Matriz de ameaças e vulnerabilidades;

b. Relatório de avaliação de impactos;

c. Matriz consolidada de riscos com priorização;

d. Recomendações iniciais para tratamento de riscos.

2.1.6.5. Etapa 5 – Documentação e Recomendações

2.1.6.5.1. Consiste na consolidação dos resultados do mapeamento em relatórios estruturados e na proposição de recomendações práticas para controles futuros, alinhadas às necessidades da Subsecretaria de Tecnologia da Informação da SGG/GO e às diretrizes da ISO/IEC 27005:2022.

2.1.6.5.2 Entregas obrigatórias

a. Relatório final do mapeamento de riscos;

b. Documento de recomendações para controles de segurança;

c. Guia de uso dos resultados para planejamento estratégico.

2.1.6.6. Etapa 6 – Validação e Encerramento:

2.1.6.6.1. Esta etapa envolve a revisão final dos resultados do mapeamento, a validação da qualidade das entregas e o encerramento do projeto com a apresentação de um relatório consolidado.

2.1.6.6.2. Entregas obrigatórias:

a. Relatório de validação dos resultados;

b. Documento final consolidado do mapeamento;

c. Declaração de conclusão do serviço.

2.2. IDENTIFICAÇÃO DE POSSÍVEIS SOLUÇÕES CAPAZES DE ATENDER A NECESSIDADE:

2.2.1. A pesquisa de mercado foi realizada com o objetivo de identificar as melhores opções para realizar o trabalho necessário, sem deixar de garantir a disponibilidade dos serviços de TIC, otimizando o desempenho dos processos organizacionais e oferecendo suporte adequado à infraestrutura e ao portfólio de serviços de TI da Secretaria-Geral de Governo, com ênfase na segurança da informação. O mercado de TIC oferece uma ampla variedade de empresas que fornecem esses serviços, o que pode tornar a escolha desafiadora, já que a seleção deve considerar tanto as configurações mínimas exigidas pela demanda quanto o custo competitivo das soluções.

2.2.2. Para realizar esse levantamento, foram consultados contratos válidos de órgãos públicos nos portais **http://paineldeprecos.planejamento.gov.br/**, **https://www.comprasgovernamentais.gov.br/** e **https://www.bancodeprecos.com.br/**, além de diversas pesquisas complementares na internet.

2.2.3. Com base nas alternativas disponíveis no mercado, a equipe do projeto buscou identificar soluções que atendessem às necessidades específicas da Secretaria-Geral de Governo, levando em consideração a experiência necessária para adequada condução do projeto, sem que haja qualquer impacto na infraestrutura tecnológica necessária para suportar a continuidade dos serviços prestados pela instituição e, principalmente, garantindo a segurança da informação.

2.2.4. A pesquisa considerou diferentes fornecedores e soluções que asseguram a proteção e a eficiência dos serviços de TI, alinhando-se ao mapeamento de riscos e controles estabelecido pela ISO/IEC 27005:2022, para garantir que as práticas de governança e segurança estejam adequadamente implementadas. A diversidade de soluções disponíveis foi analisada, destacando-se a importância de atender às exigências mínimas de configuração, adequação ao orçamento e ao cumprimento das diretrizes legais e regulamentares que regem o setor público.

2.3. IDENTIFICAÇÃO DAS SOLUÇÕES

2.3.1. Foram identificadas 3 (três) possíveis soluções para o mapeamento de riscos da SGG/GO, com base na ISO/IEC 27005:2022, conforme relacionadas a seguir:

ID	Descrição da Solução (ou cenário)
1	Contratação de consultoria especializada para prestação do serviço
2	Realização da prestação de serviço pela equipe
3	Realização de parcerias com outros órgãos públicos para realização da prestação de serviço

2.3.2. Diante da inexistência de registros de contratações similares na administração pública que permitissem uma comparação objetiva e adequada, tornou-se imprescindível a realização de pesquisa direta com fornecedores. Para identificar fornecedores aptos à execução do serviço, foi conduzida uma busca estruturada na internet, por meio do Google, utilizando termos específicos relacionados ao objeto. A partir dessa pesquisa, foram mapeadas empresas com atuação comprovada no setor, cujos portfólios de serviços, disponibilizados em seus sites institucionais, foram analisados para verificar a aderência ao escopo da contratação.

2.3.3. Com base nessa triagem, foram solicitadas cotações formais às empresas identificadas como tecnicamente qualificadas, conforme apontado no "orçamento estimado", as quais subsidiaram a definição do valor estimado da contratação.

2.3.4. Entre os principais fatores que justificam a adoção dessa metodologia, destacam-se:

- **Ausência de contratações públicas similares:** A consulta a bases como o Banco de Preços, o Portal Nacional de Contratações Públicas (PNCP) e outras fontes governamentais não identificou registros com escopo técnico e metodológico equivalente, inviabilizando a adoção de preços de referência oriundos de aquisições públicas anteriores.
- **Impossibilidade de padronização:** Os serviços de consultoria em gestão de riscos são fortemente dependentes do contexto organizacional do contratante. A natureza personalizada dessas soluções, que variam conforme o porte institucional, o setor de atuação, os ativos críticos e o grau de maturidade em segurança da informação, impacta diretamente na formação de preços e nos itens entregáveis.

2.4. Solução 01: Contratação de Consultoria Especializada para o Mapeamento de Segurança da Informação com Base na ISO/IEC 27005:2022

2.4.1. A contratação de uma consultoria especializada é uma solução passível de ser considerada quando voltada para a realização de um mapeamento detalhado dos processos de segurança da informação com base nas diretrizes da ISO/IEC 27005:2022. Essa abordagem envolve profissionais experientes que conduzem a identificação de ativos de informação, a análise de ameaças e vulnerabilidades, a avaliação de impactos e a documentação estruturada das informações relevantes para a proteção dos dados e sistemas da Secretaria-Geral de Governo (SGG/GO). A consultoria proporciona expertise para aplicar as práticas recomendadas pela ISO/IEC 27005:2022, adaptando o mapeamento às necessidades específicas da organização e garantindo uma visão clara do cenário de segurança.

2.4.2. Uma das principais vantagens dessa solução é o domínio técnico que a consultoria oferece no uso da ISO/IEC 27005:2022. Profissionais especializados possuem experiência na execução de mapeamentos abrangentes, identificando de forma precisa os elementos críticos que precisam ser protegidos e os pontos de exposição que podem comprometer a segurança da informação. Eles estão familiarizados com as metodologias mais recentes e conseguem estruturar um mapeamento que seja ao mesmo tempo detalhado e prático, proporcionando à Secretaria uma base sólida para decisões futuras relacionadas à segurança.

2.4.3. A rapidez na realização do mapeamento é outro benefício significativo. Por contarem com processos bem definidos e experiência prévia, os consultores conseguem executar o mapeamento em um prazo mais curto do que uma equipe interna sem expertise equivalente, evitando atrasos e permitindo que a Secretaria obtenha rapidamente uma visão consolidada de sua segurança da informação. Além disso, a consultoria pode oferecer suporte adicional na interpretação dos resultados do mapeamento, ajudando a organização a priorizar ações com base nas descobertas realizadas.

2.4.4. Outro aspecto positivo é a possibilidade de capacitação da equipe interna durante o processo. Ao longo do mapeamento, os consultores podem compartilhar conhecimentos práticos sobre a aplicação da ISO/IEC 27005:2022, permitindo que os colaboradores da Secretaria compreendam melhor as técnicas utilizadas e estejam preparados para realizar atualizações ou novos mapeamentos no futuro. Isso promove uma maior autonomia organizacional e reduz a necessidade de intervenções externas contínuas.

2.4.5. Por outro lado, a contratação de uma consultoria especializada pode apresentar algumas desvantagens, como o custo elevado, que pode ser um fator limitante dependendo do orçamento disponível para a Secretaria. Além disso, a dependência inicial de um parceiro externo para a realização do mapeamento pode gerar desafios, especialmente se a equipe interna não for devidamente envolvida ou capacitada para dar continuidade ao trabalho. Também é importante considerar que a aplicação da ISO/IEC 27005:2022 pode demandar adaptações às particularidades da organização, e a falta de alinhamento entre a consultoria e a equipe interna pode dificultar a efetividade do mapeamento.

2.5. Vantagens:

2.5.1. Conhecimento especializado na ISO/IEC 27005:2022 A consultoria possui expertise na aplicação das diretrizes da norma, garantindo um mapeamento detalhado e alinhado às melhores práticas internacionais.

2.5.2. Execução eficiente e ágil: Profissionais experientes conseguem realizar o mapeamento em menos tempo, entregando resultados

úteis em prazos reduzidos.

2.5.3. Documentação estruturada e clara: O mapeamento conduzido pela consultoria resulta em relatórios organizados, que facilitam a compreensão e a tomada de decisão pela Secretaria.

2.5.4. Visão abrangente da segurança da informação: A abordagem da ISO/IEC 27005:2022, aplicada pela consultoria, assegura que todos os aspectos relevantes sejam considerados, proporcionando uma visão completa do cenário de segurança.

2.5.5. Adaptabilidade às necessidades específicas: A consultoria pode personalizar o mapeamento para atender às particularidades da Secretaria, tornando os resultados mais aplicáveis ao contexto organizacional.

2.5.6. Base sólida para planejamento: O mapeamento fornece informações fundamentais que podem orientar estratégias futuras de proteção da informação.

2.6. Desvantagens:

2.6.1. Custo elevado: A contratação de consultores especializados pode envolver um investimento significativo, dependendo da complexidade e da duração do projeto.

2.6.2. Dependência inicial de terceiros: A Secretaria pode ficar dependente da consultoria para a realização inicial do mapeamento, caso a equipe interna não seja suficientemente capacitada.

2.6.3. Desafios de alinhamento: Diferenças entre a abordagem da consultoria e a cultura organizacional da Secretaria podem dificultar a aplicação prática dos resultados do mapeamento.

2.7. Solução 02: Realização do Mapeamento de Segurança da Informação pela Equipe Interna com Base na ISO/IEC 27005:2022

2.7.1. A segunda solução propõe que a Secretaria-Geral de Governo assuma total responsabilidade pelo mapeamento de segurança da informação utilizando sua própria equipe interna, com base nas diretrizes da ISO/IEC 27005:2022. Essa abordagem envolve a execução de todas as etapas do mapeamento — como a identificação de ativos de informação, análise de ameaças e vulnerabilidades, e documentação dos resultados — sem a intervenção de consultores externos. A equipe interna seria responsável por estruturar o processo, aplicar as práticas recomendadas pela norma e garantir que os dados coletados reflitam o cenário de segurança da organização.

2.7.2. Uma das vantagens dessa solução é o controle que a Secretaria teria sobre o processo de mapeamento. A equipe interna, por conhecer as operações e particularidades da organização, pode adaptar o mapeamento às suas necessidades específicas e priorizar os aspectos mais relevantes para o contexto local. Isso elimina a dependência de terceiros e permite que a Secretaria conduza o trabalho conforme suas prioridades, ajustando o ritmo conforme necessário.

2.7.3. Outro benefício é o potencial desenvolvimento de competências internas. Ao realizar o mapeamento com base na ISO/IEC 27005:2022, a equipe interna pode adquirir conhecimentos sobre as práticas recomendadas pela norma, o que pode ser útil em outras iniciativas relacionadas à segurança da informação. Esse aprendizado pode fortalecer a capacidade da Secretaria de conduzir futuros mapeamentos ou análises semelhantes, reduzindo a necessidade de intervenções externas a longo prazo.

2.7.4. No entanto, essa solução apresenta desvantagens significativas que podem comprometer sua eficácia. Primeiramente, a equipe interna frequentemente carece do nível de experiência técnica necessário para aplicar a ISO/IEC 27005:2022 de forma eficiente. O mapeamento de segurança da informação envolve metodologias complexas que exigem familiaridade com conceitos específicos e práticas detalhadas, e a falta de expertise pode levar a erros graves, como a identificação incompleta de ativos ou a subestimação de ameaças críticas, resultando em um mapeamento superficial ou impreciso.

2.7.5. Além disso, a sobrecarga de trabalho é um obstáculo considerável. Os colaboradores da Secretaria geralmente já possuem outras responsabilidades operacionais, e realizar um mapeamento detalhado com base na ISO/IEC 27005:2022 exige tempo, dedicação exclusiva e atenção a detalhes. Essa sobrecarga pode não apenas comprometer a qualidade do trabalho, mas também levar a atrasos significativos na conclusão do mapeamento, atrasando decisões importantes relacionadas à segurança da informação.

2.7.6. Outro ponto crítico é a ausência de uma perspectiva externa, o que pode limitar severamente a capacidade da equipe interna de identificar lacunas ou pontos de vulnerabilidade mais amplos. Sem a visão imparcial de especialistas externos, a equipe pode ficar restrita a uma visão interna limitada, ignorando ameaças emergentes ou práticas mais atualizadas que não fazem parte de sua experiência cotidiana. Isso aumenta o risco de que o mapeamento não contemple todos os aspectos relevantes, deixando a organização exposta a riscos não identificados.

2.7.7. Por fim, a falta de acesso a ferramentas avançadas e a experiência prática em lidar com metodologias específicas da ISO/IEC 27005:2022 pode resultar em um processo demorado e ineficiente. A equipe interna pode enfrentar dificuldades em interpretar corretamente os requisitos da norma, levando a inconsistências nos resultados ou a necessidade de retrabalho, o que eleva os custos indiretos e compromete o cronograma planejado.

2.8. Vantagens:

2.8.1. Controle sobre o processo: A Secretaria pode conduzir o mapeamento conforme suas prioridades e necessidades específicas, sem interferências externas.

2.8.2. Aproveitamento do conhecimento interno: A equipe interna, por conhecer o funcionamento da organização, pode realizar um mapeamento mais alinhado ao contexto local.

2.8.3. Redução de custos diretos com consultoria: Ao evitar a contratação de consultores externos, a Secretaria economiza recursos financeiros imediatos.

2.8.4. Desenvolvimento de competências internas: O processo proporciona aprendizado para os colaboradores, que podem aplicar os conhecimentos adquiridos em outras atividades de segurança da informação.

2.8.5. Flexibilidade no cronograma: A Secretaria pode ajustar o ritmo do mapeamento conforme sua disponibilidade, sem estar vinculada a prazos externos.

2.9. Desvantagens:

2.9.1. Falta de experiência técnica: A equipe interna geralmente não possui o nível necessário de especialização para aplicar a IISO/IEC 27005:2022 de forma eficiente, o que pode levar a erros graves, como a identificação incompleta de ameaças ou ativos, comprometendo a qualidade do mapeamento.

2.9.2. Sobrecarga de trabalho significativa: As responsabilidades adicionais do mapeamento podem sobrecarregar os colaboradores, impactando outras atividades essenciais e resultando em falhas ou atrasos no processo.

2.9.3. Ausência de visão externa crítica: Sem a perspectiva de especialistas externos, a equipe interna pode falhar em identificar vulnerabilidades ou ameaças importantes, aumentando os riscos para a organização.

2.9.4. Processo lento e ineficiente: A falta de familiaridade com a ISO/IEC 27005:2022 pode prolongar o tempo necessário para o mapeamento, atrasando a obtenção de resultados úteis e gerando retrabalho.

2.9.5. Risco de inconsistências graves: A aplicação inadequada da norma pode resultar em dados imprecisos ou incompletos, tornando o mapeamento pouco confiável para decisões estratégicas.

2.9.6. Limitação no acesso a práticas atualizadas: A equipe interna pode não estar ciente das práticas mais recentes do mercado, o que compromete a relevância e a abrangência do mapeamento.

2.9.7. Necessidade de capacitação intensiva: Para alcançar um nível mínimo de proficiência, a equipe interna pode demandar treinamentos extensos, o que implica custos adicionais e maior tempo de preparação, anulando parte das economias iniciais.

2.10. Solução 03: Realização de Parcerias com Outros Órgãos Públicos para o Mapeamento de Segurança da Informação com Base na ISO/IEC 27005:2022

2.10.1. A terceira solução propõe que a Secretaria-Geral de Governo estabeleça parcerias com outros órgãos públicos que já tenham experiência na aplicação da ISO/IEC 27005:2022 para a realização de mapeamentos de segurança da informação. Por meio dessa colaboração, a Secretaria poderia compartilhar de metodologias, ferramentas e práticas previamente estabelecidas, com o objetivo de otimizar custos e esforços. A ideia é aproveitar a experiência de outros órgãos para conduzir o mapeamento, adaptando os resultados às especificidades da Secretaria.

2.10.2. Uma das vantagens dessa solução é a possibilidade de redução de custos. Ao compartilhar recursos, como ferramentas de análise e metodologias já testadas, com outros órgãos públicos, a Secretaria pode minimizar os gastos operacionais. Não seria necessário investir pesadamente em treinamentos ou ferramentas específicas, já que os parceiros poderiam fornecer orientações e materiais prontos para uso. Além disso, a parceria oferece a oportunidade de aprender com práticas já consolidadas, o que pode facilitar o entendimento inicial da ISO/IEC 27005:2022 e agilizar algumas etapas do mapeamento.

2.10.3. A troca de conhecimento entre os órgãos também é um benefício relevante. A colaboração permite que a Secretaria aprenda com as experiências de outros entes públicos, identificando abordagens eficazes e evitando erros comuns no uso da ISO/IEC 27005:2022. Essa troca de experiências pode enriquecer o processo e ajudar a Secretaria a compreender melhor os desafios e soluções associados ao mapeamento de segurança da informação, promovendo um aprendizado conjunto que pode ser útil no futuro.

2.10.4. Entretanto, essa solução apresenta desvantagens significativas que podem comprometer sua viabilidade. A integração de práticas e metodologias entre diferentes órgãos pode ser um processo extremamente complexo e demorado. As abordagens e ferramentas utilizadas pelos parceiros podem não ser totalmente compatíveis com as necessidades ou a estrutura da Secretaria, resultando em dificuldades técnicas e atrasos consideráveis na execução do mapeamento. Isso pode gerar frustrações e exigir ajustes constantes, prolongando o tempo necessário para obter resultados úteis.

2.10.5. Outro ponto crítico é a dependência de outros órgãos para a realização do mapeamento. A Secretaria ficaria vulnerável às prioridades, limitações e possíveis instabilidades dos parceiros, o que pode impactar diretamente o progresso do trabalho. Caso um órgão parceiro enfrente dificuldades internas ou não consiga atender às expectativas, a Secretaria pode acabar com um mapeamento incompleto ou inadequado, comprometendo a segurança da informação.

2.10.6. Além disso, a falta de personalização é uma barreira significativa. As soluções e práticas adotadas por outros órgãos podem não atender às especificidades da Secretaria, resultando em um mapeamento genérico que não reflete as reais necessidades ou vulnerabilidades da organização. Isso pode levar a decisões mal fundamentadas e a uma proteção insuficiente contra ameaças específicas ao contexto da Secretaria.

2.10.7. Por fim, a colaboração entre diferentes órgãos pode gerar problemas de governança e comunicação. Divergências em prioridades, processos e até mesmo na interpretação da ISO/IEC 27005:2022 podem dificultar o alinhamento, criando lacunas no mapeamento e aumentando os riscos de falhas. A comunicação ineficiente entre as partes pode ainda resultar em atrasos adicionais ou na perda de informações críticas, tornando o processo menos confiável e mais suscetível a erros.

2.11. Vantagens:

2.11.1. Redução de custos iniciais: O compartilhamento de metodologias e ferramentas com outros órgãos pode minimizar os gastos com treinamentos ou aquisição de recursos específicos.

2.11.2. Aproveitamento de práticas existentes: A parceria permite aprender com experiências já consolidadas, o que pode facilitar a aplicação inicial da ISO/IEC 27005:2022.

2.11.3. Troca de conhecimento: A colaboração possibilita o aprendizado mútuo, ajudando a Secretaria a compreender melhor os desafios e soluções relacionados ao mapeamento.

2.11.14. Alinhamento com o setor público: A parceria pode garantir que o mapeamento siga diretrizes amplamente aceitas no setor

público, promovendo uma maior conformidade com práticas comuns.

2.12. Desvantagens:

2.12.1. Integração altamente complexa e demorada: A harmonização de práticas e ferramentas entre diferentes órgãos pode ser tecnicamente desafiadora e prolongada, gerando atrasos significativos no mapeamento.

2.12.2. Dependência crítica de outros órgãos: A Secretaria fica à mercê das prioridades e limitações dos parceiros, correndo o risco de interrupções ou inconsistências no processo caso os órgãos enfrentem dificuldades internas.

2.12.3. Falta de personalização adequada: As práticas adotadas por outros órgãos podem ser genéricas e não atender às necessidades específicas da Secretaria, resultando em um mapeamento pouco útil para o contexto local.

2.12.4. Desafios severos de governança: A gestão compartilhada pode levar a conflitos de prioridades e processos, dificultando o alinhamento e comprometendo a qualidade do mapeamento.

2.12.5. Riscos de falhas na comunicação: A falta de coordenação eficiente entre os órgãos pode gerar lacunas no mapeamento, perda de informações críticas e aumento de vulnerabilidades não identificadas.

2.12.6. Possível inconsistência na aplicação da ISO/IEC 27005:2022: Diferenças na interpretação da norma entre os órgãos podem levar a um mapeamento incoerente, com resultados pouco confiáveis para a Secretaria.

2.12.7. Demora excessiva na obtenção de resultados: O processo de adaptação a um modelo colaborativo pode ser tão prolongado que compromete a capacidade da Secretaria de agir rapidamente com base nos dados do mapeamento.

2.13. ANÁLISE DE SOLUÇÕES E ESCOLHA DA SOLUÇÃO MAIS ADEQUADA:

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução está disponível no Portal do *Software* Público Brasileiro?	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é composta por software livre ou software público?	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo *ePing*, *eMag*, *ePWG*?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da *ICP*-Brasil?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-*ARQ* Brasil?	Solução 1			X
	Solução 2			X
	Solução 3			X

2.14. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

2.14.1. A solução de tecnologia da informação indicada neste planejamento visa a realização de um mapeamento completo de segurança da informação para a Secretaria-Geral de Governo, com base nas diretrizes da ISO/IEC 27005:2022, com o objetivo de identificar e documentar ativos, ameaças, vulnerabilidades e impactos associados, garantindo uma base sólida para a proteção, confidencialidade, integridade e disponibilidade das informações processadas e armazenadas pela Secretaria, conforme as necessidades do objeto deste estudo.

2.14.2. A contratação envolverá a execução de um mapeamento estruturado, fundamentado nas boas práticas e metodologias da ISO/IEC 27005:2022, de forma a assegurar que todos os aspectos relevantes da segurança da informação sejam analisados de maneira eficaz e sistemática. A solução incluirá, entre outros, a identificação detalhada de ativos de informação, análise de ameaças e vulnerabilidades, avaliação de impactos, documentação dos resultados e recomendações para controles, além da capacitação dos colaboradores da Secretaria para uso futuro das informações geradas.

2.15. Bens e serviços que compõem a solução

2.15.1. A solução contratada compreenderá os seguintes componentes:

2.15.2. Realização do mapeamento com base na ISO/IEC 27005:2022: A equipe contratada será responsável pela análise do cenário atual da Secretaria-Geral de Governo, ou de outras secretarias parceiras quando necessário, para elaboração de um plano detalhado para o mapeamento de segurança da informação, identificação dos ativos críticos, análise de ameaças e vulnerabilidades, e avaliação de impactos potenciais. Isso incluirá a aplicação das metodologias da ISO/IEC 27005:2022 para estruturar o processo, bem como a geração de relatórios detalhados que orientem a Secretaria na priorização de ações para proteção da informação.

2.15.3. Serviços de consultoria técnica especializada: Profissionais qualificados fornecerão suporte especializado durante todo o processo de mapeamento, garantindo que a aplicação da ISO/IEC 27005:2022 seja feita de forma precisa e alinhada às especificidades da Secretaria. A consultoria cobrirá todas as etapas, desde o levantamento inicial até a entrega dos resultados finais, com foco na identificação de lacunas e na proposição de recomendações práticas para fortalecer a segurança da informação. A equipe consultiva também auxiliará na interpretação dos dados coletados, assegurando que os resultados sejam úteis para decisões estratégicas.

2.15.4. Documentação e relatórios: O mapeamento realizado resultará na entrega de toda a documentação necessária, incluindo relatórios detalhados com os resultados do levantamento, matrizes de ameaças e vulnerabilidades, avaliações de impacto, recomendações de controles e guias para uso futuro. Essa documentação será organizada de acordo com as melhores práticas daISO/IEC 27005:2022 e entregue em formato acessível à equipe de TI da Secretaria, garantindo que todas as informações estejam disponíveis para consulta e aplicação prática ao longo do tempo.

2.16. Regime de fornecimento:

2.16.1. Tendo em vista a necessidade de fornecimento dos documentos, conforme cada etapa da consultoria em momentos distintos, considera-se que a entrega será prestada de forma parcelada.

2.17. Justificativa da escolha da solução:

2.17.1. A crescente digitalização das operações e a dependência de tecnologias da informação tornam a segurança da informação uma prioridade estratégica para a Secretaria-Geral de Governo (SGG/GO). A proteção adequada dos ativos digitais, incluindo dados sensíveis e processos operacionais, é essencial para garantir a continuidade dos serviços públicos e a confiança da sociedade.

2.17.2. O mapeamento de segurança da informação, com base nas diretrizes da ISO/IEC 27005:2022, é um processo estruturado que permite à organização identificar ativos críticos, analisar ameaças e vulnerabilidades, avaliar impactos e estabelecer uma base sólida para a proteção dos dados. Esse mapeamento deve envolver todos aqueles que se relacionam direta ou indiretamente com a infraestrutura de TI da organização, como funcionários, prestadores de serviços, parceiros e terceirizados, e precisa contar com o aval da alta direção, bem como das demais áreas pertinentes, para assegurar sua legitimidade e alinhamento com as regulamentações aplicáveis.

2.17.3. Nesse contexto, a realização de um mapeamento estruturado, alinhado às melhores práticas da ISO/IEC 27005:2022, torna-se crucial. Esse processo oferece uma abordagem sistemática para compreender o cenário de segurança da informação, permitindo à SGG/GO identificar lacunas, priorizar ações e planejar controles de forma fundamentada, garantindo a confidencialidade, integridade e disponibilidade dos dados, além de facilitar a conformidade com as regulamentações vigentes.

2.17.4. Rememora-se que a sigla ISO significa *International Organization for Standardization* (Organização Internacional de Padronização, em português). A ISO é uma organização fundada em 1946, com sede em Genebra (Suíça), formada por representantes de 91 países, com o objetivo de promover o desenvolvimento de normas que impulsionem o comércio de bens e serviços, melhorando a qualidade e a padronização de produtos e processos. No Brasil, é representada pela Associação Brasileira de Normas Técnicas (ABNT).

2.17.5. A ISO/IEC 27005:2022 é uma norma internacional que fornece diretrizes para a gestão de riscos de segurança da informação, sendo amplamente reconhecida como referência para a realização de mapeamentos detalhados. Publicada pela ISO, ela tem como foco a identificação e análise de riscos, oferecendo uma metodologia estruturada para compreender ameaças, vulnerabilidades e impactos, de modo a proteger a confidencialidade, integridade e disponibilidade de dados essenciais às operações da organização.

2.17.6. A ISO/IEC 27005:2022 integra a série de normas ISO/IEC 27000, que inclui outras normas relacionadas, como a ISO/IEC 27001 (que define os requisitos para um Sistema de Gestão de Segurança da Informação) e a ISO/IEC 27002 (diretrizes para controles de segurança). Enquanto a ISO 27001 estabelece uma estrutura geral para a gestão da segurança da informação, a ISO/IEC 27005:2022 foca especificamente na análise de riscos de tecnologia da informação, sendo uma ferramenta essencial para o mapeamento inicial que orienta a implementação de controles eficazes.

2.17.7. Portanto, a realização de um mapeamento com base na ISO/IEC 27005:2022 é uma tarefa complexa, que exige um entendimento profundo de metodologias específicas, como a identificação de ativos, análise de ameaças e avaliação de impactos. A experiência prática na aplicação da norma é fundamental para garantir a qualidade e a precisão dos resultados, especialmente em um contexto onde a segurança da informação é dinâmica e constantemente desafiada por novas ameaças.

2.17.8. Por isso, a contratação de uma consultoria especializada (Solução 01) se torna a escolha mais adequada, pois proporciona acesso a profissionais com expertise comprovada, capazes de aplicar a ISO/IEC 27005:2022 de forma eficiente e adaptada às

necessidades específicas da SGG/GO. Esses especialistas podem garantir que o mapeamento seja conduzido com rigor técnico, utilizando ferramentas e metodologias avançadas, além de assegurar conformidade com outras normas da série ISO/IEC 27000 que complementam o processo, como a ISO/IEC 27002.

2.17.9. A contratação de uma consultoria especializada oferece diversos benefícios. Em primeiro lugar, ela proporciona um mapeamento detalhado do estado atual da segurança da informação na SGG/GO, permitindo identificar ativos críticos, ameaças e vulnerabilidades com maior precisão. Esse diagnóstico é fundamental para entender os pontos de exposição da infraestrutura de TI e orientar a implementação de controles futuros de maneira informada e estratégica.

2.17.10. Outro benefício significativo é a garantia de um processo estruturado e eficiente. A consultoria, com sua experiência, pode realizar o mapeamento em um prazo mais curto e com maior qualidade do que uma equipe interna (Solução 02) ou uma parceria com outros órgãos públicos (Solução 03), evitando os riscos de inconsistências, atrasos ou resultados genéricos que essas alternativas podem apresentar. A visão externa imparcial da consultoria também ajuda a identificar lacunas que podem passar despercebidas por equipes internas ou por parceiros com prioridades distintas.

2.17.11. Comparada às demais soluções, a Solução 01 (contratação de consultoria especializada) destaca-se como a mais vantajosa. A Solução 02 (equipe interna) enfrenta desafios como falta de experiência técnica, sobrecarga de trabalho e ausência de uma perspectiva externa, o que pode levar a erros, atrasos e resultados pouco confiáveis. Já a Solução 03 (parcerias com outros órgãos públicos) apresenta riscos de integração complexa, dependência de terceiros, falta de personalização e problemas de governança, comprometendo a eficácia e a rapidez do mapeamento. Em contrapartida, a Solução 01 oferece expertise técnica, eficiência, personalização e uma visão externa imparcial, garantindo um mapeamento robusto, preciso e adaptado às necessidades específicas da SGG/GO. Essa abordagem minimiza riscos, acelera o processo e fornece uma base sólida para decisões estratégicas relacionadas à segurança da informação, justificando sua escolha como a melhor opção para atender aos objetivos da Secretaria.

2.17.12. Portanto, a contratação de uma consultoria especializada é fundamental para a realização eficaz de um mapeamento de segurança da informação na SGG/GO. A experiência e o conhecimento técnico da consultoria permitirão à Secretaria obter resultados confiáveis, que orientem a proteção dos ativos digitais, minimizem vulnerabilidades e assegurem a continuidade dos serviços prestados à sociedade. Investir na Solução 01 representa não apenas um avanço significativo na compreensão do cenário de segurança da informação, mas também um passo estratégico para fortalecer a proteção dos dados e a conformidade com as melhores práticas internacionais e regulatórias.

2.18. Vigência do contrato:

2.18.1. O prazo de vigência do contrato é de 12 (doze) meses ou até a conclusão das 640 (seiscentos e quarenta) horas, considerando-se iniciada a vigência no dia da sua divulgação no Portal Nacional de Contratações Públicas (PNCP) e iniciando-se a contagem do prazo no dia subsequente, por força da aplicação combinada dos arts. 94, caput, e 183, caput, da Lei federal nº 14.133, de 1º de abril de 2021, nos termos da orientação referencial da Procuradoria-Geral do Estado exarada no Despacho nº 582/2025/GAB. Considerando que o objeto contratado é de natureza não continuada, o prazo de vigência será automaticamente prorrogado, independentemente de termo aditivo, quando o objeto não for concluído no período firmado acima, salvo quando a não conclusão decorrer de culpa da CONTRATADA, nos termos do arts. 6º, inciso XVII, e 111 da Lei federal nº 14.133, de 1º de abril de 2021**.**

Tópico 3 - ESTIMATIVA DA QUANTIDADE A SER CONTRATADA

3.1. Identificação dos itens, quantidades e unidades:

3.1.1. A estimativa da quantidade a ser contratada é justificada nos termos deste ETP, conforme disposto na Lei federal nº 14.133, de 01 de abril de 2021. A descrição com o respectivo quantitativo a ser contratado está apresentado abaixo.

3.1.2. A justificativa para as 640 horas de consultoria para a realização de um mapeamento de segurança da informação com base na ISO/IEC 27005:2022 pode ser detalhada da seguinte maneira:

3.1.3. Complexidade da Realização do Mapeamento com Base na ISO/IEC 27005:2022 A execução de um mapeamento de segurança da informação envolve diversas etapas técnicas complexas, que demandam experiência e especialização. O processo não se resume a uma simples coleta de dados, mas sim a uma série de ações que incluem o levantamento de ativos de informação, a identificação de ameaças e vulnerabilidades, a avaliação de impactos, a análise detalhada do cenário de riscos e a documentação estruturada dos resultados, conforme as diretrizes da ISO/IEC 27005:2022. Cada etapa requer aplicação rigorosa de metodologias específicas para garantir a precisão e a utilidade das informações geradas.

3.1.4. Consultoria Especializada para Adequação às Necessidades da SGG/GO A consultoria especializada será essencial para garantir que o mapeamento seja realizado de acordo com as particularidades da SGG/GO. O processo deve ser personalizado para atender às características operacionais e estruturais da organização, considerando sua infraestrutura de TI, políticas internas, eventuais necessidades de mapeamento em outras secretarias parceiras e contexto específico. Isso envolve uma análise aprofundada dos processos da Secretaria e a adaptação das práticas recomendadas pela ISO/IEC 27005:2022 para assegurar que os resultados sejam relevantes e aplicáveis à realidade da SGG/GO.

3.1.5. Criação de um Mapeamento Estruturado de Segurança da Informação: A criação de um mapeamento estruturado com base na ISO/IEC 27005:2022 é uma etapa fundamental, pois permite identificar, classificar e avaliar os elementos que impactam a segurança da informação dentro da organização. Esse processo envolve uma análise detalhada de ativos críticos, ameaças potenciais, vulnerabilidades existentes e impactos associados, proporcionando uma visão clara das áreas de maior exposição. Com o mapeamento, é possível tomar decisões mais assertivas sobre prioridades e controles futuros. A consultoria será responsável por liderar esse processo, aplicando as metodologias da ISO/IEC 27005:2022 e garantindo que todas as dimensões relevantes sejam devidamente documentadas e analisadas.

3.1.6. Gerenciamento de Mudanças e Avaliação de Resultados: A realização de um mapeamento detalhado pode implicar ajustes nos processos organizacionais ou na forma como a segurança da informação é percebida na SGG/GO, e a consultoria deve auxiliar na gestão dessas mudanças. As 640 horas de consultoria incluem o tempo necessário para avaliar a qualidade dos resultados obtidos, revisar os relatórios gerados e propor ajustes conforme necessário para garantir que o mapeamento atenda aos objetivos

estabelecidos. Isso assegura que as informações produzidas sejam práticas e úteis para orientar decisões futuras de proteção da informação na Secretaria.

3.1.2 Assim estimando-se o prazo de conclusão de cada etapa chegamos a quantidade de horas necessárias para este projeto

#	Etapa	Estimativa de horas
1	Planejamento do Projeto	1 semana de trabalho - 40 horas
2	Diagnóstico do Cenário Atual:	1 mês de trabalho - 160 horas
3	Identificação e Classificação de Ativos	2 semanas de trabalho - 80 horas
4	Gerenciamento de Mudanças e Avaliação de Resultados	1 mês de trabalho - 160 horas
5	Análise e Avaliação de Riscos	2 semanas de trabalho - 80 horas
6	Documentação e Recomendações	2 semanas de trabalho - 80 horas
7	Validação e Encerramento	1 semana de trabalho - 40 horas
	TOTAL	**640 Horas**

- Considerando 40 horas semanais de trabalho de um consultor, seriam 160 horas mensais.

Tópico 4 - ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

Descrição do item 001 Código 1066 - Serviços Técnicos Especializados, consultoria técnica.	
Informações Adicionais Contratação de empresa especializada na prestação de serviços de consultoria em segurança de Tecnologia da Informação e Comunicação (TIC) para realização de um mapeamento de riscos de segurança da informação, com base na norma ISO/IEC 27005:2022	
Período (Meses)	1
Quantidade	640
Unidade	servico (s)
Participação	Ampla Participação
Local de Entrega	edifício da sti (complexo da sec. economia)
Valor Unitário	R$ 359,41
Valor Total	R$ 230.022,40

4.1. O valor médio unitário estimado para essa Contratação é de R$ 359,41 (Trezentos e cinquenta e nove Reais e quarenta e um Centavos). Totalizando assim **R$ 230.022,40 (Duzentos e trinta mil, vinte e dois Reais e quarenta centavos).**

4.1.1 A pesquisa de preços que estabelecerá o valor estimado da presente contratação, será feita em momento oportuno.

4.2. O orçamento estimado da presente contratação sera elaborado com base nos parâmetros e calculado em conformidade com o Decreto estadual n° 9.900, de 07 de julho de 2021, cujo documento de Orçamento Estimado, que contém memória de cálculo, será anexado aos autos da contratação, indicando os parâmetros, a metodologia e os preços referenciais utilizados no cálculo estimativo.

Tópico 5 - JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

5.1. Não será adotado para esta licitação o parcelamento dos itens. Desta forma, o item será licitado em lote único, sendo:

5.2. Lote único - Consultoria especializada

5.2.1. A justificativa para a formação de Lote Único para as 640 horas de consultoria especializada na realização do mapeamento de segurança da informação com base na ISO/IEC 27005:2022 fundamenta-se no disposto na Lei nº 14.133/2021, especialmente em consonância com o princípio da eficiência e da obtenção da melhor proposta para a Administração Pública.

5.2.2. A realização do mapeamento de segurança da informação com base na ISO/IEC 27005:2022 envolve uma série de etapas técnicas interdependentes que demandam uma abordagem integrada e contínua. O processo abrange desde o levantamento inicial de ativos de informação, a identificação de ameaças e vulnerabilidades, a avaliação de impactos, até a documentação detalhada dos resultados e a capacitação da equipe para uso das informações geradas. A divisão do objeto em múltiplos lotes poderia comprometer a eficiência do processo, gerando dificuldades de coordenação entre as fases do mapeamento, com risco de descontinuidade entre as atividades realizadas por fornecedores distintos. A formação de um único lote permite a execução integrada de todas as etapas, garantindo uma entrega coesa e eficaz, com maior controle por parte da Administração Pública.

5.2.3. Além disso, ao concentrar os serviços em um único lote, será possível aumentar a competitividade da licitação, permitindo que as empresas interessadas apresentem propostas mais vantajosas, ajustando seus custos para um maior volume de serviços. A agregação dos serviços favorece a obtenção de melhores condições comerciais, aproveitando a economia de escala, o que resulta em uma proposta mais benéfica para a Administração Pública.

5.2.4. O agrupamento em lote único também facilita a escolha de fornecedores que possuam qualificação técnica necessária para a execução integral do serviço, reduzindo os riscos de falhas na execução e garantindo que o mapeamento seja conduzido de acordo com as melhores práticas da ISO/IEC 27005:2022. O fornecedor vencedor, sendo responsável por todas as fases do mapeamento, pode

alinhar as atividades de forma mais eficaz e com menor risco de inconsistências ou omissões nos resultados.

5.2.5. A Lei nº 14.133/2021, em seu artigo 5º, estabelece que a licitação deverá observar o princípio da eficiência, visando a otimização dos recursos públicos. A consolidação dos serviços em um único lote visa não apenas a eficiência na execução do objeto, mas também o melhor aproveitamento dos recursos públicos, com a redução de custos e a simplificação da gestão contratual, minimizando a necessidade de múltiplos contratos e a complexidade de acompanhamento.

5.2.6. Dessa forma, a formação do Lote Único para as 640 horas de consultoria especializada se justifica pela necessidade de garantir a integração das etapas do mapeamento de segurança da informação, pela maximização da competitividade e economia de escala, e pela necessidade de contratar um fornecedor qualificado e especializado para a execução do objeto de forma coordenada, eficaz e com a melhor relação custo-benefício para a Administração Pública.

5.2.7. Portanto, a adjudicação se dará por menor preço global.

Tópico 6 - REQUISITOS DA CONTRATAÇÃO

6.1. O objeto da contratação deve seguir os requisitos e padrões nacionalmente estabelecidos, em conformidade com a norma ISO/IEC 27005:2022 e legislações pertinentes.

6.2. REQUISITOS DE NEGÓCIO

6.2.1. A CONTRATADA deverá prover serviços de consultoria especializada para realização de um mapeamento de riscos baseado na ISO/IEC 27005:2022, incluindo identificação de ativos, análise de ameaças e vulnerabilidades, avaliação de impactos e recomendações de controles, visando fortalecer a segurança da informação na Subsecretaria de Tecnologia da Informação da Secretaria-Geral de Governo (SGG/GO).

6.2.2. Deverá entregar documentação detalhada, incluindo relatórios, matrizes de riscos e recomendações, que sirvam como base para a governança da segurança da informação e a implementação de controles futuros.

6.2.3. Deverá garantir a conformidade com as melhores práticas nacionais e internacionais de gestão de riscos, atendendo às necessidades de proteção de dados sensíveis e infraestrutura tecnológica da Subsecretaria de Tecnologia da Informação da SGG/GO.

6.2.4. Deverá assegurar a execução do serviço dentro do prazo estimado de 640 horas, conforme dimensionado no Estudo Técnico Preliminar, com qualidade e eficiência que atendam aos objetivos estratégicos da Subsecretaria de Tecnologia da Informação da SGG/GO.

6.3. REQUISITOS LEGAIS

6.3.1. A contratada deverá cumprir os requisitos legais estabelecidos em contrato, bem como os critérios técnicos descritos neste Termo de Referência e no Estudo Técnico Preliminar.

6.3.2. Durante a vigência contratual, a contratada deverá manter as condições de habilitação técnica, conforme exigido na legislação aplicável, incluindo a Lei nº 14.133/2021.

6.3.3. A contratada será responsável por todos os encargos e obrigações sociais previstos na legislação trabalhista vigente, sem vínculo empregatício. sob qualquer hipótese, entre seus profissionais e a Subsecretaria de Tecnologia da Informação da SGG/GO.

6.4. REQUISITOS TÉCNICOS

6.4.1. A contratada deverá utilizar a metodologia da ISO/IEC 27005:2022 como base para o mapeamento de riscos, abrangendo todas as etapas previstas na norma: identificação de ativos, análise de ameaças, avaliação de vulnerabilidades, cálculo de riscos e proposição de controles.

6.4.2. Os consultores alocados devem possuir expertise comprovada na aplicação da ISO/IEC 27005:2022, com experiência em segurança da informação e gestão de riscos cibernéticos, sendo profissionais capacitados, experientes e certificados na norma em questão.

6.4.3. O serviço deverá ser executado preferencialmente in loco nas instalações da SGG/GO, em horário comercial, salvo acordo prévio para atividades remotas, respeitando as normas de segurança da contratante.

6.4.4. A contratada deverá entregar relatórios claros e estruturados, contendo:

- Inventário de ativos de TI;
- Matriz de riscos com classificação de probabilidade e impacto;
- Recomendações de controles priorizados;
- Plano de ação para mitigação de riscos.

6.5. REQUISITOS DE EQUIPE TÉCNICA

6.5.1. A contratada deverá disponibilizar profissionais com experiência mínima de 2 anos em consultoria de segurança da informação e aplicação da ISO/IEC 27005:2022, conforme comprovado por certificações e atestados de capacidade técnica.

6.5.2. O quantitativo de profissionais deverá ser suficiente para cumprir as 640 horas previstas, respeitando o prazo estabelecido no cronograma a ser apresentado.

6.5.3. A qualificação mínima dos consultores deverá ser comprovada por meio de:

- Certificações em segurança da informação (ex.: ISO 27001, CISSP, CRISC);
- Declarações ou atestados de serviços anteriores similares.

6.5.4. A qualificação mínima de cada consultor será objeto de análise pela CONTRATANTE, que poderá rejeitar alguma certificação, documentação ou declaração apresentada, facultando à CONTRATANTE aceitar que a CONTRATADA apresente nova documentação ou substitua o consultor disponibilizado.

6.6. REQUISITOS DE CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

6.6.1. A contratada deverá assinar Termo de Compromisso de Sigilo, conforme o Anexo V, garantindo a confidencialidade de todas as informações acessadas durante a execução do serviço, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018).

6.6.2. Todos os profissionais envolvidos deverão assinar Termo de Ciência Individual de Sigilo, conforme o Anexo VI, comprometendo-se a não utilizar a infraestrutura da Subsecretaria de Tecnologia da Informação da SGG/GO para fins pessoais.

6.6.3. A contratada será responsável por qualquer violação de sigilo ou uso indevido de dados, devendo adotar medidas de segurança alinhadas às políticas da Subsecretaria de Tecnologia da Informação da SGG/GO.

6.7. REQUISITOS DE DOCUMENTAÇÃO E PROPRIEDADE INTELECTUAL

6.7.1. Toda a documentação gerada (relatórios, matrizes, planos) será de propriedade exclusiva da Subsecretaria de Tecnologia da Informação da SGG/GO, nos termos do artigo 93 da Lei nº 14.133/2021, sendo vedada sua reprodução ou comercialização pela contratada, sob qualquer hipótese.

6.7.2. A contratada deverá transferir todo o conhecimento técnico produzido à Subsecretaria de Tecnologia da Informação da SGG/GO ao final da execução, incluindo metodologias utilizadas e, se for o caso, sugestão de materiais de capacitação.

6.8. REQUISITOS DE GARANTIA

6.8.1. Será exigida a garantia da contratação de que trata o art. 96, da Lei federal nº 14.133, de 01 de abril de 2021

6.8.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

6.8.3. O prazo de vigência da apólice será igual ou superior ao prazo estabelecido no contrato principal e deverá acompanhar as modificações referentes à vigência deste mediante a emissão do respectivo endosso pela seguradora.

6.8.4. Em caso de opção de garantia, nas modalidades caução ou fiança bancária, esta deverá ser prestada em até 10 (dez) dias úteis após a assinatura do contrato.

Tópico 7 - RESULTADOS PRETENDIDOS

7.1. Considerando que as contratações públicas devem buscar resultados positivos para a Administração, são apontados os resultados pretendidos, em termos de eficiência, eficácia, efetividade e economicidade, em busca do melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, bem como de desenvolvimento nacional sustentável.

7.2. Assim, a presente contratação pretende alcançar o(s) seguinte(s) resultado(s):

7.2.1. A contratação de consultoria especializada para a realização de um mapeamento de segurança da informação com base na ISO/IEC 27005:2022 trará os seguintes resultados:

7.2.2. Aumento da maturidade na compreensão da segurança da informação: A execução de um mapeamento estruturado, alinhado às melhores práticas da ISO/IEC 27005:2022, proporcionará à SGG/GO uma visão mais clara e detalhada do seu cenário de segurança da informação, permitindo identificar ativos críticos, ameaças, vulnerabilidades e impactos de forma sistemática. Isso promoverá uma base sólida para decisões futuras relacionadas à proteção dos dados e sistemas, elevando o nível de maturidade organizacional no tema.

7.2.3. Fortalecimento da capacidade de planejamento contra ameaças cibernéticas: O mapeamento fornecerá informações fundamentais para compreender o ambiente de riscos da SGG/GO, possibilitando a priorização de ações para proteger ativos de dados e infraestrutura contra ameaças cibernéticas cada vez mais sofisticadas, como ataques de *ransomware*, *phishing* e outras técnicas avançadas utilizadas por cibercriminosos. A análise detalhada permitirá à Secretaria planejar controles mais eficazes e direcionados.

7.2.4. Redução de incertezas e base para resposta a incidentes: A identificação e avaliação de ameaças e vulnerabilidades por meio do mapeamento permitirá à SGG/GO mitigar incertezas relacionadas à segurança da informação, oferecendo uma visão clara dos pontos de exposição. Isso servirá como base para o desenvolvimento de planos de resposta a incidentes, possibilitando uma abordagem mais informada e estruturada para lidar com possíveis violações no futuro, minimizando impactos adversos.

7.2.5. Estabelecimento de uma base para governança e controles futuros: O mapeamento proporcionará uma estrutura inicial para a governança da segurança da informação, com relatórios detalhados e recomendações documentadas que orientarão a implementação de controles apropriados. Essa base será essencial para alinhar as ações da SGG/GO às melhores práticas da ISO/IEC 27005:2022 e normas relacionadas, promovendo a conformidade organizacional e a continuidade dos serviços públicos.

7.2.6. Melhoria na eficiência operacional e na priorização de recursos de TI: O mapeamento permitirá uma visão mais clara dos ativos críticos e dos riscos associados, possibilitando à Secretaria otimizar o uso de recursos tecnológicos e direcionar esforços para as áreas mais vulneráveis. A consultoria auxiliará na análise e organização dos dados coletados, oferecendo uma abordagem mais ágil e precisa para a gestão dos sistemas de TI e a alocação estratégica de recursos.

7.2.7. Maior preparação para conformidade com regulamentos e padrões: O mapeamento com base na ISO/IEC 27005:2022 fornecerá informações que facilitarão o alinhamento às exigências legais e regulatórias pertinentes, como a Lei Geral de Proteção de Dados (LGPD) e outras normas da série ISO/IEC 27000. Isso garantirá que a SGG/GO tenha uma base sólida para atender a requisitos de segurança da informação e proteção de dados pessoais e sensíveis.

7.2.8. Aumento da confiabilidade e da imagem institucional: A realização de um mapeamento detalhado e estruturado, conduzido por uma consultoria especializada, fortalecerá a imagem da SGG/GO como uma organização comprometida com a segurança da informação. Isso aumentará a confiança de cidadãos, parceiros e outras entidades governamentais, contribuindo para uma gestão mais transparente e segura, mesmo que a certificação ISO/IEC 27001 não seja o objetivo imediato deste processo.

Tópico 8 - POSSÍVEIS IMPACTOS AMBIENTAIS E MEDIDAS MITIGADORAS

8.1. Considerando que o objeto desta contratação refere-se exclusivamente à prestação de serviços de mão de obra especializada e consultoria técnica, conforme especificado neste Estudo Técnico, não há evidência de impactos ambientais diretos ou indiretos decorrentes da execução do contrato.

- **Natureza do serviço**: Atividades intelectuais e administrativas, sem intervenção física em áreas naturais, consumo de recursos naturais ou geração de resíduos;+
- **Escopo contratual**: Não envolve obras, instalações, transporte de materiais ou qualquer ação passível de alteração do meio ambiente;

8.2. Diante do exposto, não se aplicam medidas de mitigação, compensação ou monitoramento ambiental.

Tópico 9 - GERENCIAMENTO DE RISCO

FASE DE ANÁLISE – ESTUDO TÉCNICO PRELIMINAR	
Risco ETP01 – Estudo Técnico Preliminar incompleto ou inadequado	
Probabilidade	( ) Baixa (X) Média ( ) Alta
Impacto	( ) Baixo ( ) Médio (X) Alto
Nível de Risco	( ) Aceitável ( ) Aceitação intermediária (X) Inaceitável

Id	**Danos**
1	Elaboração de TR/Edital inadequado gerando recursos ou impugnação quando da sua publicação.
2	Atraso no procedimento licitatório devido à republicação do edital.
3	Contratação com prejuízos para administração.

Id	**Ação Preventiva**	**Responsável**
1	Capacitar pessoal ou designar pessoal capacitado para executar a atividade.	GCIBER

Id	**Ação de Contingência**	**Responsável**
1	Recomendar correções e/ou adequações no termo de referência ou projeto básico.	SUOSTI
2	Não aprovar ETP.	STI

Risco ETP02 – Entrega incompleta dos serviços pela CONTRATADA	
Probabilidade	(X) Baixa ( ) Média ( ) Alta
Impacto	( ) Baixo ( ) Médio (X) Alto
Nível de Risco	( ) Aceitável ( ) Aceitação intermediária (X) Inaceitável

Id	**Danos**
1	Impossibilidade de utilização dos serviços contratados.

Id	**Ação Preventiva**	**Responsável**
1	Acompanhar e validar os serviços prestados, executando análises após a entrega.	GCIBER

Id	**Ação de Contingência**	**Responsável**
1	Realizar nova contratação.	GCIBER

Risco ETP03 – Ambiente inadequado ou indisponível na CONTRATANTE para entrega dos serviços contratados	
Probabilidade	(X) Baixa ( ) Média ( ) Alta
Impacto	( ) Baixo ( ) Médio (X) Alto
Nível de Risco	( ) Aceitável ( ) Aceitação intermediária (X) Inaceitável

Id	Danos	
1	Impossibilidade de prestação dos serviços pela CONTRATADA.	
2	Possibilidade de distrato após a contratação.	
Id	**Ação Preventiva**	**Responsável**
1	Disponibilizar, verificar e configurar o ambiente, hardware e S.O. para que a CONTRATADA possa finalizar a verificação e entrega dos serviços contratados.	GINT
Id	**Ação de Contingência**	**Responsável**
1	Acionar a STI/SGG para disponibilização de ambiente.	GCIBER/CONTRATADA

TABELA DE NÍVEL DE RISCO				
NÍVEL DE RISCO		**PROBABILIDADE DO RISCO**		
		BAIXA	MÉDIA	ALTA
IMPACTO DO RISCO	BAIXO	ACEITÁVEL	ACEITÁVEL	ACEITAÇÃO INTERMEDIÁRIA
	MÉDIO	ACEITÁVEL	ACEITAÇÃO INTERMEDIÁRIA	INACEITÁVEL
	ALTO	ACEITAÇÃO INTERMEDIÁRIA	INACEITÁVEL	INACEITÁVEL

Tópico 10 - PROVIDÊNCIAS PRÉVIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO

10.1. Não há necessidade de adequação do ambiente da SGG/GO para a implantação dos serviços da consultoria a ser contratada, haja vista que se trata de prestação de serviços a serem realizados *in loco*.

10.2. Ademais, pela característica do objeto aqui tratado, não há necessidade de capacitação de servidores para fiscalização e gestão contratual.

Tópico 11 - CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

11.1. Para atendimento da finalidade desta contratação, não há contratações correlatas ou interdependentes vinculadas ao objeto em questão. A presente aquisição constitui ação autônoma e auto-suficiente, não dependendo de outras licitações, contratos ou aquisições paralelas para sua execução integral.

Tópico 12 - AVALIAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

12.1. Com base nas análises realizadas ao longo do Estudo Técnico Preliminar (ETP), a Equipe de Planejamento declara a viabilidade técnica e econômica da contratação de consultoria especializada para mapeamento de riscos conforme a norma ISO/IEC 27005:2022, considerando:

Relevância estratégica: A atividade é essencial para o desenvolvimento das atividades da Secretaria-Geral de Governo, garantindo a segurança da informação e a conformidade com melhores práticas internacionais.

Adequação orçamentária: Os custos previstos atendem ao princípio da economicidade, sendo compatíveis com os benefícios esperados.

Gestão de riscos: Os riscos identificados são administráveis e a área requisitante compromete-se a fornecer todos os insumos necessários para o sucesso do projeto.

12.2. Observações:

- A presente manifestação restringe-se à análise técnica, não convalidando eventuais atos em desacordo com a legislação vigente, conforme atribuições desta equipe.
- A contratação está alinhada aos dispositivos da Lei Federal nº 14.133/2021 e ao Decreto Estadual nº 10.207/2023, que regulamentam as aquisições públicas.

12.3. Conclusão: O ETP demonstra a necessidade e viabilidade da solução "Prestação de Serviços - Consultoria em Riscos de TI" para o atendimento das demandas institucionais, recomendando sua formalização conforme os parâmetros técnicos e legais expostos.

EQUIPE DE PLANEJAMENTO RESPONSÁVEL PELA ELABORAÇÃO DESTE ETP:

Responsável	Função	Equipe
WILLIAN ADAO RABELO	Integrante Técnico	Equipe de Planejamento
VALDENICE NASCIMENTO DE MOURA	Integrante Administrativo	Equipe de Planejamento