



PRESIDÊNCIA DA REPÚBLICA

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO(ETP) -TIC

Processo nº 00180.000078/2021-96

Histórico de Revisões

Data	Versão	Descrição	Autor
04/10/2021	2.0	Segunda versão do documento	Equipe de Planejamento da Contratação

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda 2379874, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS**1.1. Identificação das necessidades de negócio**

Estuda-se no presente documento a aquisição de uma solução de tecnologia de informação capaz de realizar o pré-processamento das informações recebidas das diversas fontes (sensores e agentes externos), de forma a facilitar o processo de triagem do tratamento de incidentes cibernéticos. Neste contexto, a solução deve prover uma pré-triagem ou pré-análise das informações recebidas e fornecer alto grau de automatização de ações que hoje são realizadas de forma manual pela Área Demandante do GSI/PR.

A Área Demandante do sistema, é uma coordenação ligada ao Departamento de Segurança da Informação (DSI) subordinado ao Gabinete de Segurança Institucional da Presidência da República (GSI-PR), conforme Decreto Nº 9.668, de 2 de janeiro de 2019.

Trata-se de um CSIRT de responsabilidade nacional de coordenação e realização de ações destinadas à gestão de incidentes computacionais (monitoramento, prevenção, tratamento e resposta a incidentes computacionais) em órgãos e entidades governamentais, e tem, entre suas competências, conforme portaria nº 91, de 26 de julho de 2017:

- acompanhar e analisar tecnicamente os incidentes de segurança nas redes do governo;
- implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança nas redes do governo;
- orientar os administradores de redes do governo quanto aos procedimentos de proteção e recuperação de incidentes de rede, bem como quanto à redução de riscos, prevenção de ameaças e vulnerabilidades cibernéticas;
- pesquisar e analisar possíveis impactos de vulnerabilidades e falhas de segurança de redes do governo;
- armazenar e analisar informações relativas a ameaças e tendências de vulnerabilidades cibernéticas; e
- orientar as equipes de tratamento de incidentes de redes do governo na verificação da conformidade dos controles estabelecidos de segurança da informação.

A relação entre a quantidade de eventos recebidos e capacidade humana para execução do processo de triagem, quanto à priorização e análise dos referidos eventos, impossibilita a reação rápida da Área Demandante do GSI/PR, quanto aos eventos mais críticos para a Administração Pública Federal, considerando elementos diferenciadores, como o nível de criticidade do tipo de incidente e o tipo de entidade envolvida.

Também não há um processo de monitoramento abrangente, em tempo real, que faça correlações de eventos e permita a produção de uma inteligência situacional e afins.

O sistema de gerenciamento e tratamento de incidentes “Request Tracker”, chamado comumente de RT (<https://bestpractical.com/request-tracker>), implementado em 2011, atualmente, necessita de automatizações para auxiliar no Processo de Tratamento de Incidentes. É importante salientar que, em 10 anos, a estrutura tecnológica da *constituency* da Área Demandante do GSI/PR, evoluiu em termos de quantidade de serviços digitais, armazenamento de dados, produção de conhecimento estratégico, criticidade dos sistemas, criticidade dos ativos tecnológicos e, conseqüentemente, riscos decorrentes da interrupção de serviços considerados essenciais para a sociedade. A quantidade de informações em todo âmbito da administração pública federal ainda é crescente diante

da transformação digital em curso, do crescimento dos centros de dados e do valor das informações para apoio às estratégias de negócio.

A Área Demandante do GSI/PR utiliza o RT (*Request Tracker*), customizado, com várias extensões desenvolvidas sob demanda, e aplicações externas que apoiam o processo de triagem. Essa característica requer que a Área Demandante do GSI/PR tenha capacidade de manter e desenvolver novas extensões e aplicações para se adaptar aos novos tipos de incidentes e situações que surgem e estão em constante evolução.

Um outro problema é a linguagem na qual o RT é desenvolvido. O Perl é de difícil compreensão e possui uma curva de aprendizado longa. Atualmente é difícil encontrar recursos humanos capacitados para desenvolver em Perl e, adicionalmente, a linguagem está deixando de receber atualizações e evoluir, tornando-se obsoleta.

A Área Demandante do GSI/PR recebe, diariamente, diversos eventos relacionados a incidentes de segurança cibernética. Estes eventos são recebidos por meio de dados advindos das seguintes fontes:

- sensores próprios, no qual convertem informações processadas em formato específico e enviam, via e-mail, ao sistema de gerenciamento e tratamento de incidentes “Request Tracker”, chamado comumente de RT (<https://bestpractical.com/request-tracker>), no qual são gerados automaticamente tickets para análise dos respectivos eventos;
- de e-mails enviados por entidades governamentais, em especial da Administração Pública Federal, e parceiros como o CERT br e o CDCiber;
- de qualquer pessoa que deseja reportar um incidente e utiliza o e-mail ctir@ctir.gov.br conforme recomendado em <https://www.ctir.gov.br/contato/>.

Todos estes eventos são recebidos em uma fila, passam por um responsável (triagem) pela confirmação, priorização e distribuição dos tickets, para serem tratados, de forma individual, pelos analistas de incidentes cibernéticos.

A dificuldade de codificar as regras de priorização dos eventos/incidentes no sistema e as notificações recebidas de forma não estruturada (e-mails de agentes externos e pessoas) dificultam a classificação de forma adequada, fazendo com que exista um volume grande de tickets a serem tratados sobrecarregando o processo de Triagem.

Isso pode levar a uma demora no tempo de resposta à incidentes e eventos cibernéticos mais críticos que deveriam ser analisados com prioridade sobre os de menos criticidade, ocasionando perdas significativa às entidades envolvidas quanto ao requisito de disponibilidade e integridade das informações ao cidadão e ao governo, além das demais entidades que poderiam receber alertas preventivos por parte da Área Demandante do GSI/PR, a fim de poderem evitar danos similares em seus órgãos.

Neste contexto, faz-se necessário, uma automatização da classificação e priorização dos eventos/incidentes recebidos pelo sistema, facilitando o tempo de resposta à incidentes e eventos cibernéticos mais críticos.

Ao analisar as necessidades do Documento de Oficialização da Demanda que originou o presente estudo, identifica-se, previamente, uma concordância com os seguintes objetivos estratégicos de TI da PR, a saber:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS Tecnologia da Informação e Comunicação da Presidência da República (2021-2022) (Ref: http://www4.planalto.gov.br/cgd/assuntos/pdti-2015-2018/plano-diretor-de-tic-na-pr-pdticpr-2019-2022-revisao-2021.pdf)	
ID	Objetivos estratégicos
OE01	Entregar soluções de TIC que agreguem valor estratégico para a PR
OE02	Aumentar o nível de satisfação do usuário de TIC da PR
OE03	Viabilizar o uso da inteligência da informação como solução de TIC
OE08	Promover a inovação e a modernização da infraestrutura e serviços de TIC
OE10	Ampliar a capacidade e a qualidade da entrega dos serviços de TIC

A solução que se deseja planejar também encontra alinhamento com o Planejamento Estratégico do Gabinete de Segurança Institucional GSI/PR par ao período de 2018-2023, a saber:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS Gabinete de Segurança Institucional – GSI/PR (2018-2023) (Ref: https://www.gov.br/gsi/pt-br/arquivos/planejamento-estrategico-do-gsi.pdf)	
ID	Objetivos estratégicos
OE-2	Garantir a soberania, os interesses nacionais e a Segurança do Estado
OE-6	Aperfeiçoar os mecanismos de Governança e Gestão Corporativa
OE-7	Promover a inovação dos serviços e processos com foco na simplificação e transformação digital
OE-8	Promover a inovação e a modernização da infraestrutura e serviços de TIC.
OE-9	Intensificar os mecanismos de proteção da Presidência da República e de outras instituições de Estado
OE-14	Proporcionar soluções tecnológicas, integradas, seguras e de alto desempenho

Alinhamento ao PDTIC/PR 2021-2022:

ALINHAMENTO AO PDTIC/PR 2021-2022 (Ref: http://www4.planalto.gov.br/cgd/assuntos/pdti-2015-2018/plano-diretor-de-tic-na-pr-pdticpr-2019-2022-revisao-2021.pdf)	
ID	Ação no PDTIC
A40	Implantar software de auditoria e análise de vulnerabilidades

Alinhamento ao PAC 2021:

ALINHAMENTO AO PAC 2021	
Item	Descrição
1749	Solução de tecnologia de informação capaz de realizar o pré-processamento das informações recebidas das diversas fontes (sensores e agentes externos) de forma a facilitar o processo de triagem do tratamento de incidentes.

1.2. Identificação das necessidades tecnológicas

O objeto de estudo é a aquisição de 1 (uma) solução de tecnologia da informação com garantia de suporte técnico por 12 (doze) meses.

Item	Descrição	Unidade	Qtde
-------------	------------------	----------------	-------------

01	<p>Licença perpétua de uso de solução de tecnologia de informação customizada de forma a ser capaz de realizar o pré-processamento das informações recebidas de diversas fontes (sensores e agentes externos), com o objetivo de facilitar o processo de triagem do tratamento de incidentes pela Área Demandante do GSI/PR.</p> <p>Instalação e configuração da solução em ambiente da CONTRATANTE.</p> <p>Garantia de suporte por 12 (doze) meses.</p>	Unidade	1
----	--	---------	---

Os demais requisitos e especificações técnicas constam dos Anexos I a IV - 2971558, 2971563, 2971592, 2972088 e 2972099.

1.3. Identificação das necessidades legais

Lei Federal nº 8.666, de 21 de junho de 1993, que institui normas para licitações e contratos da Administração Pública Federal direta, autárquica e fundacional.

Lei Federal nº 10.520/2002, de 17 de julho de 2002, que institui a modalidade de licitação denominada pregão para bens e serviços comuns.

Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração Pública Federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

Decreto nº 10.332 de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências (revoga o decreto nº 8.638 de 15 de janeiro de 2016)

Instrução Normativa SGD/ME nº 202, de 18 de setembro 2019, da Secretaria Governo Digital do Ministério da Economia, que altera a Instrução Normativa nº 1, de 4 de abril de 2019

Instrução Normativa SGD/ME nº 1, de 4 de Abril de 2019, da Secretaria Governo Digital do Ministério da Economia (SGD/ME), que dispõe sobre o processo de contratações de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração de Recursos de Informação e Informática (SISP).

Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional.

Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da Presidência da República.

Plano Anual de Contratações (PAC) - número do item: 1749 Tipo: TIC Código do item: 26077

Planejamento Estratégico do GSI 2018/2023

1.4. Identificação das necessidades de manutenção

Prover rapidez e tempestividade na execução da assistência técnica presencial na sede do GSI/PR.

Após a CONTRATADA concluir a instalação, configuração e/ou as substituições de itens com não conformidade de funcionamento de acordo com as condições e prazos exigidos no Termo de Referência, a CONTRATANTE emitirá o Termo de Recebimento Provisório em até 5 (cinco) dias úteis, contados a partir da comunicação de conclusão da entrega, quando couber.

Em até 15 (quinze) dias úteis após a emissão do Termo de Recebimento Provisório e sendo confirmada a operação e desempenho a contento da solução adquirida, nos termos das especificações técnicas e do atestado de homologação, a CONTRATANTE emitirá o Termo de Recebimento Definitivo de cada item que foi adquirido, instalado, configurado e/ou substituído, quando couber.

A CONTRATADA deverá atender as especificações de tempo e local de atendimento de garantia da solução adquirida.

A CONTRATADA deverá solucionar qualquer problema em até 5 (cinco) dias úteis, respeitando os prazos previstos no TR, após demanda da CONTRATANTE e designar preposto para representá-la perante a CONTRATANTE.

1.5. Identificação das necessidades temporais

O cronograma de implementação, instalação e capacitação da solução será apresentado, conforme o estipulado no Termo de Referência.

A data de entrega da solução deverá seguir as normas existentes podendo ser ajustada em contrato, em função do tipo/origem do bem adquirido.

Para a implementação da solução em cada instalação presidencial, a CONTRATANTE, mediante acordo com a CONTRATADA, fixará um cronograma de execução com base nos seguintes parâmetros mínimos:

- Recebimento provisório dos bens fornecidos (conforme prazo estipulado no Termo de Referência).
- Conferência quantitativa e qualitativa dos bens fornecidos, a ser executado por Comissão nomeada pela CONTRATANTE, devendo ter a participação de representante da CONTRATADA.
- Indicação de servidores da CONTRATADA, responsáveis pela instalação e configuração da solução nos equipamentos da CONTRATANTE, visando o cadastramento dos mesmo e autorização de acesso às instalações.

Organização de cronograma de execução dos trabalhos de instalação da solução (em conformidade com o Cronograma Físico-Financeiro previsto no Termo de Referência), a ser planejado por representantes da CONTRATANTE e CONTRATADA, tendo no mínimo os seguintes aspectos a considerar:

- Responsável técnico indicado pela CONTRATADA;
- Pessoal empregado pela CONTRATADA nas atividades, além do técnico responsável;
- Data de início e fim das atividades;
- Horários para início e fim das atividades diárias;
- Indicação dos aspectos a serem avaliados durante a instalação da solução nos equipamentos da CONTRATANTE, prevendo a metodologia a ser aplicada e os resultados apresentados, mediante a formalização de relatório específico a ser executado por Comissão indicada pela CONTRATANTE;
- Cronograma de execução de possíveis correções identificadas pela CONTRATANTE;
- Reanálise dos serviços executados e confecção do Termo de Recebimento Definitivo.

1.6. Identificação das necessidades de segurança

A CONTRATADA deve aderir e cumprir a Política de Segurança do Gabinete de Segurança Institucional da Presidência da República e a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República - POSITEC/PR e, ainda, observar e cumprir a legislação vigente relativa à Segurança da Informação.

O representante legal da CONTRATADA, bem como todos os funcionários da mesma que tiverem acesso às informações ou dependências da Presidência da República, deverão assinar o Termo de Confidencialidade, contendo declaração de manutenção de sigilo e ciência em relação às políticas de segurança da informação, às normas de segurança vigentes no GSI/PR e, quando couber, nos demais ministérios da Presidência da República.

Naquilo que couber, recomenda-se observar o contido na Resolução Nº 4, de 05 de junho de 2020, que institui a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República - POSITEC/PR, que dispõe:

"Seção V

Do Tratamento e da Classificação da Informação

Art. 21. Os dados, as informações e os sistemas de informação da Presidência da República deverão ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir-lhes a disponibilidade, a integridade, a confidencialidade e a autenticidade.

...

Seção XI

Da Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Art. 33. As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação deverão observar os padrões, critérios e controles de segurança dispostos em normas e na legislação específica."

A CONTRATADA deve informar a relação dos funcionários que irão realizar a entrega e instalação da solução na sede da CONTRATANTE e o dia de realização mesma. Os funcionários devem estar devidamente identificados, com uso de crachás e uniforme específico da empresa enquanto permanecerem nas instalações da CONTRATANTE. Os empregados somente poderão adentrar nas instalações da CONTRATANTE e lá permanecerem acompanhados de um servidor do órgão.

A CONTRATADA deve adotar as melhores práticas de mercado em gestão de segurança da informação na realização das atividades para a CONTRATANTE.

A CONTRATADA deve usar meios especializados e de alta qualidade. Pode ser definido um melhor ambiente para executar cada serviço, com diferentes requerimentos de segurança, ferramentas diferentes e o sistema operacional mais adequado para cada serviço, quando couber.

A solução deve estar de acordo com a política de segurança definida pela CONTRATANTE.

A empresa a ser contratada não poderá armazenar consigo qualquer documento técnico ou dados que contemplem configurações e regras de segurança implantados no GSI/PR.

Será considerada ilícita a divulgação, o repasse ou utilização indevida de informações, bem como dos documentos, imagens, gravações, dados e informações utilizados durante a prestação dos serviços.

Qualquer anormalidade verificada no curso da prestação de serviços será imediatamente comunicada por escrito à empresa contratada.

A empresa a ser contratada deverá guardar inteiro sigilo dos dados processados, reconhecendo ser estes de propriedade exclusiva GSI/PR, sendo vedada a sua cessão, locação ou venda a terceiros sem prévia autorização formal, de acordo com os termos constantes do Termo de Compromisso a ser elaborado conjuntamente ao contrato.

Todas as informações, imagens, aplicativos e documentos providos pelo GSI/PR, ou oriundos das informações que forem manuseados e utilizados, são de propriedade exclusiva deste Gabinete, não podendo ser repassadas, copiadas, alteradas ou absorvidas na relação de bens das empresas a serem contratadas, bem como de seus executores, sem expressa autorização formal e escrita.

Cumprir, no que couber, a seguinte legislação:

- Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações - Lei de Acesso à Informação (LAI);
- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);
- Decreto nº 10.332 de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022;
- Decreto nº 9.637, de 26 de dezembro de 2018, estabelece a Política Nacional de Segurança da Informação.
- Resolução nº 4, de 05 de junho de 2020, que Institui a Política de Segurança da Informação em Meios Tecnológicos da Presidência da República - POSITEC/PR.
- Norma Complementar nº 16 /IN01/DSIC/GSIPR, que estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.
- Norma VIII-201 Ver. 2 de Março de 2014 da Secretaria de Administração da Presidência da República, que trata sobre desenvolvimento de sistemas.

1.7. Identificação das necessidades de projeto e implementação

Os trabalhos atinentes à execução do contrato a ser celebrado para a consecução do objeto do presente Estudo Preliminar a Contratação deverão ser executados por profissionais treinados e capacitados da empresa a ser contratada, segundo perfis e qualificações necessários.

1.8. Identificação da metodologia de trabalho

Todas as atividades necessárias à instalação, configuração e manutenção da solução deverão observar e respeitar o horário de funcionamento do GSI/PR, exceto nos casos de manutenção corretiva, quando, a qualquer horário, a empresa contratada deverá ser acionada.

Todo o trabalho realizado pela empresa a ser contratada estará sujeito à avaliação técnica, sendo homologado quando estiver de acordo com o padrão de qualidade exigido pelo órgão e de acordo com os prazos definidos.

Para execução da solução, a CONTRATADA deverá apresentar projeto simples, contendo no mínimo:

- Estrutura básica da solução;
- Fases de implementação; e
- Realização de testes.

1.9. Identificação das necessidades sociais, ambientais e culturais

Todos os documentos, manuais e termos de garantias da solução, assim como a documentação produzida pela CONTRATADA, devem estar no idioma português do Brasil. Poderá ser admitido, pela CONTRATANTE, o idioma inglês de soluções importadas pelo fornecedor que serão entregues à CONTRATANTE.

Todo o resíduo reciclável gerado deve ser descartado em compartimentos adequados, em cumprimento às normas ambientais vigentes.

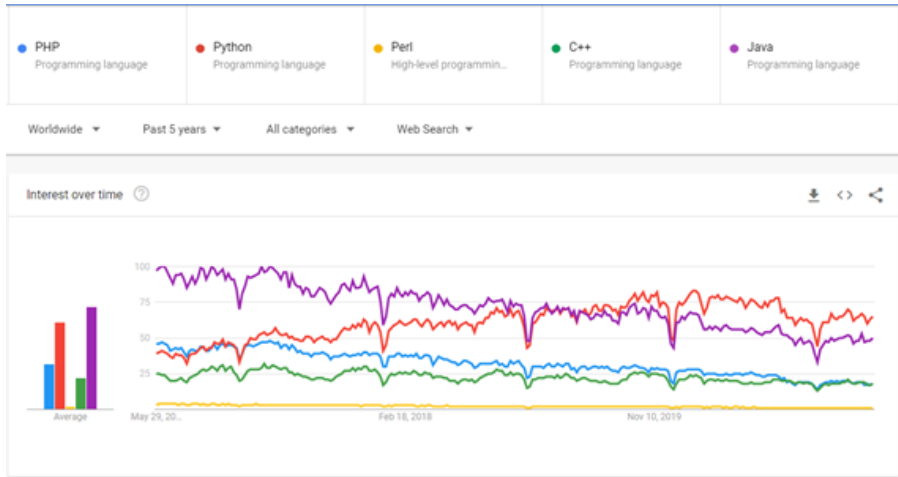
Salvo quando acordado de forma diferente, as embalagens ou invólucros dos bens fornecidos deverão ser removidas pela CONTRATADA antes da emissão do Termo de Recebimento Definitivo, para que não permaneça na área de responsabilidade do

3 – ANÁLISE DE SOLUÇÕES

As alternativas de solução para a demanda em questão que foram consideradas no Documento de Análise de Viabilidade (Nota Técnica nº 19/2021/CGGSI/DSI - 2683202), constante no processo SEI nº 00180.000078/2021-96 são:

- Manter a solução atual – *Request Tracker*.
- Substituir a solução atual por sua versão mais atualizada.
- Adoção da solução utilizada por outros CSIRT.
- Contratar o serviço de desenvolvimento de uma nova solução.
- Adquirir uma solução de mercado customizada para as necessidades da Área Demandante do GSI/PR.

3.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
a)	<p>Em relação a alternativa a) manter a solução atual – <i>Request Tracker</i>, deve-se observar o seguinte:</p> <p>O Request Tracker (RT) é desenvolvido em Perl e o RTC (funcionalidade desenvolvida pelo CTIR Gov) utiliza a linguagem PHP. Esta aplicação apoia a atividade de triagem permitindo realizar algumas operações que não são possíveis utilizando-se somente o RT.</p> <p>A ferramenta atual, o Request Tracker (RT) poderia ser customizado para atender os requisitos essenciais definidos no documento “DSI – CTIR Gov - Requisitos funcionais - v 2”. No entanto, essa alternativa não seria recomendável pelos seguintes motivos:</p> <ul style="list-style-type: none"> Utilização da linguagem Perl: <ul style="list-style-type: none"> O principal problema do Perl está no fato que essa linguagem tem a reputação de gerar mensagens de erro ruins e confusas e ter uma filosofia de codificação muito aberta (com o lema “a sempre mais de uma maneira de resolver um problema”) que acaba gerando código confuso e de difícil interpretação. Esses problemas se devem especialmente ao fato do Perl 5 atender a vários estilos diferentes de sintaxe. O Perl é considerado, na verdade, uma linguagem em desuso. Conforme o gráfico abaixo (obtido no Google Trend em 25/05/2021), verifica-se que o interesse em PERL tem sido quase nulo nos últimos 5 anos.  <ul style="list-style-type: none"> O Perl está em declínio há algum tempo, praticamente atingindo zero de participação de mercado. Portanto, pode-se afirmar que o Perl pode ser considerado uma linguagem morta e definitivamente não deve ser utilizada para novos projetos. Cabe observar que a afirmação de que a “...linguagem é considerada como obsoleta em virtude de não estar mais sendo evoluída” não está correta. <ul style="list-style-type: none"> Em outubro de 2019, o criador do Perl, Larry Wall, aprovou a renomeação do Perl 6 como Raku (https://raku.org), após quase duas décadas de trabalho na versão 6 que, conseqüentemente, viu o Perl preso na versão 5. As versões anteriores do Perl foram lançadas com uma cadência de 1 a 2 anos.

	<ul style="list-style-type: none"> ○ Assim sendo, o Perl saltará da versão 5 para a 7. No entanto, Ignorar a sexta versão principal de uma linguagem não é algo sem precedentes, com o PHP saltando de 5 para 7 em 2015. • Não há pessoal capacitado no CTIR Gov para desenvolver código em Perl e, em função do desuso, será cada vez mais difícil encontrar pessoal capacitado na linguagem. Além disso, conforme lembrado que as personalizações realizadas no RT são peculiares, cada nova customização tornará o processo mais complexo. <ul style="list-style-type: none"> ○ Em termos práticos, o RT poderia ser customizado desde que fosse alocado pessoal capacitado na linguagem da ferramenta ou na utilização da API para desenvolver e integrar funcionalidades desenvolvidas em outra linguagem. ○ É importante ressaltar que, além da barreira causada pela linguagem, os módulos não são bem documentados, nem as relações entre os módulos internos são conhecidas. Portanto, seria necessário considerar o tempo que essa equipe necessitaria para estudar as customizações já existentes a fim de determinar a melhor solução para incorporar novas customizações e/ou novos módulos ao RT. • O gerenciamento de contatos é deficiente, atendendo parcialmente as necessidades do CTIR Gov. Na ferramenta atual é necessário manipulação direta na base de dados para alteração de contatos com mais de um endereço de e-mail. Não é a solução mais adequada e isso cria uma grande dificuldade de gerenciar os contatos no RT. • Pelos motivos expostos, a alternativa a) foi considerada desaconselhável tecnicamente.
b)	<p>A alternativa b) substituir a ferramenta atual por sua versão mais atualizada, também foi considerada pela equipe como desaconselhável tecnicamente.</p> <ul style="list-style-type: none"> • A nova versão do Request Tracker (RT) poderia ser customizada para atender os requisitos essenciais definidos no documento “DSI – CTIR Gov - Requisitos funcionais”. No entanto, essa alternativa não seria recomendável pelos seguintes motivos: <ul style="list-style-type: none"> ○ A linguagem utilizada ainda é o Perl, logo os problemas que existem na versão atual persistiriam na nova versão. ○ Ao contrário da versão atual, a nova versão tem seus módulos documentados (https://docs.bestpractical.com/rt/5.0.0/index.html). No entanto, a nova versão utiliza o Perl 5, o qual deverá ser substituído em breve pelo Raku (Raku.org) ou pelo Perl 7. ○ A ferramenta atualizada acarretaria condições iguais ou semelhantes às da ferramenta atual. <ul style="list-style-type: none"> ▪ O CTIR Gov não possui equipe de desenvolvimento para avaliação dos módulos do sistema e, com isso, não tem condições de identificar as mudanças efetivadas e/ou utilizadas para personalizar as regras de negócio aplicadas na versão atual. Com isso, não é possível avaliar os impactos de uma migração para nova versão. • Assim como ocorreu na alternativa a), a customização da versão atualizada dependeria da alocação de pessoal capacitado na linguagem da ferramenta ou na utilização da API para desenvolver e integrar funcionalidades desenvolvidas em outra linguagem. <ul style="list-style-type: none"> ○ No caso específico, a equipe de CTIR Gov necessitaria trabalhar em conjunto com a equipe alocada a fim de estudar as reais capacidades da versão atualizada e definir quais customizações seriam necessárias. <ul style="list-style-type: none"> ▪ Essa prática geraria dependência com a versão utilizada ou a necessidade de correções nas funcionalidades desenvolvidas em caso de necessidade de nova atualização da ferramenta. ○ É relevante observar, ainda, que as personalizações realizadas no RT atual são peculiares. São ações e procedimentos complexos que demandam uma avaliação detalhada do código para fazer o levantamento das funcionalidades para que as mesmas possam ser aplicadas em uma nova versão do RT.
c)	<p>A alternativa c) adoção da solução adotada por outros CSIRTs foi considerada inviável, nesse momento, pela equipe.</p> <ul style="list-style-type: none"> • Em função da necessidade de maiores estudos por parte da equipe do CTIR Gov e da urgência da atualização do ambiente de gestão de incidentes do CTIR Gov, essa alternativa foi descartada. • Outro aspecto considerado foi o levantamento de soluções e informações realizado pela equipe do CTIR Gov. <ul style="list-style-type: none"> ○ De acordo com levantamento feito, verificou-se que: <ul style="list-style-type: none"> ▪ O CAIS/RNP utiliza um sistema próprio, aprimorado do RT ao longo do tempo, que chama-se SIGIS (Sistema Integrado de Gestão de Incidentes Cibernéticos). Há uma expectativa, da mesma forma que o CTIR Gov, de tomada de decisão para modernizar o processo e estuda-se o uso da ferramenta “The Hive”. ▪ O CERT.br afirmou que vários CERTs nacionais utilizam “The Hive”, mas a maioria utiliza o RT ou algum outro sistema de acompanhamento de tickets, como OTRS. Em todos estes casos são feitas personalizações internas, por pessoal interno. Já o CERT.br, por sua vez, utiliza um conjunto de sistemas desenvolvidos

	<p>internamente, que lidam com as necessidades de triagem e acompanhamento em ambiente totalmente baseado em software livre.</p> <ul style="list-style-type: none"> ▪ É importante ressaltar que, no Brasil, o CTIR Gov é um dos dois CSIRTs nacionais de coordenação, sendo o CERT.br o outro CSIRT com atuação similar. <ul style="list-style-type: none"> • Da mesma forma que os órgãos consultados, o CTIR Gov também necessita de uma solução que seja específica para suas atividades, o que provavelmente levaria ao descarte das soluções adotadas por outros CSIRTs no país ou a necessidade de um longo trabalho de customização de uma das soluções já em uso, a quais, por sua vez, já foram customizadas para uso específico de cada CSIRT. <ul style="list-style-type: none"> ◦ Assim como ocorreu na alternativa a) e na alternativa b), a adoção de uma ferramenta adotada por outros CSIRTs certamente implicará na customização dessa ferramenta, o que implicaria na alocação de pessoal capacitado na linguagem da ferramenta ou na utilização da API para desenvolver e integrar funcionalidades desenvolvidas em outra linguagem. <ul style="list-style-type: none"> ▪ No caso específico, a equipe de CTIR Gov necessitaria trabalhar em conjunto com a equipe alocada a fim de estudar as reais capacidades da ferramenta e definir quais as customizações que seriam necessárias. ▪ Essa prática geraria dependência com a versão utilizada ou a necessidade de correções nas funcionalidades desenvolvidas em caso de necessidade de nova atualização da ferramenta.
d)	<p>A alternativa d) contratação do serviço de desenvolvimento de uma nova solução é considerada viável tecnicamente, sendo considerada pelo integrante técnico João Alberto Muniz Gaspar, SIAPE 01586222, como a mais adequada para atender as necessidades da área demandante, pois com ela haveria:</p> <ul style="list-style-type: none"> • a garantia de que o produto final certamente seria desenvolvido exatamente de acordo com as necessidades e interesses da equipe do CTIR Gov; e • a possibilidade de determinar que a solução seja desenvolvida utilizando os procedimentos e linguagens homologados pela DITEC/PR, o que permitiria, no futuro, incorporar a necessidade de novas customizações nos processos de contratação de fábrica de software da Presidência da República. <p>No entanto, em função de restrições temporais (todo o processo, inclusive a contratação da solução necessita ser realizada este ano ainda, sob pena de perda dos recursos orçamentários alocados, uma vez que este processo se iniciou no ano passado, mas não foi finalizado em função de problemas na especificação da solução, na elaboração do ETP e do Termo de Referência. Além disso, há grande possibilidade de que não se consigam recursos orçamentários para realizar o processo no próximo ano), ela apresenta os seguintes obstáculos para sua adoção nesse momento:</p> <ul style="list-style-type: none"> • Necessidade de alocação de um servidor qualificado e com experiência na atividade de análise de sistemas e levantamento de requisitos para realizar as seguintes atividades: <ul style="list-style-type: none"> ◦ Estudar o código implementado na solução atual; ◦ Definir a forma como as regras de negócio do CTIR Gov no Tratamento e Resposta a Incidentes Cibernéticos devem ser implantadas numa nova solução; ◦ Projetar a nova solução de forma modular, especificando os requisitos e regras para cada módulo; e ◦ Calcular o total de pontos-de-função (FP) para implementação da solução, discriminando o total de pontos-de-função (FP) por módulo, a fim de que seja possível realizar o levantamento do custo de desenvolvimento dessa nova solução • É importante ressaltar que caso não seja possível alocar um servidor para realizar essas atividades, será necessária a contratação de um serviço de consultoria para a alocação de um profissional com a qualificação necessária. <ul style="list-style-type: none"> ◦ Isso implicará na elaboração de um processo de contratação de serviço, o que aumentará ainda mais o tempo para que a solução demandada seja projetada. • As atividades descritas anteriormente demandarão um tempo significativo para sua conclusão. Optando-se por esta alternativa, há a certeza de que o processo não se encerrará neste ano em função da complexidade das atividades de modelagem e cálculo de pontos-de-função que serão necessárias. <p>Pelos motivos expostos acima, a alternativa d) contratação do serviço de desenvolvimento de uma nova solução, apesar de viável tecnicamente, foi considerado inviável para a situação atual.</p>
e)	<p>A alternativa e) adquirir uma solução de mercado customizada para as necessidades do CTIR Gov é considerada tecnicamente viável em função dos seguintes aspectos:</p> <ul style="list-style-type: none"> • A equipe do CTIR Gov participou de apresentações de algumas das soluções existentes no mercado e apesar de nenhuma das soluções ter atendido integralmente as necessidades do CTIR Gov, uma delas, em especial, se mostrou bastante

alinhada com os objetivos pretendidos em virtude de já ser um barramento com possibilidade de customização com diversas aplicações de gerenciamento de tickets, incluindo o RT em qualquer versão.

- As empresas garantiram ter a capacidade de integrar suas soluções com o sistema em produção no CTIR Gov e desenvolver as customizações necessárias.
- Em função da limitação de tempo, a aquisição de uma solução customizada é um processo mais rápido que o necessário para a contratação de um serviço de desenvolvimento de uma nova solução.

É importante ressaltar alguns riscos que essa alternativa apresenta, antes mesmo da análise de risco completa, a partir do momento em que se apresenta a lista de requisitos essenciais da solução para a realização da cotação de preços pelas empresas fornecedoras:

- As empresas podem apresentar um valor para disponibilizar a solução com as customizações necessárias acima do disponível para a aquisição da solução;
- A contratada pode ser incapaz de entregar o produto com as customizações necessárias em prazo hábil em função da complexidade de alguns dos requisitos; e
- As empresas podem considerar que as customizações necessárias não são, efetivamente, possíveis para as soluções que estão ofertando, declinando então de participar do certame, o que pode levar a uma licitação deserta.

3.2 – ANÁLISE COMPARATIVA DE SOLUÇÕES

Apesar desses riscos, caso o processo logre sucesso, a aquisição de uma solução de mercado customizada garantiria a substituição da solução existente em curto prazo por um conjunto de ferramentas mais moderno, modular, e com possibilidade de evolução futura.

Considerando as limitações temporais impostas ao projeto, a equipe de planejamento da contratação escolheu a **alternativa e) adquirir uma solução de mercado customizada para as necessidades do CTIR Gov** para prosseguir o processo, por ser a única que conseguiria atender os prazos para a conclusão do processo.

Conforme consta no documento de análise de viabilidade, essa recomendação foi acatada pelo Diretor do DSI/GSI/PR, Marcelo Paiva Fontenelle em 01 de julho de 2021, que determinou o prosseguimento do processo.

Requisito	Solução	Sim	Não	Não se aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução a)			X
	Solução b)			X
	Solução c)			X
	Solução d)			X
	Solução e)			X
A Solução está disponível no Portal do Software Público Brasileiro?	Solução a)			X
	Solução b)			X
	Solução c)			X
	Solução d)			X
	Solução e)			X
A Solução é composta por software livre ou software público?	Solução a)			X
	Solução b)			X

	Solução c)	x ¹		
	Solução d)			X
	Solução e)			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução a)			X
	Solução b)			X
	Solução c)			X
	Solução d)			X
	Solução e)			X
A Solução é aderente às regulamentações da ICP-Brasil?	Solução a)			X
	Solução b)			X
	Solução c)			X
	Solução d)			X
	Solução e)			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil?	Solução a)			X
	Solução b)			X
	Solução c)			X
	Solução d)			X
	Solução e)			X

X¹ – parcialmente. Algumas das soluções adotadas pelos CSIRTs foram baseadas em software livre ou público, mas foram customizadas por equipes próprias. Outros adotaram ferramentas proprietárias.

4 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Das alternativas consideradas, foram consideradas inviáveis:

c) adoção da solução adotada por outros CSIRT;

d) contratação do serviço de desenvolvimento de uma nova solução.

Em relação a alternativa c) adoção da solução adotada por outros CSIRT, conforme visto anteriormente, a Área Demandante do GSI/PR necessita de uma solução que seja específica para as suas atividades. Logo, seria necessário estudar profundamente as soluções adotadas pelos outros CSIRT consultados, as quais já foram modificadas para atender as suas necessidades. Não existe equipe, nesse momento, disponível para essa atividade a qual demandaria longa duração.

Em relação a alternativa d) contratação do serviço de desenvolvimento de uma nova solução, apesar de ser tecnicamente viável, a inexistência de equipe capaz de realizar o levantamento de requisitos com a devida modelagem dos processos; de forma que fosse possível realizar a contagem de pontos de função, o que permitiria determinar o custo da solução. Logo, essa solução tornou-se inviável para o processo atual, especialmente em função do tempo limite para a conclusão do processo dentro do exercício de 2021.

As alternativas a) Manter a solução atual – Request Tracker e b) Substituir a solução atual por sua versão mais atualizada foram consideradas não recomendadas tecnicamente, conforme discutido anteriormente.

Cabe observar que a possibilidade da contratação da solução como um serviço em nuvem não foi sequer considerada em função da natureza das informações que são armazenadas, que expõem vulnerabilidades de diversos órgãos da administração pública federal e

em razão da necessidade da segurança dessas informações, que são consideradas pela área demandante como de acesso restrito.

5 – ANÁLISE COMPARATIVA DE CUSTOS (TCO)

Considerando que o inciso III do art. 11 da Instrução Normativa nº 1, de 4 de abril de 2019, instrui que se deve proceder a comparação de custos totais de propriedade para as soluções técnica. A equipe técnica entendeu, após estudo presente neste ETP, que, para o caso em evidência, não se aplica a análise comparativa de custos (TCO), uma vez que as alternativas a) e b) não foram recomendadas tecnicamente, a alternativa c) foi considerada inviável e a alternativa d), apesar de ser viável, não é considerada adequada em função das restrições temporais impostas ao processo.

Neste caso serão apresentados apenas os custos totais de propriedade da solução escolhida.

6 – DESCRIÇÃO DE SOLUÇÃO DE TIC A SER CONTRATADA

Solução de tecnologia de informação capaz de realizar o pré-processamento das informações recebidas das diversas fontes (sensores e agentes externos) de forma a facilitar o processo de triagem do tratamento de incidentes, conforme requisitos técnicos estabelecidos em detalhes no Anexo I – Requisitos Funcionais e Operacionais, Anexo II – Matriz de Incidentes, Anexo III – Matrizes das Regras de Negócio, e Anexo IV – Descrição das Extensões/Aplicações Existentes no RT, com garantia de suporte por 12 (doze) meses.

7 – ESTIMATIVA INICIAL DE CUSTO TOTAL DA CONTRATAÇÃO

Foram apresentadas as propostas conforme quadro a seguir:

Empresa	CNPJ	Item	Descrição	Valor unitário	Qtde	Valor Total	Validade da proposta
Harpia Tecnologia	34.460.760/0001-01	1	Solução tecnológica apta a realizar o pré-processamento das informações recebidas das diversas fontes de dados empregadas pela Área Demandante do GSI/PR (sensores e agentes externos), automatizando o processo de triagem do tratamento de incidentes, comercializada na forma de licença perpétua.	R\$6.302.557,34	1	R\$6.302.557,34	09/10/2021
Harpia Tecnologia	34.460.760/0001-01	2	Treinamento	R\$14.721,33	2	R\$29.442,66	
Valor Total da solução						R\$6.332.000,00	
AvantSec – Prestação de serviços e comércio de produtos de informática Ltda - ME	17.625.177/0001-86	1	Licença perpétua AvantData Pacote C3i2* – Resposta a Incidentes 24 meses, com serviço de customização	R\$1.850.000,00	1	R\$1.850.000,00	23/08/2021
AvantSec – Prestação de serviços e comércio de produtos de	17.625.177/0001-86	2	Treinamento	R\$20.000,00	1	R\$20.000,00	

informática Ltda - ME							
Valor Total da solução						R\$1.870.000,00	
Atech Negócios em Tecnologia S/A	11.262.624/0001-01	1	Fornecimento de solução composta por módulos do Arkhe C2 e Arkhe Data, customizados de forma a atender aos requisitos da Área Demandante do GSI/PR	R\$1.541.783,00	1	R\$1.541.783,00	26/10/2021
Atech Negócios em Tecnologia S/A	11.262.624/0001-01	2	Treinamento	R\$ 45.892,00	1	R\$ 45.892,00	
Valor Total da solução						R\$1.587.675,00	
SmartCyber Soluções em TI Ltda	22.234.780/0001-77	1	Fornecimento de solução de software Wazuh, versão 4.1.5, com licenciamento perpétuo e Open Source com código auditável, customizada de forma a atender os requisitos da Área Demandante do GSI/PR.	R\$987.715,00	1	R\$987.715,00	09/09/2021
SmartCyber Soluções em TI Ltda	22.234.780/0001-77	2	Treinamento	R\$ 34.263,46	1	R\$ 34.263,46	
Valor Total da solução						R\$ 1.021.978,46	
Média do Valor Total da Solução						R\$2.702.913,37	

Com base na tabela, considerando as propostas aceitas e os fundamentos que solidificaram os estudos realizados, a estimativa do custo total da contratação é da ordem de **R\$ 2.702.913,37 (dois milhões, setecentos e dois mil, novecentos e treze reais e trinta e sete centavos)**, conforme o valor total médio das propostas apresentadas pelas empresas Harpia Tecnologia, CNPJ 34.460.760/0001-01, AvantSec – Prestação de serviços e comércio de produtos de informática Ltda – ME, CNPJ 17.625.177/0001-86, Atech Negócios em Tecnologia S/A, CNPJ 11.262.624/0001-01 e SmartCyber Soluções em TI LTDA, CNPJ 22.234.780/0001-77.

Os recursos advêm da Ação Orçamentária 21AP, que foi disponibilizado pela Lei nº 14.144, de 22 de abril de 2021. O valor disponibilizado no Planejamento e Gerenciamento de Contratações (PAC) é de **R\$ 2.600.000,00 (dois milhões e seiscentos mil reais)**. Solicitou-se aos gestores do orçamento do Gabinete de Segurança Institucional (GSI/PR) a disponibilização do valor complementar de **R\$ 102.913,37 (cento e dois mil, novecentos e treze reais e trinta e sete centavos)** para a aquisição supracitada.

8 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

O presente estudo técnico preliminar evidenciou que a contratação garantirá o atendimento às necessidades, sendo viável do ponto de vista técnico e de negócio.

É importante ressaltar, no entanto, que, no artefato de Análise de Riscos (Nota Técnica nº 20/2021/CGGSI/DSI - 2702868), incluído no processo referenciado SEI nº 00180.000078/2021-96, verificou-se que 65% dos riscos estão na faixa crítica da relação entre probabilidade de ocorrência e impacto da ocorrência, sendo 20% considerados de altíssima gravidade e 45% de alta gravidade. Apenas 20% dos riscos foram classificados como média gravidade e os restantes 15% foram classificados como de baixa gravidade.

Além disso, verificou-se que, mais da metade dos riscos (55%), encontra-se na faixa Alto Impacto. Dentre eles, os de maior probabilidade de ocorrência são os riscos de ausência de propostas comerciais para a solução de TI pretendida; incapacidade de execução total ou parcial dos serviços pela contratada; não aquisição da solução de TI demandada dentro do exercício 2020; e incapacidade de manutenção ou evolução da solução de TI adquirida, por meio da utilização dos contratos de fábrica de software da DITEC. Esses riscos deverão ser acompanhados com maior atenção durante todo o processo de planejamento da contratação, seleção

de fornecedores e gestão contratual.

Em relação ao risco de incapacidade de execução total ou parcial dos serviços pela contratada, a probabilidade de sua ocorrência foi considerada como média-alta, uma vez que, ao contrário do que ocorre quando se desenvolve uma solução, no qual a probabilidade seria considerada como média em função da complexidade dos requisitos, a alternativa adotada prevê a customização de uma solução de TI já existente.

O que se pretende, portanto, é que uma empresa seja capaz de adaptar um código existente de seu produto, incluindo novas funcionalidades, sem impactar a solução de TI já existente. Esse tipo de atividade possui grande complexidade, pois é necessário conhecer o detalhamento do código dessa solução de TI, inclusive as relações e trocas de dados entre os módulos da solução. Dependendo-se da maneira como o código foi desenvolvido, podem ser exigidos tempo e esforços extremos, o que tornaria tal adaptação economicamente inviável para a empresa.

Em função dessas análises, é importante ressaltar que, para a alternativa escolhida, apesar de todos os esforços realizados pela Área Demandante e pela Equipe de Planejamento de Contratação, **existe a possibilidade de que o processo venha a apresentar impeditivos para a sua conclusão com o devido êxito.**

Essas conclusões a respeito do risco estão descritas no artefato de Análise de Riscos, sendo consideradas aceitáveis pelo Diretor do Departamento de Segurança da Informação, Marcelo Paiva Fontenele, que determinou a continuidade do processo.

Assim, diante do exposto acima, a contratação da solução demandada é VIÁVEL.

9 – APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 20-COFIC, de 17 de março de 2021, e pela Portaria 33-COFIC, de 09 de julho de 2021.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC, ou autoridade superior, se aplicável, conforme o § 3º do Art. 11 da IN SGD/ME nº 01, de 2019:

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
<p style="text-align: center;"> <hr/> MICHAEL GUANIERY TOMÉ DE ARAUJO 1º Sgt (EB) Matrícula SIAPE: 3089056 </p>	<p style="text-align: center;"> <hr/> SABRINA DOS PASSOS BARBOSA CC (MB) Matrícula SIAPE: 3125299 </p> <p style="text-align: center;"> <hr/> MAURÍCIO LEITE FERREIRA DA SILVA Matrícula SIAPE: 1265546 </p>

AUTORIDADE MÁXIMA DA ÁREA DE TIC e AUTORIDADE COMPETENTE

MARCELO PAIVA FONTENELE
 Matrícula SIAPE: 1046931



Documento assinado eletronicamente por **Mauricio Leite Ferreira da Silva, Assessor(a) Técnico(a)**, em 29/10/2021, às 19:37, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Michael Guaniery Tomé de Araujo, Assistente**, em 29/10/2021, às 21:19, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Sabrina dos Passos Barbosa, Assessor(a) Técnico(a) Militar**, em 08/11/2021, às 12:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Marcelo Paiva Fontenele, Diretor do Departamento de Segurança da Informação/GSI/PR**, em 12/11/2021, às 16:58, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade do documento pode ser conferida informando o código verificador **2912759** e o código CRC **606D9CBB** no site: https://sei-pr.presidencia.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0