ANEXO I - Requisitos Funcionais e Operacionais

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
1	A solução deve se integrar, via REST API, na base de dados da instância MISP (Malware Information Sharing Platform) da Área Demandante do GSI/PR e extrair os registros de eventos pertinentes a incidentes cibernéticos.	O MISP suporta a integração com outras ferramentas por meio de bibliotecas para acesso a sua API, além de módulos de expansão, exportação e importação. A lista com todos os módulos, bibliotecas e informações técnicas detalhadas está disponível no link: https://www.misp-project.org/tools/.
2	A solução deve implementar um barramento que permita a inclusão de outras fontes de coleta (interface REST ou outra). A solução deve prover uma interface de acesso ao barramento (conectores para acesso ao barramento) que organize os dados recebidos por agentes externos.	A API de comunicação deve ser usada por estes agentes na implementação do envio de informações para a Área Demandante do GSI/PR. A solução deve fornecer um modelo de implementação da API de comunicação para ser usado pelos agentes externos que desejarem compartilhar informações sobre a ocorrência de eventos cibernéticos com a Área Demandante do GSI/PR. A API deverá implementar a padronização e a classificação dos eventos. Os e-mails gerados pelas informações recebidas dos agentes externos não possuem um padrão e são considerados dados não estruturados que devem ser armazenados, separadamente, das informações pré-tratadas. Para as informações não estruturadas e armazenadas separadamente deverão ser gerados alertas. Os e-mails gerados pelos sensores são considerados estruturados por possuírem um padrão previamente definido e devem ser classificados. Para os dados pré-tratados, os respectivos *tickets* devem ser gerados.

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
2.1	A solução deve implementar todas as funcionalidades, atualmente realizadas por extensões codificadas para o RT em uma camada independente.	Operacional: (linguagem Perl, PHP e Python), incluindo a aplicação RTC (desenvolvida pelo CTIR Gov em PHP). A relação das extensões está no Anexo IV - Descrição das extensões/aplicações existentes no RT.
2.2	Todas as informações estruturadas de entrada (via barramento) devem ser armazenadas (classificadas e priorizadas) em um banco de dados independente que conterá as informações "pré-tratadas", permitindo a rápida decisão do responsável pela triagem.	Operacional: Como será feita a classificação de acordo com as Matrizes da Regra de Negócio - Anexo III.
2.3	As informações não estruturadas (não classificadas automaticamente) deverão ser encaminhadas para uma fila separada (ex: geral).	Operacional: Da fila geral podem ser selecionados eventos que devem ser re-categorizados nas filas pré-existentes adequadas pela triagem.
2.4	A solução deve decriptografar mensagens recebidas pelo correio eletrônico utilizando a chave privada da Área Demandante do GSI/PR.	Operacional: A criptografia ocorre quando qualquer agente externo ou pessoa enviar uma mensagem ao email ctir@ctir.gov.br, esta será redirecionada ao barramento usando a chave pública da Área Demandante do GSI/PR, a fim de criptografar o conteúdo do email. A criação e a manipulação das chaves pública e privada da Área Demandante do GSI/PR são feitas pelo produto GPG-GNU *Privacy Guard*. O corpo do email criptografado com a chave pública da Área Demandante do GSI/PR inicia com a linha: -----BEGIN PGP MESSAGE----- e termina com a linha: -----END PGP MESSAGE-----. O sistema deverá decifrar automaticamente as mensagens cifradas recebidas; para isso, deverá acessar a chave privada da Área Demandante do GSI/PR, armazenada em servidor interno de PKI, para extrair o texto em claro. Este texto em claro deverá ser anexado à mensagem original cifrada.
3	A solução deve prover a possibilidade de parametrização da matriz de incidentes, constante no Anexo II - Matriz de Incidentes, conforme as seguintes permissões:	

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
3.1	Permitir realizar a inclusão, a alteração (inclusive o nome) e a exclusão de incidentes e vulnerabilidades a serem tratados, juntamente com seus campos (quais) e características (quais), de maneira que o tratamento de incidentes possa ser escalável e de fácil configuração.	Conforme Anexo II - Matriz de Incidentes. Para os casos de desfiguração de sítio, coletar o *printscreen* do *site* e anexar a imagem ao respectivo *ticket,* no formato .png, com nome idêntico ao número do *ticket.* No caso de várias imagens, nomear sequencialmente (ex: 200461,200461_1 etc). Para os casos de *spamdexing,* o sistema deverá coletar *printscreen* do código fonte da página afetada nos locais onde as palavras-chave (buscadas pelos sensores) são encontradas e anexar a imagem ao respectivo *ticket,* no formato .png, com nome idêntico ao número do *ticket.* Adotar, para o caso de várias imagens, o procedimento do exemplo anterior. As condições a serem implementadas com relação aos tipos de incidente X estão no campo "Log Content", campo que contém as evidências de vulnerabilidades que são coletadas a partir de testes efetuados por sensores e são enviadas como log ao final da notificação para orientar o dono do ativo e detalhar o que foi detectado. Essa atualização deverá ser automatizada o máximo possível. A empresa deve fazer a leitura da regra de negócio atualmente implementada nas filas de *tickets,* de acordo com o Anexo III - Matrizes da Regra de Negócio, para implementar corretamente as evidências coletadas atualmente. A empresa deve avaliar as funcionalidades do sistema atual para desacoplar o processamento dos dados do sistema de gestão de tickets.
3.2	Permitir a categorização dos incidentes e vulnerabilidades, de maneira agrupada ou individual, por classe de prioridade de incidente.	Uma fila com os campos previstos no Anexo II - Matriz de Incidentes. Recategorização por classe de prioridade do incidente, bem como a inclusão, a alteração e a exclusão da classe de prioridade para o incidente deverá funcionar como uma alteração de campo do incidente ou da vulnerabilidade.(Anexo II - Matriz de Incidentes).
4	A solução deve prover a possibilidade de inclusão, alteração e exclusão de órgãos, com seus respectivos campos e fornecer as seguintes funcionalidades de parametrização:	Conforme Anexo III - Matrizes da Regra de Negócio.
4.1	Deverá ser possível categorizar os órgãos por classe de prioridade, de maneira agrupada ou individual.	Conforme Anexo III - Matrizes da Regra de Negócio.

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
4.2	A categorização por classe de prioridade do órgão, bem como a inclusão, a alteração e a exclusão da classe de prioridade, deverá funcionar como uma alteração de campo do órgão.	Conforme Anexo III - Matrizes da Regra de Negócio.
5	A solução deve prover a possibilidade de visualização e alteração, por meio de uma interface ou ambiente amigável, da matriz de prioridade de incidentes cruzada com a matriz de prioridade de órgãos, que resultará na matriz de prioridade de tratamento de incidentes utilizada pelo responsável pela triagem e pela análise.	Conforme Anexo III - Matrizes da Regra de Negócio.
6	A solução deve prover a visualização das informações existentes, em tempo real, organizadas por prioridade de tratamento, como resultado da implementação da matriz de prioridade para tratamento de incidentes.	Conforme Anexo III - Matrizes da Regra de Negócio.
7	A solução deve fornecer um ambiente de gerenciamento de contatos independente, que funcione de maneira integrada com as ações de tratamento de incidentes para o envio de alertas e notificações.	Implementação de um ambiente de gerenciamento de contatos independente preferencialmente em banco de dados. Ao gerar a notificação, o sistema deverá acessar o sistema de contatos para selecionar o contato específico do caso). Alertas por e-mail, Telegram ou outro serviço de mensageria. Definir tipos de contatos (ex: autoridades ou definição de outros grupos). Deverá ser possível agrupar os contatos por organização, por domínios ou por faixas de IP.
7.1	Deverá ser possível inserir, excluir ou modificar os contatos.	A edição dos dados devem ser feitas tanto manualmente quanto atualizadas automaticamente em horário definido, utilizando a base do *whois.* Operacional: As informações de contato, além da manipulação manual, devem ser extraídas utilizando a aplicação *whois.*
7.2	As informações de contato também deverão estar disponíveis para uso por outras aplicações.	Operacional: Ser acessível via API por outras aplicações para a gestão dos contatos; ter acesso via web à base de contatos, independente de dispositivo (responsivo).

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
8	A interface dos analistas deve organizar visualmente os dados processados no barramento, de maneira a permitir a rápida avaliação do responsável pela triagem e o rápido acionamento do órgão envolvido. A solução deve organizar automaticamente os *tickets* e os alertas com base na matriz de priorização, que deve ser implementada.	Operacional: deve aparecer, como é priorizado, classificado, correlacionado (item 11), falsos positivos, campos personalizados. Dominio URL, IP, repetidos e os não-classificados. Os *tickets* também devem ser apresentados, correlacionados com outros *tickets* em possíveis ataques cibernéticos.
9	A solução deve implementar o reconhecimento e a classificação de eventos, automaticamente, com base na matriz de incidentes, pela leitura/interpretação das informações contidas nos e-mails recebidos.	A funcionalidade deve ter a mesma operacionalização atualmente implementada em uma extensão no RT chamada RT-Client.
10	A solução deve organizar automaticamente os *tickets* e os alertas com base na matriz de priorização, que deve ser implementada.	Conforme Anexo III - Matrizes da Regra de Negócio.
10.1	A matriz de priorização (OP) (anexar o modelo) a ser implementada deve possibilitar alterações em decorrência do contexto situacional (parametrização).	Conforme Anexo III - Matrizes da Regra de Negócio.
10.2	A matriz de priorização deverá permitir que os órgãos sejam inseridos ou retirados de uma classe de prioridade, eventos podem ser inseridos ou retirados de determinada classe de prioridade.	Conforme Anexo III - Matrizes da Regra de Negócio.
10.3	Os *tickets* devem ser apresentados, além de priorizados, correlacionados com os atores externos envolvidos (agentes maliciosos, quando for o caso).	Operacional: Deseja-se que seja possível consultar no histórico do sistema quais agente externos estão atacando que órgãos; e que órgãos estão sendo atacados por quais grupos.

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
11	A solução deve prover funcionalidade que facilite a coleta de evidências e sua correlação com o respectivo *ticket* (para cada tipo de incidente, relacionar o tipo de evidência). Essa evidência deve ser coletada em uma etapa de pré-processamento (enriquecimento), após a entrada no barramento e antes de ser apresentado ao analista.	Conforme Anexo II - Matriz de Incidentes. Para os casos de desfiguração de sítio, coletar o *printscreen* do site e anexar a imagem ao respectivo *ticket,* no formato .png, com nome idêntico ao número do *ticket.* No caso de várias imagens, nomear sequencialmente (ex: 200461,200461_1 etc). Para os casos de *spamdexing,* o sistema deverá coletar *printscreen* do código fonte da página afetada, nos locais onde as palavras-chaves (buscadas pelos sensores) são encontradas e anexar a imagem ao respectivo *ticket,* no formato .png, com nome idêntico ao número do *ticket.* Adotar, para o caso de várias imagens, o procedimento do exemplo anterior. As condições a serem implementadas com relação aos tipos de incidente X situação estão no campo “Log Content”, campo que contém as evidências de vulnerabilidades coletadas a partir de testes efetuados por sensores e enviadas como log ao final da notificação para orientar o dono do ativo e detalhar o que foi detectado. Essa atualização deverá ser automatizada o máximo possível. A empresa deve fazer a leitura da regra de negócio atualmente implementada nas filas de tíquetes, de acordo com o Anexo III - Matrizes da Regra de Negócio, para implementar corretamente as evidências coletadas atualmente. A empresa deve avaliar as funcionalidades do sistema atual para desacoplar o processamento dos dados do sistema de gestão de *tickets.*
12	A solução deve gerar automaticamente os tickets desdobrados (tickets filhos) quando for possível identificar que o evento possui desdobramentos. como, por exemplo, varias URLs de um mesmo sitio (mesmo domínio) em um mesmo e-mail com origem nos sensores.	
12.1	Um *ticket* possuirá desdobramento se um e-mail contendo várias URLs (mesmo domínio) com defacement;	

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
12.2	Um *ticket* possuirá desdobramento se um email possuir vários sites do governo com vulnerabilidade SSL;	
12.3	Um *ticket* possuirá desdobramento se um e-mail do CERT.br contiver vários endereços de e-mails de diferentes órgãos de governo que estão disseminando *spam.*	
13	A solução deve tratar os dados coletados no sentido de identificar e eliminar as duplicações de *tickets* (mesma URL, domínio e endereço IP), referentes ao mesmo problema, que chegam por meio dos sensores e dos agentes externos (CDCiber e CERT.br).	
13.1	Os *tickets* devem ser agrupados por tipo de evento/vulnerabilidade, criando um *ticket* principal para cada grupo, mantendo as demais ocorrências repetidas somente como referências ao principal evitando que os tickets repetidos entre nas estatísticas.	
13.2	Para o caso de *tickets* duplicados mas com datas diferentes (ex: um mesmo evento, não tratado, é novamente reportado gerando um *ticket)* , a solução deve correlacionar o ticket novo com o ticket mais antigo. As datas originais de cada *ticket* devem ser mantidas.	
13.3	Um *ticket* fechado deve ser correlacionado apenas para referência.	
14	A solução deve encadear e relacionar as notificações para um mesmo órgão, de *tickets* abertos (considerados ainda em tratamento) de maneira a permitir que o órgão em questão possa entender o contexto da situação em determinado espaço temporal.	
14.1	A solução deve fornecer mecanismo de busca, por órgão, evento/vulnerabilidade, que permita a fácil compreensão da situação com relação aos *tickets* encadeados.	
14.2	Os *tickets* fechados devem ser relacionados possibilitando a geração de um registro histórico.	
15	A solução deve realizar o envio automático de alertas, por e-mail, para os órgãos envolvidos com base nas informações coletadas e prioridade atribuída de acordo com modelos de texto específicos para cada situação.	

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados		
Requisitos Funcionais		**Requisitos Operacionais**
15.1	A solução deve permitir a inclusão, alteração e exclusão de modelos de alerta. Os e-mail utilizados serão os existentes na base de contatos independente.	
16	A solução deve automatizar a mudança do status do ticket com base na matriz de classificação x status, como por exemplo, se um *ticket* é classificado como falso positivo automaticamente é atribuído o status de rejeitado.	
17	A solução deve fornecer mecanismos para gerar estatísticas sobre os eventos, alertas, notificações, falsos positivos etc., com base em parâmetros dinâmicos como tipo de incidente xXlocalidade, tipo de incidente X órgão da APF entre outras correlações. Estas relações deverem ser customizáveis.	Devem ser implementadas no mínimo as que estão no site do CTIR Gov, URL: https://www.ctir.gov.br/. A solução para geração de estatísticas, deve ser preferencialmente, *open source* . (caso a empresa não possua nenhuma ferramenta de BI já incorporadana solução, é desejável que a futura ferramenta de BI seja o QuickSense). A solução deve permitir a visualização e emissão de relatórios, de forma customizada por seleção de atributos, nos formatos: .pdf, .html, .odt. A solução deve permitir a seleção de períodos customizáveis para a geração dos relatório, além de possibilitar correlações com outros períodos similares anteriores. A solução deve poder exportar dados nos formatos: .csv, .json, .ods (odf) e .xml, entre outros que poderão ser sugeridos entre outros que poderão ser sugeridos e incorporados.
18	A solução deve apresentar de forma gráfica a associação entre cracker X publicações realizadas pelo criminoso na internet relacionadas com os incidentes que estão no sistema.	

Anexos a este documento:

Anexo II - Matriz de Incidentes

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados	
Requisitos Funcionais	**Requisitos Operacionais**

Anexo III - Matrizes da Regra de Negocio

Anexo IV - Descrição das extensões/aplicações existentes no RT

ANEXO II – MATRIZ DE INCIDENTES

MATRIZ DE INCIDENTES DE REDES										
		Informações								
Nº	Tipos e subtipos de Incidentes	IP	Dominio	URL	Snapshot	Tag	Arquivo / Código	Logs	Corpo Email	Cabeçalho Email
1	Abuso de Sítio									
1.1	Desfiguração de Sitio									
1.2	Conteudo Incompativel									
1.3	Redirecionamento de Pagina									
1.4	Exposição de Codigo									
1.5	Spamdexing									
1.6	Listagem de Diretorio									
1.7	Abuso de Forum / Comentarios									
1.8	Cross Site Scripting (XSS)									
1.9	Possivel Vulnerabilidade									
1.10	Possivel Vulnerabilidade - JBOSS									
2	Analise de Malware									
3	Indisponibilidade de Sítio									
4	Páginas Falsa									
5	Ransoware									
6	Scans									
7	Vazamento de Informação									
7.1	Exposição de Dados Sensiveis									
7.2	Possivel Vazamento de Informação									
7.3	Vazamento de Email Institucional									
7.4	Vazamento de Email Institucional (Personalizado)									
				Informações necessárias que devem ser coletadas						

Os eventos representados na matriz acima não se esgotam; ainda, existem os tipos de incidentes/vulnerabilidades que serão tratados pela Área Demandante do GSI/PR.

As outras informações serão detalhadas e refinadas posteriormente.

Tipos de Incidentes, Pesos e Criticidade

Tipos de incidentes	Peso
abuso de sítios (desfiguração, spamdexing, XSS, Sql injection)	5
inclusão remota de arquivos	5
uso abusivo de servidores de e-mail	5
Botnet	5
Código malicioso	3
hospedagem ou redirecionamento de artefatos ou código malicioso	3
ataques de negação de serviço (DOS, DDOS)	5
acesso não autorizado a sistemas ou dados	5
varredura de portas	1
comprometimento de computadores ou redes	5
desrespeito à política de segurança ou uso inadequado dos recursos	1
ataques de engenharia social - phishing	1
cópia e distribuição não autorizada de material protegido por direitos	1
uso abusivo ou indevido de redes sociais para difamação, calúnia,	3
Abuso de DNS	5
Ransomware	5
Outros	1

Código de criticidade	Criticidade do incidente	Peso
C5	Altíssima	5
C4	Alta – sem possibilidade de propagação	4
C3	Média – com possibilidade propagação	3
C2	Média – sem possibilidade de propagação	2
C1	Baixa	1
Obs: Peso maior é mais crítico		

Tipos de Órgãos e Pesos		
Código de prioridade de órgão	**Prioridade definida**	**Peso**
APF1	Órgão da APF – Alta Prioridade	6
APF2	Órgão da APF – Média Prioridade	5
APF3	Órgão da APF – Baixa Prioridade	4
NAPF1	Entidade não-pertencente à APF – Alta Prioridade	3
NAPF2	Entidade não-pertencente à APF – Média Prioridade	2
NAPF3	Entidade não-pertencente à APF – Baixa Prioridade	1
Obs1: Peso maior é mais prioritário		

Exemplos de órgãos e pesos	
e-mail - órgão	**Peso**
alguem@orgao1.gov.br	6
alguem@orgao2.gov.br	6
alguem@orgao3.gov.br	6
alguem@orgao4.gov.br	6
alguem@orgao5.gov.br	6
alguem@orgao6.gov.br	5
alguem@orgao7.gov.br	5
alguem@orgao8.gov.br	5
alguem@orgao9.gov.br	4
alguem@orgao10.gov.br	4
alguem@orgao11.gov.br	3
alguem@orgao12.gov.br	3
alguem@orgao13.gov.br	2
alguem@orgao14.gov.br	2
alguem@orgao15.gov.br	1
alguem@orgao16.gov.br	1
OUTROS E-MAILS	1

Cálculo da Prioridade			
Cálculo da Prioridade = Peso Órgão x Peso do tipo de incidente			
Cálculo da Prioridade			
Se o cálculo for igual maior que	Nível de prioridade final	Código da Prioridade	Ação
25	Altíssima	P5	Relação órgão x incidente por ordem de prioridade
20	Alta	P4	Envio de alerta incidente prioritário aos integrantes CTIR
15	Média	P3	Envio de alerta ao órgão
10	Baixa	P2	Modelos de informação
5	Baixíssima	P1	Mudança de status do evento/incidente

Regra de Priorização por Órgão					
Tipo de órgão	**Gravidade do Incidente**				
	C1	**C2**	**C3**	**C4**	**C5**
APF1	P1	P2	P3	P4	P5
APF2	P1	P2	P4	P5	P5
APF3	P1	P2	P4	P5	P5
NAPF1	P1	P3	P4	P5	P5
NAPF2	P1	P3	P4	P5	P5

ANEXO IV – DESCRIÇÃO DAS EXTENSÕES/APLICAÇÕES EXISTENTES NO RT

Nome da extensão/aplicação	Descrição	Linguagem
CtirGov-RTx-Install	Extensão básica para carregar os dados e scripts básicos da "AreaDemandanteGSIPR"-RT. É a extensão mais importante da customização do RT e consolida todos os scripts da versão anterior (3.8.8)	Perl
CtirGov-RTx-Cli	Extensão que amplia as capacidades da extensão RT-REST. É consumida pela ferramenta chamada RT-Client	Perl
RT-Client	Cria um Command Line Interface (CLI) para ser um meio adicional de integrar com uma instancia do RT. O servidor RT deve possuir duas extensões: RT-Extension-REST (desenvolvida pelo fabricante) e "AreaDemandanteGSIPR"-RTx-Cli. Essa extensão é muito importante para a atividade da triagem, permitindo manipular tíquetes, realizar decriptografia, criar filhos (desdobramentos) de tickets automaticamente, realizar verificações, etc.	PHP
Sensor RB-Twitter	Busca postagens de divulgação de incidentes, normalmente abuso de sítios, vazamento e ataques de negação de serviços.	Perl
Sensor RB-Zone-H	Busca, no site http://www.zone-h.org/ ocorrências contendo referências aos domínios do governo brasileiro. O site Zone-H é utilizado por hackers para divulgar abuso de sítios.	Perl
Sensor RB-Google-CSE	Busca, através do google, abusos de sítio.	Perl
Sensor RB-Website-Tester	Verifica a disponibilidade de websites visando identificar ataques DDos. Atualmente desativado.	Perl
ETL	Implementa o processo de Extract-Transform-Load da base do RT para o formato DW, a ser utilizado inicialmente para uso no site EmNumeros, e posteriormente numa ferramenta de BI.	PHP
CtirGov-Common	Inclui uma coleção de sub-rotinas uteis para os diversos módulos.	Perl
CtirGov-Bot	Biblioteca usada por todos os sensores.	Perl
CtirGov-RTx-Clipboard	Extensão do RT que inclui botões para facilmente copiar textos. Basicamente faz a cópia da notificação a ser enviada pelo analista.	Perl
CtirGov-RTx-Correlate	Refatora a lógica dos tickets relacionados, utilizando o rtx-install criando um quadro que exibe todos os tickets correlatos ao ticket atual.	Perl
Dns-recursivo-aberto	Busca por servidores DNS com recursivo aberto	Python
Shadow Server	Envia diariamente informações sobre 80 tipos de vulnerabilidades em redes nacionais. 14 tipos são enviados automaticamente para a triagem.	N/A Externo

ANEXO V – Etapas da Implementação

a. Módulos x Atividades, Customizações e Artefatos Obrigatórios

Módulos	ATIVIDADES, CUSTOMIZAÇÕES E ARTEFATOS
1	**Fase 1 - Integração:**
	A solução deve implementar um barramento que permita a inclusão de outras fontes de coleta (interface REST ou outra). A solução deve prover uma interface de acesso ao barramento (conectores para acesso ao barramento) que organize os dados recebidos por agentes externos.
	A solução deve implementar todas as funcionalidades atualmente realizadas, por extensões codificadas para o RT em uma camada independente (Anexo X).
	A solução deve se integrar, via REST API, na base de dados da instância MISP (*Malware Information Sharing Platform*) da Área Demandante do GSI/PR e extrair os registros de eventos pertinentes a incidentes cibernéticos.
	Fase 2 – Tratamento das informações recebidas:
	Todas as informações estruturadas de entrada, via barramento, devem ser armazenadas, classificadas e priorizadas, de acordo com as regras de negócio, em um banco de dados independente que conterá as informações "pré-tratadas", permitindo a rápida decisão do responsável pela triagem. Nesta fase, faz-se necessária a codificação das Matrizes de Regras de Negócio que se encontram no Anexo III.
	As informações não estruturadas (não classificadas automaticamente) deverão ser encaminhadas para uma fila separada (ex: não classificada).
	A solução deve descriptografar mensagens recebidas pelo correio eletrônico utilizando a chave privada da Área Demandante do GSI/PR.
	Fase 3 – Organização de tickets automatizada:
	A solução deve gerar automaticamente os *tickets* desdobrados (*tickets* filhos) quando for possível identificar que o evento possua desdobramentos, como várias URLs de um mesmo sítio (mesmo domínio) em um mesmo *e-mail* com origem nos sensores.
	Um *ticket* possuirá desdobramento se um e-mail contendo várias URLs (de governo) com *defacement*.
	Um *ticket* possuirá desdobramento se um e-mail possuir vários sites do governo com vulnerabilidade SSL;
	Um *ticket* possuirá desdobramento se um e-mail do CERT.br contiver vários endereços de e-mails de diferentes órgãos de governo que estão disseminando *spam*.
	A solução deve tratar os dados coletados no sentido de identificar e eliminar as duplicações de *tickets* (mesma URL, domínio, e endereço IP) referentes ao mesmo problema, que chegam por meio dos sensores e dos agentes externos (CDCiber e CERT.br) e os que já se encontram cadastrados no próprio sistema de *tickets*.
	Os *tickets* devem ser agrupados por tipo de evento/vulnerabilidade, criando um *ticket* principal para cada grupo, mantendo as demais ocorrências repetidas somente como referências ao principal, evitando que os *tickets* repetidos entrem nas estatísticas.
	Para o caso de *tickets* duplicados, mas com datas diferentes (ex: um mesmo evento, não tratado, é novamente reportado gerando um ticket), a solução deve correlacionar o *ticket* novo com o mais antigo. As datas originais de cada *ticket* devem ser mantidas. Um *ticket* fechado deve ser correlacionado apenas para referência.
	A solução deve encadear e relacionar as notificações para um mesmo órgão, de *tickets* abertos (considerados ainda em tratamento), de maneira a permitir que o órgão em questão possa entender o contexto da situação em determinado espaço temporal.
	A solução deve fornecer mecanismo de busca, por órgão, evento/vulnerabilidade, que permita a fácil compreensão da situação com relação aos *tickets* encadeados.

2	**Fase 4 – Customização da Matriz de priorização de Incidentes:**
	A solução deve prover a possibilidade de parametrização da matriz de incidentes, constante no Anexo II, além de: • permitir realizar a inclusão, a alteração (inclusive do nome) e a exclusão de incidentes e vulnerabilidades a serem tratados, juntamente com seus campos (quais) e características (quais), de maneira que o tratamento de incidentes possa ser escalável e de fácil configuração; • permitir a categorização dos incidentes e vulnerabilidades, de maneira agrupada ou individual, por classe de prioridade de incidente.
	A solução deve prover a possibilidade de inclusão, alteração e exclusão de órgãos, com seus respectivos campos e fornecer funcionalidades de parametrização, além de: • ser possível categorizar os órgãos por classe de prioridade, de maneira agrupada ou individual; • permitir a categorização por classe de prioridade do órgão, bem como a inclusão, a alteração e a exclusão da classe de prioridade deverá funcionar como uma alteração de campo do órgão.
	A solução deve prover a possibilidade de visualização e de alteração, por meio de uma interface ou de um ambiente amigável, da matriz de prioridade de incidentes cruzada com a matriz de prioridade de órgãos, a qual resultará na matriz de prioridade de tratamento de incidentes utilizada pelo responsável pela triagem e pela análise.
	A solução deve prover a visualização das informações existentes, em tempo real, organizadas por prioridade de tratamento, como resultado da implementação da matriz de prioridade para tratamento de incidentes.
	A interface dos analistas deve organizar visualmente os dados processados no barramento, visualmente, de maneira a permitir a rápida avaliação do responsável pela triagem e o rápido acionamento do órgão envolvido. A solução deve organizar automaticamente os *tickets* e os alertas com base na matriz de priorização, que deve ser implementada.
	A matriz de priorização a ser implementada deve possibilitar alterações em decorrência do contexto situacional (parametrização).
	A matriz de priorização deverá permitir que os órgãos sejam inseridos ou retirados de uma classe de prioridade, eventos podem ser inseridos ou retirados de determinada classe de prioridade.
	Etapa 5 – Classificação automatizada:
	A solução deve implementar o reconhecimento e a classificação de eventos, automaticamente, com base na matriz de incidentes, pela leitura e interpretação das informações contidas nos e-mails recebidos.
	A solução deve organizar automaticamente os *tickets* e os alertas com base na matriz de priorização que deve ser implementada.
	Os *tickets* devem ser apresentados, além de priorizados, correlacionados com os atores externos envolvidos (agentes maliciosos, quando for o caso).
	Etapa 6 – Coleta de evidências:
	A solução deve prover funcionalidade que facilite a coleta de evidências e a sua correlação com o respectivo *ticket* (para cada tipo, relacionar o tipo de evidência). Essa evidência deve ser coletada em uma etapa de pré-processamento (enriquecimento), após o barramento e antes de ser apresentado ao analista.
	A solução deve apresentar de forma gráfica a associação entre cracker X publicações realizadas pelo criminoso na internet relacionadas com os incidentes que estão no sistema (isso não é um requisito).
3	**Etapa 7 – Gerenciamento de contatos:**
	A solução deve fornecer um ambiente independente de gerenciamento de contatos que funcione de maneira integrada com as ações de tratamento de incidentes para o envio de alertas e notificações.
	Deverá ser possível inserir, excluir ou modificar os contatos.
	As informações de contato também deverão estar disponíveis para uso por outras aplicações.
4	**Etapa 8 – Alertas automáticos:**
	A solução deve realizar o envio automático de alertas, por e-mail, para os órgãos envolvidos com base nas informações coletadas e com prioridade atribuída de acordo com modelos de texto específicos para cada situação.
	A solução deve permitir a inclusão, a alteração e a exclusão de modelos de alerta. Os e-mails utilizados serão os existentes na base de contatos independente.
	Etapa 9 – Geração de estatísticas:

	A solução deve fornecer mecanismos para gerar estatísticas sobre eventos, alertas, notificações, falsos positivos, resolvidos, pendentes, rejeitados, não resolvidos etc., com base em parâmetros dinâmicos como tipo de incidente x localidade, tipo de incidente x órgão da APF entre outras correlações. Estas relações deverem ser customizáveis.
	Etapa 10 – Geração de Relatórios:
	Relatório de Notificações, Incidentes e Vulnerabilidades X resolvidos, pendentes, rejeitados, não resolvidos.
	Relatório de Incidentes/Vulnerabilidades por órgão da APF.
	Relatório de Incidentes/Vulnerabilidades por Estado.
	Relatório de Incidentes/Vulnerabilidades por Esfera (Executivo, Legislativo e Judiciário).
	Relatório de Notificações enviadas/recebidas de outros países.
	Relatório de Tempo de Resolução dos Incidentes/Vulnerabilidades.
	Relatório de subtipos de Desfiguração de Sítios.
	Relatório de Top 10 Hackers envolvidos em incidentes governamentais.
	Relatório de Top 10 tipos de incidentes governamentais.
	OBS: Todos relatórios devem prover filtro de períodos

b. Prazo para Entrega dos Módulo

O prazo máximo para entrega de todos os módulos previstos neste anexo é de **8 (oito) meses**.

ANEXO VI – TERMO DE ACEITE DE INSTALAÇÃO E CONFIGURAÇÃO

TERMO DE ACEITE DE INSTALAÇÃO E CONFIGURAÇÃO

Processo Administrativo nº: _____

Objeto: _____

Nº do Contrato: _____

Contratada: _____

CNPJ: _____

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 140, inciso II, alínea "a", da Lei nº 14.133, de 1º de abril de 2021, e no artigo 33, inciso VIII, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 e suas alterações, que:

a) Todos os módulos previstos para entrega pela CONTRATADA foram homologados pela equipe técnica da CONTRATANTE;
b) A CONTRATADA instalou e configurou, sob supervisão de analistas da CONTRATANTE, a solução objeto da contratação e que não foram constatadas anormalidades ou problemas durante a verificação de conformidade desse serviço; e
c) Os bens e/ou serviços relacionados no quadro abaixo possuem as quantidades e a qualidade compatível com as condições e exigências constantes do Edital de Pregão Eletrônico n° ____/____.

Item	Descrição	Identificação	Unidade	Qtde

Local/UF, data

Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante da Área Requisitante
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante Legal da Empresa
Cargo
CPF

ANEXO VII – TERMO DE RECEBIMENTO DEFINITVO

TERMO DE RECEBIMENTO DEFINITVO

Processo Administrativo nº: _____

Objeto: _____

Nº do Contrato: _____

Contratada: _____

CNPJ: _____

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 140, inciso II, alínea “b”, da Lei nº 14.133, de 1º de abril de 2021, e no artigo 33, inciso VIII, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 e suas alterações, que os bens e/ou serviços relacionados no quadro abaixo possuem as quantidades e a qualidade compatível com as condições e exigências constantes do Edital de Pregão Eletrônico n° ____/____.

Item	Descrição	Identificação	Unidade	Qtde

Local/UF, data

Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante da Área Requisitante
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante Legal da Empresa
Cargo
CPF

ANEXO VIII – TERMO DE RECEBIMENTO PROVISÓRIO

TERMO DE RECEBIMENTO PROVISÓRIO

Processo Administrativo nº: _____

Objeto: _____

Nº do Contrato: _____

Contratada: _____

CNPJ: _____

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 140, inciso II, alínea "a", da Lei nº 14.133, de 1º de abril de 2021, e no artigo 33, inciso I, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 e suas alterações, que os bens e/ou serviços relacionados no quadro abaixo foram recebidos pelo agente responsável.

Item	Descrição	Identificação	Unidade	Qtde

Ressaltamos que o recebimento definitivo dos bens e/ou serviços ocorrerá conforme previsto no Termo de Referência e no instrumento contratual proveniente do Edital de Pregão Eletrônico SRP n° ____/____.

Local/UF, data

Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante da Área Requisitante
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante Legal da Empresa
Cargo
CPF

ANEXO IX – AVALIAÇÃO DA CAPACITAÇÃO

a. Formulário de Avaliação da Capacitação - Capacitação Presencial

Nº do Contrato: _____

Contratada: _____ CNPJ: _____

Período da Capacitação: ___/___/___ a ___/___/___ Carga horária total: ____ h

Instrutor: _____

Nome do Treinando: _____ Matrícula: _____

Tópicos de Avaliação	**Nota (1 – Insatisfatório 10 – Excelente)**									
Programa e Metodologia	1	2	3	4	5	6	7	8	9	10
O significado e a importância do tema do treinamento foram compreendidos e abordados adequadamente.										
Os tempos destinados à apresentação e exploração dos conteúdos de cada tópico foram suficientes.										
De uma maneira geral os objetivos do evento foram alcançados.										
Instrutoria	1	2	3	4	5	6	7	8	9	10
O instrutor conhece os temas tratados e os apresentou de forma objetiva, organizada, segura e fluente.										
O instrutor incentivou o envolvimento dos participantes nas atividades do treinamento.										
O instrutor esclareceu adequadamente as questões e dúvidas dos participantes.										
Organização	1	2	3	4	5	6	7	8	9	10
As técnicas didáticas utilizadas foram adequadas para abordar os objetivos propostos.										
A qualidade dos recursos e materiais didáticos utilizados foi satisfatória.										
Autoavaliação	1	2	3	4	5	6	7	8	9	10
Os conhecimentos adquiridos foram suficientes para cumprir os objetivos propostos.										
Os conhecimentos adquiridos são úteis, importantes e serão aplicados na utilização da solução.										
O treinamento sugeriu formas de aplicação prática dos conteúdos abordados.										

b. Formulário de Avaliação da Capacitação - Capacitação on-line

Nº do Contrato: _____

Contratada: _____ CNPJ: _____

Período da Capacitação: ___/___/___ a ___/___/___ Carga horária total: ____ h

Instrutor: _____

Nome do Treinando: _____ Matrícula: _____

Tópicos de Avaliação	**Nota (1 – Insatisfatório 10 – Excelente)**									
Programa e Metodologia	1	2	3	4	5	6	7	8	9	10
O significado e a importância do tema do treinamento foram compreendidos e abordados adequadamente.										
Os tempos destinados à apresentação e exploração dos conteúdos de cada tópico foram suficientes.										
De uma maneira geral os objetivos do evento foram alcançados.										
Instrutoria	1	2	3	4	5	6	7	8	9	10
O instrutor conhece os temas tratados e os apresentou de forma objetiva, organizada, segura e fluente.										
O instrutor incentivou o envolvimento dos participantes nas atividades do treinamento.										
O instrutor esclareceu adequadamente as questões e dúvidas dos participantes.										
Organização	1	2	3	4	5	6	7	8	9	10
As técnicas didáticas utilizadas foram adequadas para abordar os objetivos propostos.										
A qualidade dos recursos e materiais didáticos utilizados foi satisfatória.										
As condições e configuração do ambiente virtual de treinamento foram adequadas (conexão estável, áudio e imagem sem falhas etc).										
Autoavaliação	1	2	3	4	5	6	7	8	9	10
Os conhecimentos adquiridos foram suficientes para cumprir os objetivos propostos.										
Os conhecimentos adquiridos são úteis, importantes e serão aplicados na utilização da solução.										
O treinamento sugeriu formas de aplicação prática dos conteúdos abordados.										

ANEXO X – RELATÓRIO CONSOLIDADO DA AVALIAÇÃO DA CAPACITAÇÃO

a. Relatório Consolidado de Avaliação da Capacitação - Capacitação Presencial

Nº do Contrato: _____

Contratada: _____ CNPJ: _____

Período da Capacitação: ___/___/___ a ___/___/___ Carga horária total: ____ h

Instrutor: _____

Total de Treinandos: _____

Total de Treinandos com no mínimo 75% de frequência: ____

Tópicos de Avaliação		
Programa e Metodologia	**Média do Item**	**Média do Tópico**
O significado e a importância do tema do treinamento foram compreendidos e abordados adequadamente.		
Os tempos destinados à apresentação e exploração dos conteúdos de cada tópico foram suficientes.		
De uma maneira geral os objetivos do evento foram alcançados.		
Instrutoria	**Média do Item**	**Média do Tópico**
O instrutor conhece os temas tratados e os apresentou de forma objetiva, organizada, segura e fluente.		
O instrutor incentivou o envolvimento dos participantes nas atividades do treinamento.		
O instrutor esclareceu adequadamente as questões e dúvidas dos participantes.		
Organização	**Média do Item**	**Média do Tópico**
As técnicas didáticas utilizadas foram adequadas para abordar os objetivos propostos.		
A qualidade dos recursos e materiais didáticos utilizados foi satisfatória.		
Autoavaliação	**Média do Item**	**Média do Tópico**
Os conhecimentos adquiridos foram suficientes para cumprir os objetivos propostos.		
Os conhecimentos adquiridos são úteis, importantes e serão aplicados na utilização da solução.		
O treinamento sugeriu formas de aplicação prática dos conteúdos abordados.		
MÉDIA FINAL DA TURMA (DESCONSIDERADA A MÉDIA DO TÓPICO AUTOAVALIAÇÃO)		

Em função das médias obtidas, o resultado da capacitação foi considerado **SATISFATÓRIO / INSATISFATÓRIO**.

Local e data

_____

Nome – matrícula

Gestor do Contrato

b. Relatório Consolidado de Avaliação da Capacitação - Capacitação on-line

Nº do Contrato: _____

Contratada: _____ CNPJ: _____

Período da Capacitação: ___/___/___ a ___/___/___ Carga horária total: ____ hs

Instrutor: _____

Total de Treinandos: _____

Total de Treinandos com no mínimo 75% de frequência: ____

Tópicos de Avaliação		
Programa e Metodologia	**Média do Item**	**Média do Tópico**
O significado e a importância do tema do treinamento foram compreendidos e abordados adequadamente.		
Os tempos destinados à apresentação e exploração dos conteúdos de cada tópico foram suficientes.		
De uma maneira geral os objetivos do evento foram alcançados.		
Instrutoria	**Média do Item**	**Média do Tópico**
O instrutor conhece os temas tratados e os apresentou de forma objetiva, organizada, segura e fluente.		
O instrutor incentivou o envolvimento dos participantes nas atividades do treinamento.		
O instrutor esclareceu adequadamente as questões e dúvidas dos participantes.		
Organização	**Média do Item**	**Média do Tópico**
As técnicas didáticas utilizadas foram adequadas para abordar os objetivos propostos.		
A qualidade dos recursos e materiais didáticos utilizados foi satisfatória.		
As condições e configuração do ambiente virtual de treinamento foram adequadas (conexão estável, áudio e imagem sem falhas etc).		
Autoavaliação	**Média do Item**	**Média do Tópico**
Os conhecimentos adquiridos foram suficientes para cumprir os objetivos propostos.		
Os conhecimentos adquiridos são úteis, importantes e serão aplicados na utilização da solução.		
O treinamento sugeriu formas de aplicação prática dos conteúdos abordados.		
MÉDIA FINAL DA TURMA (DESCONSIDERADA A MÉDIA DO TÓPICO AUTOAVALIAÇÃO)		

Em função das médias obtidas, o resultado da capacitação foi considerado **SATISFATÓRIO / INSATISFATÓRIO**.

Local e data

_____

Nome – matrícula

Gestor do Contrato

ANEXO XI – TERMO DE ACEITE DA CAPACITAÇÃO

TERMO DE ACEITE DA CAPACITAÇÃO

Processo Administrativo nº: _____

Objeto: _____

Nº do Contrato: _____

Contratada: _____

CNPJ: _____

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 140, inciso II, alínea "a", da Lei nº 14.133, de 1º de abril de 2021, e no artigo 33, inciso VIII, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 e suas alterações, que o serviço de capacitação fornecido pela CONTRATADA foi considerado SATISFATÓRIO e que os bens e/ou serviços relacionados no quadro abaixo, possuem as quantidades e a qualidade compatível com as condições e exigências constantes do Edital de Pregão Eletrônico n° ____/____.

Item	Descrição	Identificação	Unidade	Qtde

Ressalta-se que a CONTRATANTE se reserva o direito de reproduzir trechos do material didático utilizado na capacitação, desde que registradas as devidas fontes, para realizar capacitações internas de seus empregados no futuro.

Local/UF, data

Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante da Área Requisitante
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante Legal da Empresa
Cargo
CPF

ANEXO XII – MODELO DE PROPOSTA COMERCIAL

PROPOSTA COMERCIAL

(em papel timbrado da empresa)

Ao Gabinete de Segurança Institucional da Presidência da República – GSI/PR

Referência: Pregão Eletrônico SRP nº ___/____.

Proposta que faz a empresa _____, inscrita no CNPJ nº _____ e inscrição estadual nº _____, estabelecida no(a) _____, para eventual aquisição (ou contratação) para atender às necessidades da Área Demandante do GSI/PR, de acordo com as especificações e condições constantes do Pregão em referência, bem como do respectivo Edital e seus Anexos.

Planilha de Proposta de Preços

Item	Descrição do Item	Qtde total	UN	Valor Unitário	Valor Total
1	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, instalada e configurada em ambiente da CONTRATANTE.	1	Unidade		
2	Capacitação Técnica para 6 (seis) servidores	1	Turma		
Valor Total da Contratação (R$)					

1) Dados da Proposta: Valor Total: R$ _____ (VALOR POR EXTENSO).

2) Detalhamento dos Itens:

2.1) Item 1: será composto pelo software(s) (nome do software) - versão (nº da versão), em sua versão (completa / modificada), onde serão aplicadas as customizações necessárias para atender as especificações definidas no Edital e seus Anexos.

Obs: no caso de não ser fornecida a versão completa do software, deverá ser informado as funcionalidades que não estarão disponíveis.

2.2) Item 2: a capacitação será realizada (presencialmente / a distância), conforme as condições previstas no Edital e seus anexos.

3) Validade da Proposta: 90 (noventa) dias, a contar da data de sua apresentação.

4) Informamos, por oportuno, que nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

5) Dados da empresa:

a) Razão Social: _____

b) CNPJ (MF) nº _____

c) Inscrição Estadual nº: _____

d) Endereço: _____

e) Telefone: _____ Fax: _____ e-mail: _____

f) Cidade: _____ Estado: _____

g) CEP: _____

h) Representante(s) legal(is) com poderes para assinar o contrato:

a. Nome: _____

b. Cargo: _____

c. CPF: _____ RG: _____ _____-____

i) Dados Bancários:

a. Banco:_____ b. Agência:_____ c. Conta Corrente:_____

j) Dados para Contato:

a. Nome: _____

b. Telefone/Ramal: _____

Declaramos, para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui o Anexo "__" do Edital.

Declaramos, ainda, que inexiste qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com serviço ou dirigente do Ibama; e que foi (realizada a vistoria nas instalações da Área Demandante do GSI/PR, tomando conhecimento dos serviços a serem realizados / apresentada recusa formal de vistoria), não sendo admitidas, em hipótese alguma, alegações posteriores de desenvolvimento dos serviços e de dificuldades técnicas não previstas.

Local e data _____

_____

Representante Legal

Cargo _____ CPF _____

ANEXO XIII – TERMO DE CONFIDENCIALIDADE

TERMO DE CONFIDENCIALIDADE

Cláusula Primeira - OBJETO

1.1 Constitui objeto deste Termo o estabelecimento de condições especificas para regulamentar as obrigações a serem observadas pela contratada, doravante denominada PARTE RECEPTORA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela contratante, doravante denominada PARTE REVELADORA, por força dos procedimentos necessários para a execução do objeto do contrato celebrado entre as partes.

Cláusula Segunda - CONCEITOS E DEFINIÇÕES

2.1 Para os efeitos deste TERMO aplicam-se os seguintes termos e definições:

2.1.1 Confidencialidade ou Sigilo: Propriedade de que a informação não seja revelada a pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

2.1.2 Contrato: Negócio jurídico celebrado entre as partes com base na Ata de Registro de Preços.

2.1.3 Dado pessoal: Informação relacionada a pessoa natural identificada ou identificável (Lei n° 13.709/2018).

2.1.4 Dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

2.1.5 Informação: Conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades especificas e/ou tomada de decisão.

2.1.6 Informação de acesso restrito: Aquelas que estão submetidas temporariamente a restrição de acesso público.

2.1.7 Informação sigilosa: Aquelas que estão submetidas a restrição de acesso público, cujo conhecimento e divulgação estão regidos por esse instrumento.

2.1.8 Informações de acesso restrito, sigilosas por legislação específica (não exaustivas):

I. Hipóteses de sigilo aplicáveis a informações de natureza patrimonial:
  a) Segredo industrial (L. 9.279/1996);
  b) Direito autoral (L. 9.610/1998); e
  c) Propriedade intelectual de Software (L. 9.609/1998).

II. Hipóteses de sigilo decorrentes de direitos de personalidade:
  a) Sigilo Fiscal (Art. 198 da Lei n° 5.172/196);
  b) Sigilo bancário (Art. 10 da LC n° 105/2001);
  c) Sigilo Comercial (§2° do art. 155 da Lei n° 6.404/1976);
  d) Sigilo Empresarial (Art. 169 da Lei n° 11.101/2005); e
  e) Sigilo Contábil (Art. 1.190 e 1.191 da Lei n° 5.869/1973).

III. Hipóteses de sigilo decorrentes de processos e procedimentos:
  a) Sigilo de inquérito policial (Art. 20 da Lei n° 3.689/1941);
  b) Segredo de justiça no processo civil (Art. 155 da Lei n° 5.869/1973); e
  c) Segredo de justiça no processo penal (§6° do art. 201 da Lei n° 3.689/1941).

2.1.9 Necessidade de conhecer: Condição pessoal inerente à função ou atividade, indispensável para que o colaborador tenha acesso a dados ou informações classificadas. De acordo com este princípio, os colaboradores só devem ter acesso às informações necessárias para o desenvolvimento de suas atividades dentro da empresa.

2.1.10 Tratamento ou processamento de dados pessoais: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Cláusula Terceira - INFORMAÇÕES SIGILOSAS

3.1 Serão consideradas como informações sigilosas, toda e qualquer informação, revelada a outra parte por razão da execução do contrato, contendo ou não marcação ou rótulo de grau de sigilo. O termo “informação" abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou

intangível, podendo incluir, mas não se limitando, a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da contratante e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao(s) Contrato(s), doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a PARTE RECEPTORA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do(s) Contrato(s) celebrado(s) entre as partes.

3.2 A PARTE RECEPTORA compromete-se a não revelar, copiar, transmitir, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do Contrato, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do Contrato.

3.3 As estipulações e obrigações contidas neste Termo não serão aplicadas a qualquer informação que seja comprovadamente de domínio público, exceto se decorrer de ato ou omissão do beneficiado ou tenha sido comprovada e legitimamente recebida de terceiros, estranhos ao presente instrumento ou ainda informações resultantes de pesquisa pelo beneficiado.

Cláusula Quarta - EXTENSÃO DA RESPONSABILIDADE

4.1 A PARTE RECEPTORA se obriga a:

4.1.2 Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das informações sigilosas por seus agentes, representantes ou por terceiros; e

4.1.3 Comunicar à PARTE REVELADORA de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente.

Cláusula Quinta - DIREITOS E OBRIGAÇÕES

5.1 A PARTE RECEPTORA se compromete e se obriga a utilizar a informação sigilosa revelada pela PARTE REVELADORA exclusivamente para os propósitos da execução do(s) Contrato(s), em conformidade com o disposto neste deste Termo.

5.2 A PARTE RECEPTORA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da PARTE REVELADORA.

5.3 A PARTE RECEPTORA se compromete a obter o aceite formal dos funcionários que atuarão direta ou indiretamente na execução do(s) Contrato(s) sobre a existência deste Termo, bem como da natureza sigilosa das informações, a instruir sobre as formas de tratamento das informações a que terão acesso, e dar ciência à PARTE REVELADORA dos documentos comprobatórios quando solicitado.

5.4 A PARTE RECEPTORA obriga-se a tomar todas as medidas necessárias a proteção da informação sigilosa, bem como para evitar e prevenir a revelação a terceiros.

5.5 A PARTE RECEPTORA deve adotar Política de Segurança de Informação que comprove o atendimento dos requisitos de sigilo e segurança definidos no âmbito do contrato.

5.6 A PARTE RECEPTORA deverá, quando requerido pela PARTE REVELADORA, proceder com o imediato descarte de forma irreversível, incluindo todas e quaisquer cópias eventualmente existentes em qualquer suporte de todas as informações sigilosas sob sua custódia referentes ao(s) Contrato(s).

Cláusula Sexta - PROTEÇÃO DE DADOS PESSOAIS

6.1 Ambas as partes se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, em qualquer formato ou suporte, cooperando mutuamente para observar e seguir a Lei n° 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD).

6.2 Necessidades de coleta de consentimento para outras finalidades deverão ser identificadas e correr sob responsabilidade da PARTE REVELADORA.

6.3 São escopo de tratamento somente os dados pessoais indispensáveis para a execução do objetivo contratual, e conforme bases legais pré-estabelecidas e acordadas, cabendo à PARTE RECEPTORA observar estritamente a finalidade a que se destinam os dados pessoais a que venha a ter conhecimento.

6.4 À PARTE RECEPTORA é vedada qualquer forma de compartilhamento de dados pessoais com terceiros fora do âmbito do(s) contrato(s).
6.5 Ao término do(s) contrato(s), a PARTE RECEPTORA deverá comprovar a cessação de acessos, uso e o descarte definitivo, conforme procedimentos a serem determinados pela PARTE REVELADORA.
6.6 A PARTE RECEPTORA adotará todas as medidas de segurança necessárias para impedir o acesso não autorizado, divulgação, alteração ou destruição não autorizada dos dados pessoais, no que couber.

Cláusula Sétima - DISPOSIÇÕES GERAIS
7.1 Surgindo divergências quanto a interpretação do acordo pactuado neste instrumento ou quanto a execução das obrigações dele decorrentes ou, se constatados casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade e da economicidade.
7.2 O disposto no presente Termo prevalecerá sempre em caso de dúvida, e salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Cláusula Oitava - DISPOSIÇÕES ESPECIAIS
8.1 Ao assinar o presente instrumento, a PARTE RECEPTORA manifesta sua concordância no sentido de que:

8.1.1 o não exercício, por qualquer uma das Partes, de direitos assegurados neste instrumento não importará em renúncia aos mesmos, sendo considerado como mera tolerância para todos os efeitos de direito;

8.1.2 todas as condições, termos e obrigações ora constituídas serão regidas pela legislação e regulamentação brasileiras pertinentes;

8.1.3 o presente Termo somente poderá ser alterado mediante termo aditivo firmado pelas partes;

8.1.4 teve acesso e compromete-se a seguir a 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;

8.1.5 alterações do número, natureza e quantidade das informações disponibilizadas para a PARTE RECEPTORA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste Termo de Sigilo, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

8.1.6 o acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a PARTE RECEPTORA, serão incorporados a este Termo, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas; e

8.1.7 este Termo não deve ser interpretado como criação ou envolvimento das Partes, ou suas afiliadas, nem em obrigação de divulgar informações sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – VIGÊNCIA
9.1 O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de início das atividades pertinentes ao Contrato, mantendo-se em vigor por prazo indeterminado, a não ser que haja disposição em contrário por escrito, estipulada pela PARTE REVELADORA mesmo após o término do Contrato regidos por este Instrumento.

[local], [data] de [mês] de [ano].

Departamento de Segurança da Informação **DSI/PR**	Parte Receptora

ANEXO XIV – TERMO DE ACEITE DE MÓDULO

TERMO DE ACEITE DE MÓDULO

Processo Administrativo nº: _____

Objeto: _____

Nº do Contrato: _____

Contratada: _____

CNPJ: _____

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 140, inciso II, alínea “b”, da Lei nº 14.133, de 1º de abril de 2021, e no artigo 33, inciso VIII, da Instrução Normativa SGD/ME nº 1, de 4 de abril de 2019 e suas alterações, o Módulo relacionado abaixo foi homologado pela equipe técnica e possui a qualidade compatível com as condições e exigências constantes no Anexo V do Termo de Referência relativo ao Edital de Pregão Eletrônico n° ____/____.

Nr. do módulo	Etapas Componentes do Módulo	Funcionalidades

Este Termo de Aceite de Módulo é condição essencial para que se inicie a etapa de instalação e configuração da solução, e não deve ser considerado como declaração de recebimento definitivo de artefato da solução.

Ressaltamos que o recebimento definitivo dos bens e/ou serviços ocorrerá conforme previsto no Termo de Referência e no instrumento contratual proveniente do Edital de Pregão Eletrônico SRP n° ____/____.

Local/UF, data

Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante da Área Requisitante
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante Legal da Empresa
Cargo
CPF

ANEXO XV – TERMO DE ENCERRAMENTO DO CONTRATO

TERMO DE ENCERRAMENTO DO CONTRATO

Processo Administrativo nº: _____

Objeto: _____

Nº do Contrato: _____

Contratada: _____

CNPJ: _____

Por este instrumento, as partes abaixo identificadas resolvem registrar o encerramento do contrato em epígrafe e ressaltar o que segue:

O presente contrato está sendo encerrado por motivo de <motivo>.

As partes concedem-se mutuamente plena, geral, irrestrita e irrevogável quitação de todas as obrigações diretas e indiretas decorrentes do Contrato, não restando mais nada a reclamar de parte a parte, exceto as relacionadas no parágrafo a seguir.

Não estão abrangidas pela quitação ora lançada e podem ser objeto de exigência ou responsabilização, mesmo após o encerramento do vínculo contratual:

As obrigações relacionadas a processos iniciados de penalização contratual.

As garantias sobre bens e serviços entregues ou prestados, tanto legais quanto convencionais.

A reclamação de qualquer tipo sobre defeitos ocultos nos produtos ou serviços entregues ou prestados.

<inserir pendências, se houver>.

E, assim tendo lido e concordado com todos os seus termos, firmam as partes o presente instrumento, em duas vias iguais, para que surta seus efeitos jurídicos.

Local, ____ de _____ de _____.

Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

Representante Legal da Empresa
Cargo
CPF

Estudo Técnico Preliminar 25/2021

1. Informações Básicas

Número do processo: 00180.000078/2021-96

2. 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 Nr 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.

3. Descrição da necessidade

DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.1. 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, consequentemente, 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; e
- 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

3.2. 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	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. Instalação e configuração da solução em ambiente da CONTRATANTE. Garantia de suporte por 12 (doze) meses.	Unidade	1

Os demais requisitos e especificações técnicas constam do ANEXO I ao ETP – Especificações Técnicas

3.3. Identificação das necessidades legais

3.3.1 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.

3.3.2 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.

3.3.3 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.

3.3.4 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)

3.3.5 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.

3.3.6 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).

3.3.7 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.

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

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

3.3.10 Planejamento Estratégico do GSI 2018/2023.

3.4. Identificação das necessidades de manutenção

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

3.4.2 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.

3.4.3 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.

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

3.4.5 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.

3.5. Identificação das necessidades temporais

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

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

3.5.3 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:

3.5.3.1 Recebimento provisório dos bens fornecidos (conforme prazo estipulado no Termo de Referência).

3.5.3.2 Conferência quantitativa e qualitativa dos bens fornecidos, a ser executado por Comissão nomeada pela CONTRATANTE, devendo ter a participação de representante da CONTRATADA.

3.5.3.3 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.

3.5.4 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:

3.5.4.1 Responsável técnico indicado pela CONTRATADA;

3.5.4.2 Pessoal empregado pela CONTRATADA nas atividades, além do técnico responsável;

3.5.4.3 Data de início e fim das atividades;

3.5.4.4 Horários para início e fim das atividades diárias;

3.5.4.5 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;

3.5.4.6 Cronograma de execução de possíveis correções identificadas pela CONTRATANTE;

3.5.4.7 Reanálise dos serviços executados e confecção do Termo de Recebimento Definitivo.

3.6. Identificação das necessidades de segurança

3.6.1 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.

3.6.2 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.

3.6.3 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."

3.6.4 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.

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

3.6.6 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.

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

3.6.8 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.

3.6.9 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.

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

3.6.11 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.

3.6.12 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.

3.6.13 Cumprir, no que couber, a seguinte legislação:

3.6.14.1 Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações - Lei de Acesso à Informação (LAI);

3.6.14.2 Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

3.6.14.3 Decreto nº 10.332 de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022;

3.6.14.4 Decreto nº 9.637, de 26 de dezembro de 2018, estabelece a Política Nacional de Segurança da Informação.

3.6.14.5 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.

3.6.14.6 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.

3.6.14.7 Norma VIII-201 Ver. 2 de Março de 2014 da Secretaria de Administração da Presidência da República, que trata sobre desenvolvimento de sistemas.

3.7. 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, segundos perfis e qualificações necessários.

3.8. Identificação da metodologia de trabalho

3.8.1 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.

3.8.2 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.

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

3.8.3.1 Estrutura básica da solução;

3.8.3.2 Fases de implementação; e

3.8.3.3 Realização de testes.

3.9. Identificação das necessidades sociais, ambientais e culturais

3.9.1 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.

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

3.9.3 Salvo quando acordado de forma diferente, as embalagens/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 CONTRATANTE nenhum resíduo da embalagem ou qualquer peça solta. Tal exigência é condicionante para emissão do Termo de Recebimento Definitivo.

3.9.4 No que for aplicável, a solução adquirida deve atender às especificações relativas ao limite de emissão sonora e produção de resíduos dos órgãos competentes homologados pelo INMETRO. Além disso, deverão ser constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme norma da ABNT e estarem em conformidade com os requisitos técnicos que favorecem uma maior vida útil, um menor custo de manutenção e uma maior eficiência energética.

3.9.5 No que for aplicável, a solução fornecida, em decorrência da aquisição de bens ou de realização de serviços, deve estar, preferencialmente, acondicionada em embalagem individual adequada, com o menor volume possível e que utilizem materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

3.9.6 No que for aplicável, a solução fornecida, em decorrência da aquisição de bens ou de realização de serviços, não deve conter substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), Cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

3.9.7 A comprovação do disposto, sempre que solicitado, poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste que o bem ou equipamento fornecido cumpre com as exigências do Termo de Referência.

3.9.8 A empresa a ser contratada deverá fornecer, no ato da assinatura do contrato a ser formulado, o Plano de Gerenciamento de Resíduos Sólidos ou Declaração de Sustentabilidade Ambiental, comprovando a correta destinação dos materiais utilizados para disponibilização do serviço, porventura descartados em virtude de manutenção no curso da execução do contrato, bem como o pleno atendimento à legislação anteriormente citada.

3.9.9 Todos os descartes deverão ser realizados pela empresa a ser contratada, segundo as recomendações normativas sobre o assunto, dando um fim responsável a tais materiais de tal forma que cause o menor impacto possível, de acordo com as boas práticas de preservação do meio ambiente.

4. Área requisitante

Área Requisitante	Responsável
Gabinete de Segurança Institucional (Departamento de	

Segurança da Informação - DSI) SABRINA DOS PASSOS BARBOSA

5. Descrição dos Requisitos da Contratação

ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

5.1 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, com suporte por 12 (doze) meses.

5.2 Capacitação da Equipe Técnica do CTIR Gov

Os requisitos técnicos detalhados estão especificados nos documentos anexos, a saber:

- 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.

6. Levantamento de Mercado

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) constante no processo SEI 00180.000078/2021-96 são:

a) Manter a solução atual – *Request Tracker*;

b) Substituir a solução atual por sua versão mais atualizada;

c) Adoção da solução utilizada por outros CSIRTs;

d) Contratar o serviço de desenvolvimento de uma nova solução; e

e) Adquirir uma solução de mercado customizada para as necessidades da Área Demandante do GSI/PR..

6.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
	Em relação a **alternativa a) manter a solução atual – *Request Tracker***, deve-se observar o seguinte: 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. 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: • Utilização da linguagem Perl: ○ 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.

a)	○ 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, conforme figura no Anexo VIII. • 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. • 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, consequentemente, viu o Perl preso na versão 5. As versões anteriores do Perl foram lançadas com uma cadência de 1 a 2 anos. • 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. ○ 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)	A **alternativa b) substituir a ferramenta atual por sua versão mais atualizada**, também foi considerada pela equipe como **desaconselhável tecnicamente**. • 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: ○ 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.bestpratctical.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. • 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. ○ 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. • 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)	A **alternativa c) adoção da solução adotada por outros CSIRTs foi considerada inviável,** nesse momento**,** pela equipe. • 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. ○ De acordo com levantamento feito, verificou-se que: • 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 internamente**, que lidam com as necessidades de triagem e acompanhamento em ambiente totalmente baseado em software livre. • 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. • 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. ○ 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. • 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)	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**:** ○ 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. 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**: • 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: ○ 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. ○ 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. 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**.
e)	A **alternativa e) adquirir uma solução de mercado customizada para as necessidades do CTIR Gov é considerada tecnicamente viável** em função dos seguintes aspectos: • 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 apresente a lista de requisitos essenciais da solução para a realização da cotação de preços pelas empresas fornecedoras: • A 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.

6.2 – 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 Fontenele 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

X[1] – parcialmente. Algumas das soluções adotadas pelos CSIRTs foram baseadas em software livre ou público, mas foram customizadas por equipes próprias. Outros adotaram ferramentas proprietárias.

6.4 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Das alternativas consideradas, foram consideradas inviáveis:

c) adoção da solução adotada por outros CSIRTs. E

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

Em relação a alternativa c) adoção da solução adotada por outros CSIRTs, conforme visto anteriormente, o CTIR Gov necessita de uma solução que seja específica para suas atividades. Logo, seria necessário estudar profundamente as soluções adotadas pelos outros CSIRTs consultados, as quais já foram profundamente modificadas para atender as necessidades daquelas instituições. Não existe equipe, nesse momento, disponível para essa atividade, que seria de 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 a que fosse possível realizar a contagem de pontos de função, o que permitiria determinar o custo da solução, tornou a solução inviável para o processo atual, especialmente em função do tempo limite para a conclusão do processo.

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.

7. Descrição da solução como um todo

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 e suporte por 24 (vinte e quatro) meses.

8. Estimativa das Quantidades a serem Contratadas

A estimativa da demanda foi feita com base nos dados obtidos por meio do Documento de Oficialização da Demanda constante do processo SEI 00180.000078/2021-96 e assinado no dia 12 de fevereiro de 2021 e nas necessidades previstas no PDTIC 2021-2022 da Presidência da República, devendo atender o CTIR Gov.

Está previsto 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. Para tanto, a solução pretendida deve ser capaz de, entre outros aspectos:

- normalizar, armazenar e correlacionar os dados de diferentes fontes e formatos, por meio de funcionalidades analíticas;
- permitir consultas em estruturas de pesquisa dinâmicas e complexas, por meio da aplicação de filtros para a manipulação dos dados coletados;
- assinalar as informações mais relevantes para o contexto analisado, por meio da aplicação de técnicas de mineração de dados (data mining), tais como detecção de anomalias, aprendizado de regras de associação, aglomeração (*clustering*), classificação, regressão e sumarização e outras técnicas;
- apresentar os resultados de consultas nas estruturas de pesquisa estáticas e dinâmicas em uma interface integrada de forma gráfica, clara e acessível; e
- permitir a exportação dos resultados de consultas, bem como emitir relatórios sobre elas.

Os requisitos técnicos detalhados estão especificados nos documentos anexos, a saber:

- 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.

9. Estimativa do Valor da Contratação

ESTIMATIVA 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 préprocessamento das informações recebidas das diversas fontes de dados empregadas pelo CTIR Gov (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
		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
		3	Treinamento	R$20.000,00	1	R$20.000,00	

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 do CTIR	R$1.541.783,00	1	R$1.541.783,00	26/10/2021
		-	Treinamento	R$ 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 do CTIR.	R$987.715,00	1	R$987.715,00	09/09/2021
		-	Treinamento	R$ 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 a Solução escolhida, os fundamentos que solidificaram os estudos realizados que fundamentaram este ETP, 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 centavos)** conforme o valor 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). Solicita-se aos gestores do orçamento do Gabinete de Segurança Institucional (GSI) 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.

10. Justificativa para o Parcelamento ou não da Solução

10.1. O objeto da pretendida contratação, bem como a composição dos itens do escopo de fornecimento deste Estudo Técnico Preliminar, que formam o conjunto de bens e serviços a serem contratados, configuram uma única solução de Tecnologia da Informação.

10.1.1. Todos os itens do escopo de fornecimento possuem correlação entre si e são elementos inseparáveis de uma mesma e única solução de Tecnologia da Informação para prover o ambiente desejado para as atividades de triagem e tratamento de incidentes do CTIR Gov.

10.1.2. Assim posto, o presente ETP está em conformidade com o artigo 3º, inciso I, da IN SGD/ME 01 /2019 e alterações, que preceitua que

"Art. 3º Não poderão ser objeto de contratação:

I - mais de uma solução de TIC em um único contrato, devendo o órgão ou entidade observar o disposto nos §§ 2º e 3º do art. 12;"

10.1.3. Por fim, em função do exposto, o objeto desta contratação será adquirido como lote único, não sendo admitido o seu parcelamento.

11. Contratações Correlatas e/ou Interdependentes

Não se aplica ao processo atual.

12. Alinhamento entre a Contratação e o Planejamento

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

13. Resultados Pretendidos

Automatização da classificação e priorização dos eventos/incidentes recebidos pelo sistema, facilitando o tempo de resposta à incidentes e eventos cibernéticos mais críticos.

14. Providências a serem Adotadas

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**.**

15. Possíveis Impactos Ambientais

Não há.

16. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

16.1. Justificativa da Viabilidade

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 durante o processo de elaboração do artefato de Análise de Riscos (Nota Técnica nº 20 /2021/CGGSI/DSI) 2702868 que consta do processo SEI 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%) encontrava-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; e incapacidade de manutenção /evolução da solução de TI adquirida através da utilização dos contratos de fábrica de software da DITEC. Esses riscos deverão ser acompanhados com maior atenção durante todo o processo de planejamento e gestão contratuais.

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 está desenvolvendo uma solução (contratação do serviço de desenvolvimento de software, 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 o código já existente de seu produto, incluindo novas funcionalidades, sem impactar o restante da solução. Ora, esse tipo de atividade é extremamente complexa (é necessário conhecer o código em detalhes, inclusive as relações e trocas de dados entre os módulos da solução) e, dependendo da maneira como o código foi desenvolvido, pode exigir tempo e esforço extremos, o que tornaria tal adaptação economicamente inviável para a empresa.

Em função desses resultados, 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 problemas que podem levar à sua conclusão sem lograr o devido êxito**.

Essas conclusões a respeito do risco foram encaminhadas 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, entendemos ser VIÁVEL a contratação da solução demandada.

17. Responsáveis

SABRINA DOS PASSOS BARBOSA
INTEGRANTE REQUISITANTE

MAURÍCIO LEITE FERREIRA DA SILVA
INTEGRANTE REQUISITANTE

JOÃO ALBERTO MUNIZ GASPAR
INTEGRANTE TÉCNICO

MICHAEL GUANIERY TOMÉ DE ARAUJO
INTEGRANTE TÉCNICO

VALNELI FARIAS GARCIA
INTEGRANTE ADMINISTRATIVO

MARCELO PAIVA FONTENELE
AUTORIDADE MÁXIMA DA ÁREA DE TIC

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Requisitos Funcionais e Operacionais.pdf (671.64 KB)
- Anexo II - Matriz de incidentes.pdf (64.26 KB)
- Anexo III - Matrizes da Regra de Negócio.xls (156.0 KB)
- Anexo IV - Descrição das extensões aplicações existentes no RT.pdf (53.44 KB)
- Anexo V - Propostas das empresas.7z (12.71 MB)
- Anexo VI - PGC-PAC-TIC - Extrato.pdf (25.55 KB)
- Anexo VII - Gráfico obtido no Google Trend em 25_05_2021.png (46.61 KB)

Anexo I - Requisitos Funcionais e Operacionais.pdf

ANEXO I - Requisitos Funcionais e Operacionais

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
1	A solução deve se integrar, via REST API, na base de dados da instância MISP(Malware Information Sharing Platform) do CTIR Gov e extrair os registros de eventos pertinentes a incidentes cibernéticos.		O MISP suporta a integração com outras ferramentas por meio de bibliotecas para acesso a sua API, alé de módulos de expansão, exportação e importação. A lista com todos os módulos, bibliotecas e informações técnicas detalhadas está disponível no link: https://www.misp-project.org/tools/.
2	A solução deve implementar um **barramento** que permita a inclusão de outras fontes de coleta (interface REST ou outra). A solução deve prover uma interface de acesso ao barramento (conectores para acesso ao barramento) que organize os dados recebidos por agentes externos.		A API de comunicação deve ser usada por estes agentes na implementação do envio de informações para o CTIR. A solução deve fornecer um modelo de implementação da API de comunicação para ser usado pelos agentes externos que desejarem compartilhar informações sobre a ocorrência de eventos cibernéticos com o CTIR Gov. A API deverá implementar a padronização e a classificação dos eventos. Os e-mails gerados pelas informações recebidas dos agentes externos não possuem um padrão e são considerados dados não estruturados que devem ser armazenados, separadamente, das informações pré-tratadas. Para as informações não estruturadas e armazenadas separadamente deverão ser gerados alertas. Os e-mails gerados pelos sensores são considerados estruturados por possuírem um padrão previamente definido e devem ser classificados. Para os dados pré-tratados, os respectivos tickets devem ser gerados.

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
2.1	A solução deve implementar todas as funcionalidades, atualmente realizadas por extensões codificadas para o RT em uma camada independente.		Operacional: (linguagem Perl, PHP e Python), incluindo a aplicação RTC (desenvolvida pelo CTIR Gov em PHP). A relação das extensões está no Anexo IV - Descrição das extensões/aplicações existentes no RT.
2.2	Todas as informações estruturadas de entrada (via barramento) devem ser armazenadas (classificadas e priorizadas) em um banco de dados independente que conterá as informações “pré-tratadas”, permitindo a rápida decisão do responsável pela triagem.		Operacional: Como será feita a classificação de acordo com as Matrizes definida em nossa Regra de Negócio. ANEXO C.
2.3	As informações não estruturadas (não classificadas automaticamente) deverão ser encaminhadas para uma fila separada (ex: geral).		Operacional: Da fila geral podem ser selecionados eventos que devem ser re-categorizados nas filas pré-existentes adequadas pelo Triagem
2.4	A solução deve decriptografar mensagens recebidas pelo correio eletrônico utilizando a chave privada do CTIR Gov.		Operacional: A criptografia acontece quando qualquer agente externo ou pessoa envia uma mensagem ao email ctir@ctir.gov.br será redirecionado ao barramento usando nossa chave pública para criptografar o conteúdo do email. A criação e a manipulação das chaves publica e privada do CTIR são feitas pelo produto GPG-GNU Privacy Guard. O corpo do email criptografado com a chave pública do CTIR Gov inicia com a linha: -----BEGIN PGP MESSAGE----- e termina com a linha: -----END PGP MESSAGE----- O sistema deverá decifrar automaticamente as mensagens cifradas recebidas. Para isso, deverá acessar a chave privada do CTIR Gov, armazenada em servidor interno de PKI, e utilizá-la para extrair o texto em claro. Este texto em claro deverá ser anexado à mensagem original cifrada.
3	A solução deve prover a possibilidade de parametrização da matriz de incidentes, constante no Anexo II - Matriz de Incidentes. A saber:		

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
3.1	Permitir realizar a inclusão, a alteração (inclusive o nome) e a exclusão de incidentes e vulnerabilidades a serem tratados, juntamente com seus campos (quais) e características (quais), de maneira que o tratamento de incidentes possa ser escalável e de fácil configuração.		Conforme Anexo II - Matriz de Incidentes. Para os casos de desfiguração de sítio, coletar o printscreen do site e anexar a imagem ao respectivo ticket, no formato png, com nome idêntico ao número do ticket. No caso de várias imagens, nomear sequencialmente (ex: 200461,200461_1 etc). Para os casos de spamdexing, o sistema deverá coletar printscreen do código fonte da página afetada, nos locais onde as palavras-chave (buscadas pelos sensores) são encontradas e anexar a imagem ao respectivo ticket, no formato png, com nome idêntico ao número do ticket. Adotar, para o caso de várias imagens, o procedimento do exemplo anterior. As condições a serem implementadas com relação aos tipos de incidente x situação estão no campo “Log Content”, campo que contém as evidências de vulnerabilidades que são coletadas a partir de testes efetuados por sensores e são enviadas como log ao final da notificação para orientar o dono do ativo e detalhar o que foi detectado. Essa atualização deverá ser automatizada o máximo possível. A empresa deve fazer a leitura da regra de negócio atualmente implementada nas filas de tíquetes, de acordo com o Anexo III - Matrizes da Regra de Negocio, para implementar corretamente as evidências coletadas atualmente. A empresa deve avaliar as funcionalidades do sistema atual para desacoplar o processamento dos dados do sistema de gestão de tíquetes.
3.2	Permitir a categorização dos incidentes e vulnerabilidades, de maneira agrupada ou individual, por classe de prioridade de incidente.		Uma fila com os campos previstos na matriz de incidentes (Anexo II - Matriz de Incidentes). Recategorização por classe de prioridade do incidente, bem como a inclusão, a alteração e a exclusão da classe de prioridade para o incidente deverá funcionar como uma alteração de campo do incidente ou da vulnerabilidade.(Anexo II - Matriz de Incidentes).
4	A solução deve prover a possibilidade de inclusão, alteração e exclusão de órgãos, com seus respectivos campos e fornecer funcionalidades de parametrização, a saber:		Conforme Anexo III - Matrizes da Regra de Negocio.
4.1	Deverá ser possível categorizar os órgãos por classe de prioridade, de maneira agrupada ou individual.		Conforme Anexo III - Matrizes da Regra de Negocio.

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
4.2	A categorização por classe de prioridade do órgão, bem como a inclusão, a alteração e a exclusão da classe de prioridade deverá funcionar como uma alteração de campo do órgão.		Conforme Anexo III - Matrizes da Regra de Negocio.
5	A solução deve prover a possibilidade de visualização e alteração, através de uma interface ou ambiente amigável, da matriz de prioridade de incidentes cruzada com a matriz de prioridade de órgãos, que consistirá na matriz de prioridade de tratamento de incidentes utilizada pelo responsável pela triagem e pela análise.		Conforme Anexo III - Matrizes da Regra de Negocio.
6	A solução deve prover a visualização das informações existentes, em tempo real, organizadas por prioridade de tratamento, como resultado da implementação da matriz de prioridade para tratamento de incidentes.		Conforme Anexo III - Matrizes da Regra de Negocio.
7	A solução deve fornecer um **ambiente de gerenciamento de contatos**, independente, que funcione de maneira integrada com as ações de tratamento de incidentes para o envio de alertas e notificações.		Implementação de um ambiente de gerenciamento de contatos, independente, preferencialmente em banco de dados. Ao gerar a notificação, o sistema deverá acessar o sistema de contatos para selecionar o contato específico do caso). Alertas por e-mail, Telegram ou outro serviço de mensageria. Definir tipos de contatos (ex: autoridades ou definição de outros grupos). Deverá ser possível agrupar os contatos por organização, por domínios ou por faixas de IP.
7.1	Deverá ser possível inserir, excluir, ou modificar os contatos.		A edição dos dados devem ser feitas tanto manualmente quanto atualizadas automaticamente em horário definido, utilizando a base do whois. Operacional:As informações de contato, além da manipulação manual, devem ser extraídas conforme/utilizando a aplicação whois.
7.2	As informações de contato também deverão estar disponíveis para uso por outras aplicações.		Operacional:Ser acessível via API por outras aplicações para a gestão dos contatos; b) ter acesso via web à base de contatos, independente de dispositivo (responsivo).
8			

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
9	A interface dos analistas deve organizar visualmente os dados processados no barramento, visualmente, de maneira a permitir a rápida avaliação do responsável pela triagem e o rápido acionamento do órgão envolvido.A solução deve organizar automaticamente os tickets e os alertas com base na matriz de priorização, que deve ser implementada.		Operacional: deve aparecer, como é priorizado, classificado, correlacionado (11.4), falsos positivos, campos personalizados. Dominio URL, IP, repetidos e os não-classificados;Os tickets também devem ser apresentados, correlacionados com outros tickets em possíveis ataques cibernéticos.
10	A solução deve implementar o reconhecimento e a classificação de eventos, automaticamente, com base na matriz de incidentes, pela leitura/interpretação das informações contidas nos e-mails recebidos.		A funcionalidade deve ter a mesma operacionalização atualmente implementada em uma extensão no RT chamada RT-Client.
11	A solução deve organizar automaticamente os tickets e os alertas com base na matriz de priorização, que deve ser implementada.		Conforme Anexo III - Matrizes da Regra de Negocio.
11.1	A matriz de priorização (OP) (anexar o modelo) a ser implementada deve possibilitar alterações em decorrência do contexto situacional (parametrização).		Conforme Anexo III - Matrizes da Regra de Negocio.
11.2	A matriz de priorização deverá permitir que os órgãos sejam inseridos ou retirados de uma classe de prioridade, eventos podem ser inseridos ou retirados de determinada classe de prioridade.		Conforme Anexo III - Matrizes da Regra de Negocio.
11.3	Os tickets devem ser apresentados, além de priorizados, correlacionados com os atores externos envolvidos (agentes maliciosos quando for o caso).		Operacional: Deseja-se que seja possível consultar no histórico do sistema quais agente externos (grupos por ex) estão atacando que órgãos; e que órgãos estão sendo atacados por quais grupos.

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
12	A solução deve prover funcionalidade que facilite a coleta de evidências e sua correlação com o respectivo ticket. (para cada tipo, relacionar o tipo de evidência). Essa evidência deve ser coletada em uma etapa de pré-processamento (enriquecimento), após o barramento e antes de ser apresentado ao analista).		Conforme Anexo II - Matriz de Incidentes. Para os casos de desfiguração de sítio, coletar o printscreen do site e anexar a imagem ao respectivo ticket, no formato png, com nome idêntico ao número do ticket. No caso de várias imagens, nomear sequencialmente (ex: 200461,200461_1 etc). Para os casos de spamdexing, o sistema deverá coletar printscreen do código fonte da página afetada, nos locais onde as palavras-chave (buscadas pelos sensores) são encontradas e anexar a imagem ao respectivo ticket, no formato png, com nome idêntico ao número do ticket. Adotar, para o caso de várias imagens, o procedimento do exemplo anterior. As condições a serem implementadas com relação aos tipos de incidente x situação estão no campo “Log Content”, campo que contém as evidências de vulnerabilidades que são coletadas a partir de testes efetuados por sensores e são enviadas como log ao final da notificação para orientar o dono do ativo e detalhar o que foi detectado. Essa atualização deverá ser automatizada o máximo possível. A empresa deve fazer a leitura da regra de negócio atualmente implementada nas filas de tíquetes, de acordo com o Anexo III - Matrizes da Regra de Negocio, para implementar corretamente as evidências coletadas atualmente. A empresa deve avaliar as funcionalidades do sistema atual para desacoplar o processamento dos dados do sistema de gestão de tíquetes.
13	A solução deve gerar automaticamente os tickets desdobrados (tickets filhos) quando for possível identificar que o evento possui desdobramentos. como, por exemplo, varias URLs de um mesmo sitio (mesmo domínio) em um mesmo e-mail com origem nos sensores.		
13.1	Um ticket possuirá desdobramento se um e-mail contendo várias URLs (mesmo domínio) com defacement;		

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
13.2	Um ticket possuirá desdobramento se um email possuir vários sites do governo com vulnerabilidade SSL;		
13.3	Um ticket possuirá desdobramento se um e-mail do CERT-br contiver vários endereços de e-mails de diferentes órgãos de governo que estão disseminando spam.		
14	A solução deve tratar os dados coletados no sentido de identificar e eliminar as duplicações de tickets (mesma URL, domínio, e endereço IP), referentes ao mesmo problema, que chegam através dos sensores e dos agentes externos (CDCiber e CERT-br).		
14.1	Os tickets devem ser agrupados por tipo de evento/vulnerabilidade, criando um ticket principal para cada grupo, mantendo as demais ocorrências repetidas somente como referências ao principal evitando que os tickets repetidos entre nas estatísticas.		
14.2	Para o caso de tickets duplicados mas com datas diferentes (ex: um mesmo evento, não tratado, é novamente reportado gerando um ticket), a solução deve correlacionar o ticket novo com o ticket mais antigo. As datas originais de cada ticket devem ser mantidas.		
14.3	Um ticket fechado deve ser correlacionado apenas para referência.		
15	A solução deve encadear e relacionar as notificações para um mesmo órgão, de tickets abertos (considerados ainda em tratamento) de maneira a permitir que o órgão em questão possa entender o contexto da situação em determinado espaço temporal.		
15.1	A solução deve fornecer mecanismo de busca, por órgão, evento/vulnerabilidade, que permita a fácil compreensão da situação com relação aos tickets encadeados.		
15.2	Os tickets fechados devem ser relacionados possibilitando a geração de um registro histórico.		
16	A solução deve realizar o envio automático de alertas, por e-mail, para os órgãos envolvidos com base nas informações coletadas e prioridade atribuída de acordo com modelos de texto específicos para cada situação.		
16.1	A solução deve permitir a inclusão, alteração e exclusão de modelos de alerta. Os e-mail utilizados serão os existentes na base de contatos independente.		
17	A solução deve automatizar a mudança do status do ticket com base na matriz de classificação x status, como por exemplo, se um ticket é classificado como falso positivo automaticamente é atribuído o status de rejeitado.		

Requisitos Funcionais Essenciais x Requisitos Operacionais Relacionados			
Requisitos Funcionais		**Requisitos Operacionais**	
18	A solução deve fornecer mecanismos para gerar estatísticas sobre os eventos, alertas, notificações, falsos positivos, etc. com base em parâmetros dinâmicos como, por exemplo tipo de incidente x localidade, tipo de incidente x órgão da APF entre outras correlações. Estas relações deverem ser customizáveis.		Devem ser implementadas no mínimo as que estão no site do CTIR Gov, URL: https://www.ctir.gov.br/. A solução para geração de estatísticas, deve ser preferencialmente, open source. (caso a empresa não possua nenhuma ferramenta de BI já incorporadana solução, é desejável que a futura ferramenta de BI seja o QuickSense). A solução deve permitir a visualização e emissão de relatórios, de forma customizada por seleção de atributos, nos formatos: pdf, html, odt. A solução deve permitir a seleção de períodos customizáveis para a geração dos relatório, além de possibilitar correlações com outros períodos similares anteriores. A solução deve poder exportar dados nos formatos: csv, json, ods (odf) e xml, entre outros que poderão ser sugeridos entre outros que poderão ser sugeridos e incorporados.
19	A solução deve apresentar, de forma gráfica, a associação entre cracker x publicações realizadas pelo criminoso na internet relacionadas com os incidentes que estão no sistema.		

Anexos a este documento:

Anexo II - Matriz de Incidentes

Anexo III - Matrizes da Regra de Negocio

Anexo IV - Descrição das extensões/aplicações existentes no RT

Anexo II - Matriz de incidentes.pdf

ANEXO II – MATRIZ DE INCIDENTES

MATRIZ DE INCIDENTES DE REDES										
		Informações								
N°	Tipos e subtipos de Incidentes	IP	Dominio	URL	Snapshot	Tag	Arquivo / Código	Logs	Corpo Email	Cabeçalho Email
1	Abuso de Sítio									
1.1	Desfiguração de Sitio									
1.2	Conteudo Incompativel									
1.3	Redirecionamento de Pagina									
1.4	Exposição de Codigo									
1.5	Spamdexing									
1.6	Listagem de Diretorio									
1.7	Abuso de Forum / Comentarios									
1.8	Cross Site Scripting (XSS)									
1.9	Possivel Vulnerabilidade									
1.10	Possivel Vulnerabilidade - JBOSS									
2	Analise de Malware									
3	Indisponibilidade de Sítio									
4	Páginas Falsa									
5	Ransoware									
6	Scans									
7	Vazamento de Informação									
7.1	Exposição de Dados Sensiveis									
7.2	Possivel Vazamento de Informação									
7.3	Vazamento de Email Institucional									
7.4	Vazamento de Email Institucional (Personalizado)									
				Informações necessárias que devem ser coletadas						

Os eventos representados na matriz acima não esgotam, ainda, os tipos de incidentes/vulnerabilidades que serão tratados pelo CTIR-Gov. As outras informações serão detalhadas e refinadas posteriormente.

Anexo IV - Descrição das extensões aplicações existentes no RT.pdf

ANEXO IV – DESCRIÇÃO DAS EXTENSÕES/APLICAÇÕES EXISTENTES NO RT

Nome da extensão/aplicação	Descrição	Linguagem
CtirGov-RTx-Install	Extensão básica para carregar os dados e scripts básicos do CtirGov-RT. É a extensão mais importante da customização do RT e consolida todos os scripts da versão anterior (3.8.8)	Perl
CtirGov-RTx-Cli	Extensão que amplia as capacidades da extensão RT-REST. É consumida pela ferramenta chamada RT-Client	Perl
RT-Client	Cria um Command Line Interface (CLI) para ser um meio adicional de integrar com uma instancia do RT. O servidor RT deve possuir duas extensões: RT-Extension-REST (desenvolvida pelo fabricante) e CtirGov-RTx-Cli. Essa extensão é muito importante para a atividade da triagem, permitindo manipular tíquetes, realizar decriptografia, criar filhos (desdobramentos) de tickets automaticamente, realizar verificações, etc.	PHP
Sensor RB-Twitter	Busca postagens de divulgação de incidentes, normalmente abuso de sítios, vazamento e ataques de negação de serviços.	Perl
Sensor RB-Zone-H	Busca, no site http://www.zone-h.org/ ocorrências contendo referências aos domínios do governo brasileiro. O site Zone-H é utilizado por hackers para divulgar abuso de sítios.	Perl
Sensor RB-Google-CSE	Busca, através do google, abusos de sítio.	Perl
Sensor RB-Website-Tester	Verifica a disponibilidade de websites visando identificar ataques DDos. Atualmente desativado.	Perl
ETL	Implementa o processo de Extract-Transform-Load da base do RT para o formato DW, a ser utilizado inicialmente para uso no site EmNumeros, e posteriormente numa ferramenta de BI.	PHP
CtirGov-Common	Inclui uma coleção de sub-rotinas uteis para os diversos módulos.	Perl
CtirGov-Bot	Biblioteca usada por todos os sensores.	Perl
CtirGov-RTx-Clipboard	Extensão do RT que inclui botões para facilmente copiar textos. Basicamente faz a cópia da notificação a ser enviada pelo analista.	Perl
CtirGov-RTx-Correlate	Refatora a lógica dos tickets relacionados, utilizando o rtx-install criando um quadro que exibe todos os tickets correlatos ao ticket atual.	Perl
Dns-recursivo-aberto	Busca por servidores DNS com recursivo aberto	Python
Shadow Server	Envia diariamente informações sobre 80 tipos de vulnerabilidades em redes nacionais. 14 tipos são enviados automaticamente para a triagem.	N/A Externo

Anexo VI - PGC-PAC-TIC - Extrato.pdf

PLANEJAMNETO E GERENCIAMENTO DE CONTRATAÇÕES
Órgão: 020101 - PRESIDENCIA DA REPUBLICA
UASG: 110322 - GABINETE DE SEGURANÇA INSTITUCIONAL
Relatório de Itens do Plano Anual **2021**
Arquivo gerado em: 30/07/2021 17:54:53

Filtros utilizados: Número do Item: 1749

Nº Item	Tipo de item	Subitem	Código do item	Descrição	Quantidade estimada	Despesa informada é somente para vincular aos aspectos/necessidades orçamentárias	Valor unitário estimado (R$)	Valor total estimado (R$)	Valor orçamentário estimado para o exercício (R$)	Participação de recursos externos	Ação orçamentária	Grupo de Despesa	Renovação de contrato	Dependência de outro item	Item Vinculado	Grau de prioridade	Data desejada	Situação do item
1749	TIC	SERVIÇOS DE TIC	26077	SOFTWARE COMO SERVICO - SAAS	1	Não	2.600.000,00	2.600.000,00	2.600.000,00	Não	-	Custeio	NÃO	NÃO	Não Possui	Alta	02/08/2021	Incluído no PAC (editado)

Total: 1 item(s)
Valor total dos itens: **R$ 2.600.000,00**

Anexo VII - Gráfico obtido no Google Trend em 25_05_2021.png

PHP
Programming language

Python
Programming language

Perl
High-level programmin...

C++
Programming language

Java
Programming language

Worldwide | Past 5 years | All categories | Web Search

Interest over time