

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 1/13

1. OBJETO

Trata-se de **aquisição de Solução Integrada de Inteligência Cibernética, incluindo Acesso Ilimitado ao Console para Investigação e Análise de Incidentes Cibernéticos, suporte técnico e análise operacional do ambiente, implantação (instalação) e treinamento**, visando atender as necessidades de melhorias e adequações de segurança da informação e do acesso digital do Tribunal de Justiça do Estado de Goiás.

Item	Objeto	Qtde	Tipo	Unidade
1	Sistema de monitoração para cibersegurança (grande porte, com redundância)	1	software	unidade
2	Serviço de análise de qualidade operacional (10 servidores)	42	serviço	endpoints/ mês

Tabela 01 – Descrição resumida dos objetos a serem adquiridos e contratados

2. JUSTIFICATIVA

Com o advento da implementação do “*home office*” (trabalho remoto) em grande escala no contexto da pandemia mundial de COVID-19, há um volume maior de acesso remoto, onde as pessoas acessam dados importantes diretamente de casa. Esse maior número de acessos facilita a invasão dos sistemas, e nesse sentido o avanço da tecnologia se faz necessário para que as organizações estejam preparadas profissionalmente frente as demandas que o setor de TI necessita para um pleno funcionamento. A importância da adoção de medidas contra ameaças relacionadas às informações exige soluções robustas, eficientes e eficazes na prevenção, análise e proteção do ambiente.

Verifica-se nos últimos anos uma onda de ataques do tipo cibernético. Independente do tamanho ou segmento da corporação, os ataques continuam se multiplicando e estar apenas atento aos *ransomwares* e *phishings* ou possuir sistemas primários de detecção já não é mais suficiente. A necessidade latente de instituir diretrizes, normas e procedimentos de segurança através do uso de ferramentas adequadas de detecção, proteção e resposta, além de possuir profissionais capacitados é cada dia mais importante e tem sido o assunto em voga, principalmente entre os órgãos públicos que carecem de maior investimento em segurança da informação, buscando minimizar os danos quando são vítimas de ações maliciosas por parte de *hackers* (agentes maliciosos) podendo ter como efeito a paralisação das estruturas de tecnologia de informação do Poder Judiciário.

Atualmente, a estrutura de Segurança da Informação do Tribunal de Justiça do Estado de Goiás (TJGO), através do Núcleo de Segurança e Administração de Dados, vem promovendo o estabelecimento de novas metodologias, por meio de processos e normas com intuito de modernizar e reestruturar as bases de segurança da informação dentro do Tribunal. Historicamente, a Segurança da Informação passou a ter uma unidade dedicada apenas recentemente, a qual ainda vem sendo pouco explorada num contexto de prerrogativa essencial para todo o ambiente de trabalho. Faz-se necessário, no entanto, que haja um maior planejamento e estruturação do ambiente que irá analisar, dirimir, mitigar os possíveis processos infecciosos dentro da instituição.

Uma das principais necessidades para a prevenção ou proteção de ações maliciosas de qualquer tipo dentro do TJGO é a visibilidade do que de fato acontece no ambiente, incluindo conexões, acessos, tráfego de rede, eventos e logs dos serviços e sistemas, entre outros. Para o *hacker*, o não conhecimento de suas atividades é seu ponto principal de sucesso, o que facilita sua

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 2/13

ação e o deixa em situação oportuna para continuar atuando dentro da instituição. Nesse contexto, como o TJGO não possui uma ferramenta para realizar a gestão de segurança cibernética no ambiente, acaba seguindo vulnerável a diversos tipos de ameaças. Apesar de possuir sistemas e ferramentas de segurança de ativos de TIC, tais como Firewall, Antivírus, Reversos para Aplicações, esses não são suficientes para analisar de forma detalhada, centralizada e em sua totalidade os eventos e ações desempenhados pelos usuários de TIC do TJGO e, portanto, não localizando ações maliciosas.

Devido a isso, o presente projeto busca a aquisição de Solução de Gestão de Segurança Cibernética, para identificação, prevenção e proteção do ambiente quanto aos acessos indevidos, quanto às vulnerabilidades de equipamentos e sistemas, quanto à proatividade e antecipação de possíveis ações maliciosas, tais como roubo, furto, apropriação de informações sigilosas ou primordiais ao funcionamento do Tribunal, intrusão ao parque computacional com risco de criptografia indevida dos dados e backups dos sistemas, como tem ocorrido recentemente em outros órgãos públicos e empresas privadas de grande porte.

Recentemente, têm-se verificado uma escalada de casos, tanto em órgãos públicos (com destaque ao caso do Superior Tribunal de Justiça, ocorrido em 2020), quanto em empresas privadas. Além disso, não raro ocorrem casos de vazamentos de dados de pessoas e empresas em grandes volumes, com exposição a dados pessoais críticos, que provocam vulnerabilidades tanto para os proprietários dos dados, quanto para as organizações que deveriam protegê-los.

Brasil sofre seu maior ataque hacker da história

Atualizado em 5 nov 2020, 19h20 - Publicado em 5 nov 2020, 19h03

Superior Tribunal de Justiça, Ministério da Saúde e Distrito Federal foram alvos de cibercriminosos, que obtiveram acesso a informações sigilosas. Disponível em: <<https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia/>>. Acesso em 22 setembro 2021.

STJ restabelece sistemas de informática 15 dias depois de ataque hacker

18.nov.2020 (quarta-feira) - 23h03

A reabilitação do sistema foi concluída 15 dias depois do ataque hacker que culminou na suspensão dos julgamentos em todos os colegiados do tribunal. Prazos processuais tiveram de ser interrompidos.

Disponível em: <<https://www.poder360.com.br/justica/stj-restabelece-sistemas-de-informatica-15-dias-depois-de-ataque-hacker/>>. Acesso em 22 setembro 2021.

Polícia Federal ainda está investigando ataque hacker ao STJ

9 de junho de 2021, 13h17

A Polícia Federal ainda está investigando o ataque hacker aos sistemas do Superior Tribunal de Justiça, conforme informado pela assessoria de imprensa do tribunal à ConJur nesta quarta-feira (9/6).

(...)

Além do STJ e do STF, o site do Tribunal de Justiça do Rio Grande do Sul (TJ-RS) foi alvo de dois ataques nos últimos meses. Da última vez, os sistemas ficaram fora do ar e os prazos processuais foram suspensos de 30 de abril a 17 de maio.

No final do ano passado, o Tribunal já havia sofrido um ataque. Na ocasião,

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 3/13

a corte informou em nota que nenhum dado foi comprometido e que apenas páginas de acesso aos processos foram afetadas.

Em janeiro deste ano, o alvo de outro ataque foi o Tribunal Regional Federal da 3ª Região. O ataque teve como objetivo sobrecarregar os sistemas e torná-los indisponíveis.

Disponível em: <<https://www.conjur.com.br/2021-jun-09/policia-federal-ainda-investigando-ataque-hacker-stj>>. Acesso em 22 setembro 2021.

Startup de cibersegurança diz que ataque à Renner gerou pânico nas empresas

21/08/21 - 18h20 - Atualizado em 22/08/21 - 14h43

Em janeiro de 2021, a startup brasileira de cibersegurança PSafe identificou o maior vazamento de dados da história do País, quando 223 milhões de brasileiros (incluindo já mortos) tiveram dados expostos e vendidos na internet. Diante de uma brecha desse tamanho, Marco DeMello, presidente da PSafe, não vê a alta de casos de sequestro de dados de empresas com surpresa. Segundo ele, as companhias ainda não se deram conta do tamanho do prejuízo a que podem estar expostas ao não proteger seus sistemas de forma diligente.

O caso da Renner criou pânico, diz Mello, que recebeu ligações de empresários com medo de virarem a próxima vítima. “Mas eu pergunto: por que o pânico só agora? A ficha tinha de ter caído há muito tempo.”

Disponível em: <<https://www.istoedinheiro.com.br/startup-de-ciberseguranca-diz-que-ataque-a-renner-gerou-panico-nas-empresas/>>.

Acesso em 22 setembro 2021.

PSafe encontra site que expõe 426 milhões de dados pessoais de brasileiros

21/09/2021 • 17:26

A empresa de segurança cibernética Psafe diz ter encontrado um site público com cerca de 426 milhões de dados pessoais de brasileiros e 109 milhões de informações de CNPJs e placas de veículos.

Disponível em: <<https://blogs.oglobo.globo.com/capital/post/psafe-encontra-site-que-expoe-426-milhoes-de-dados-pessoais-de-brasileiros.html>>. Acesso em 22 setembro 2021.

Anteriormente a preocupação relativa a ataques do tipo cibernético a um órgão ou empresa seria atacado, se o parque computacional estava seguro contra ações maliciosas, utilizando as ferramentas já existentes. Atualmente, esta perspectiva mudou para quando será o ataque e se será possível conter as ameaças e dar continuidade às atividades da organização. As notificações referentes a **ataques cibernéticos** contra empresas brasileiras **cresceram 220% no primeiro semestre** deste ano em comparação com o mesmo período de 2020. Os dados foram divulgados em julho pelo grupo Mz, empresa especializada em relações com investidores, com base em dados levantados pela Comissão de Valores Mobiliários (CVM), agência regulada pelo Ministério da Economia, causando perdas monetárias da ordem de trilhões de dólares.

Dentre as principais vantagens do investimento dentro do ambiente, entre outras, destaca-se:

- Análise de todo o tráfego, identificando as possíveis ameaças e riscos digitais;
- Organização e adequação de uma equipe de ETIR (Equipe de Tratamento e

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 4/13

Respostas à incidentes);

- Monitoramento contínuo do ambiente;
- Integração e automatização com sistemas de segurança já existentes;
- Otimização de rotinas de segurança da informação;

Como referência de estudo para as aquisições do objeto em questão, utilizou-se as *Orientações para Elaboração/Ajuste de Especificações Técnicas de Ativos de TI – Versão 3*, do antigo Ministério do Planejamento, Orçamento e Gestão (MPOG), disponível através do seguinte link: <https://www.governodigital.gov.br/documentos-e-arquivos/Orientacoes%20Especificas%20-%20Marco%20de%202017.pdf>. Esse documento dispõe sobre boas práticas, orientações e vedações na elaboração de especificações técnicas de bens e serviços de Tecnologia da Informação (TI).

Por fim, a presente contratação encontra-se alinhada com o Plano de Gestão do Poder Judiciário do Estado de Goiás para o biênio 2021-2023:

- Meta 03: Digitalizar 100% do acervo total de processos físicos em tramitação no Poder Judiciário de Goiás;
- Meta 04: Alcançar no mínimo 72% no Prêmio CNJ de Qualidade;
- Meta 07: Alcançar o nível de excelência com o índice de 0,90 no IGOVTIC-JUD.

Também está alinhada à Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2021-2026:

- Objetivo 01: aumentar a satisfação dos usuários do sistema judiciário;
- Objetivo 02: promover a transformação digital;
- Objetivo 05: aperfeiçoar a governança e a gestão;
- Objetivo 07: aprimorar a segurança da informação e a gestão de dados.

3. BENEFÍCIOS E OBJETIVOS DA CONTRATAÇÃO

São benefícios e objetivos da contratação, entre outros:

- Adequação à Lei Geral de Proteção de Dados, às diretivas de gerenciamento e segurança do CNJ: Resolução nº 396/2021, Portaria nº 162/2021, Resolução 370/2021;
- Criar estrutura de gestão de segurança cibernética no ambiente;
- Obter visibilidade do fluxo de comunicações internas e externas oriundas do TJGO;
- Identificar os possíveis incidentes de segurança existentes;
- Prevenir ou, pelo menos, diminuir as ações maliciosas investidas;
- Criar protocolos de segurança cibernética incidindo em prevenção, gerenciamento e análise de ilícitos;
- Prover serviços de TIC com excelência, com ferramentas e recursos adequados;
- Prover segurança aos sistemas e estruturas judiciais, aos usuários internos, aos cidadãos que acessam o Poder Judiciário;
- Prover segurança aos dados e informações que são parte do serviço judicial prestado pelo TJGO;
- Aumento no nível de controle e gerência;
- Continuidade do negócio;
- Satisfação dos usuários.

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 5/13

4. DO PARCELAMENTO DO OBJETO (DIVISÃO EM LOTES/ITENS)

Nessa aquisição os Itens 1 e 2 foram agrupados em um **ÚNICO LOTE** (menor preço por lote) e serão adjudicados a um mesmo fornecedor/revenda pelas seguintes razões: Todos os itens estão intrinsecamente relacionados (interdependentes). Os itens da solução de gestão de segurança cibernética, análise e resposta de qualidade operacional e incidentes de segurança, instalação, implantação e treinamento e os serviços de suporte, são todos correlacionados ao mesmo produto e fabricante, de maneira que não há como desvencilhar um item de outro;

Assim, **as propostas deverão ser apresentas por lote**, sendo que o preço global proposto deverá atender à totalidade da quantidade exigida, por lote, não sendo aceitas aquelas que contemplem apenas parte do objeto.

A separação por Lotes/Itens dará transparência aos valores individuais e aumentará a participação das empresas no certame, além de propiciar a obtenção da proposta mais vantajosa para a Administração.

Nesse contexto, o parcelamento visou atender ao Art. 15, IV da Lei nº 8.666/93, que estabelece que “as compras, sempre que possível, deverão ser subdivididas em tantas parcelas quantas necessárias para aproveitar as peculiaridades do mercado, visando economicidade”.

5. CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO

As especificações, características e observações acerca dos produtos constantes neste Termo de Referência estão detalhadas no **Anexo I deste Termo de Referência**.

Todos os requisitos dos itens contratados devem ser entregues licenciados. Palavras como: deve, permite, suporta, efetua, proporciona, possui, etc significam que a funcionalidade deve ser entregue operacional, sem ônus adicional ao Tribunal;

Todos os equipamentos fornecidos necessários ao atendimento dos requisitos deverão ser novos, de primeiro uso;

Todos os produtos devem ser entregues em ambiente de *appliance* a ser fornecido pela CONTRATANTE.

Não serão aceitos equipamentos que tenham sido descontinuados pelo fabricante até a data de entrega e recebimento definitivo dos equipamentos;

Em caso de descontinuidade, deverá ser entregue objeto sucessor da linha descontinuada preservando-se todas as características ofertadas no edital;

Os requisitos do Item 1 devem ser entregues licenciados de forma perpétua.

Caso necessário, deverão ser fornecidos todos os itens acessórios de *hardware* e *software*, incluindo cabos, licenças, conectores, interfaces, suportes, braços organizadores de cabos e demais acessórios necessários para o perfeito funcionamento da plataforma, em plena compatibilidade com as especificações constantes neste documento e recomendadas pelo fabricante;

Para o perfeito funcionamento dos dispositivos, caso sejam necessárias outras licenças de *software*, estas deverão ser ofertadas (sem ônus para este Tribunal).

Após a assinatura do contrato, a CONTRATADA deverá apresentar em 20 (vinte) dias a carta de projeto, conforme discriminado no **Anexo I deste Termo de Referência**.

A CONTRATADA deverá fornecer a documentação de todos os equipamentos e *softwares* entregues a CONTRATANTE informando:

 PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 6/13

- Modelo do Equipamento;
- Versão do software;
- Data e Término da Garantia;

A CONTRATADA será responsável por toda a instalação e configuração da solução envolvida;

O TJGO reserva-se o direito de efetuar conexões dos equipamentos a outros, bem como adicionar peças e/ou componentes, compatíveis tecnicamente, sem que isso constitua motivo para a CONTRATADA se desobrigar dos serviços CONTRATADOS, desde que tal fato não implique danos materiais ou técnicos aos equipamentos, devidamente comprovados;

A equipe do Núcleo de Segurança e Administração de Dados da Diretoria de Tecnologia da Informação detém competência e terá total autonomia para executar ações de administração, gerenciamento e configuração dos equipamentos, bem como dos softwares, podendo promover alterações e reconfigurações sempre que julgar necessário, sem que isso constitua motivo para a CONTRATADA se desobrigar da prestação dos serviços.

6. CLASSIFICAÇÃO DOS BENS E SERVIÇOS

Os bens e serviços que constituem o objeto desta contratação são caracterizados como bens/serviços comuns, em conformidade à Lei nº 10.520/2002 e ao Decreto nº 7.174/2010, por possuir especificações usuais de mercado, nos termos dos referidos diplomas legais.

Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal do órgão licitante, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

7. DA VIGÊNCIA, LOCAL E PRAZO DE ENTREGA, GESTÃO E FISCALIZAÇÃO DO CONTRATO

O período de vigência do contrato objeto deste Termo de Referência será de **12 (doze) meses** a partir da data de sua assinatura. A vigência desse período se dá, sobretudo, em virtude do período de prestação do serviço de análise de qualidade operacional (item 2) sobre a solução tecnológica contratada, cujo item será remunerado em parcelas mensais.

No ato da entrega, o TJGO fará o recebimento provisório, para efeito de posterior verificação de conformidade com a especificação definida neste Termo de Referência. Uma vez assinado o contrato, os serviços deverão ser prestados conforme a tabela a seguir:

Item	Prazo Máximo para a Contratada entregar o objeto	Prazo Máximo para o TJGO emitir o Termo de Recebimento Definitivo	Local de Entrega
1	30 (trinta) dias corridos após o recebimento da Ordem de Serviço	30 (trinta) dias corridos após a emissão do Termo de Recebimento Provisório	<p>Data center primário (sala cofre): Edifício-sede do Tribunal de Justiça do Estado de Goiás – Av. Assis Chateaubriand nº 195, Setor Oeste, Goiânia-GO, CEP: 74130-011</p> <p>Data center secundário (container): Fórum Cível da Comarca de Goiânia-GO – Av. Olinda, esquina com Rua PL-03, Qd. G, Lt. 04, Park Lozandes, Goiânia-GO, 74884-120</p>

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 7/13

2	15 (quinze) dias corridos após o envio da Ordem de Serviço	10 (dez) dias corridos após a conclusão da Ordem de Serviço	Divisão de Infraestrutura Tecnológica – Av. Assis Chateaubriand nº 195, Setor Oeste, Goiânia-GO, CEP: 74130-011
---	--	---	---

Tabela 02 – Prazo máximo e local de entrega dos produtos

A Contratada deverá promover a instalação do objeto no prazo máximo de 30 (trinta) dias, após a solicitação da Contratante, conforme estabelecido na tabela 02 e seguindo o cronograma da tabela 03;

A Contratada deverá fazer a entrega e instalação dos equipamentos nos locais indicados na Tabela 02 e seguindo o cronograma da tabela 03.

Para implantação da solução, a Contratada deverá apresentar, no prazo máximo de 05 (cinco) dias corridos, contados a partir da assinatura do contrato, um cronograma de instalação do objeto – Plano de Projeto, a ser elaborado em conjunto com os servidores da Contratante.

A execução do projeto será realizada de acordo com o cronograma estabelecido a seguir. Os prazos estabelecidos são os prazos máximos de duração de cada fase:

Item	Descrição do Evento	Prazo Máximo	Responsável
1	Envio da Ordem de Serviço	D1	Contratante
2	Reunião Inicial do Projeto	D2 = D1 + 5	Contratante e Contratada
3	Plano de Implementação e de Testes	D3 = D2 + 10	Contratada
4	Entrega da Solução	D4 = D3 + 15	Contratada
5	Treinamento	D5 = D4 + 10	Contratada
6	Instalação, configuração e implantação	D6 = D5 + 30	Contratada

Tabela 03 – Cronograma de execução do projeto

A execução do contrato será objeto de acompanhamento, controle, fiscalização e gestão dos seguintes integrantes:

Função	Nome	Cargo	Lotação	Matrícula
Gestora do Contrato, Fiscal Demandante e Técnico	Bárbara Fernandes	Auxiliar Judiciário	Núcleo de Segurança e Administração de Dados	5132495

Tabela 04 – Definição dos papéis dos integrantes da contratação

A Gestora do Núcleo de Segurança e Administração de Dados (NSAD) será responsável pela emissão do Termo de Recebimento Definitivo, além da gestão e fiscalização do contrato. O telefone para contato em horário comercial é (62) 3216-7780.

8. PROPOSTA DE PREÇOS

Deverá ser apresentada a Proposta de Preço, informando a descrição do objeto, a marca, modelo e, caso aplicável, o *part-number*, além do valor unitário e total para cada item do lote, onde todas as despesas necessárias à perfeita execução desse projeto (fretes, seguros, taxas, impostos e demais encargos) devem estar inclusas nos preços cotados.

Item	Descrição do objeto	Valor Unitário / mensal	Valor Unitário / anual	Valor Total
...	...	R\$...	R\$...	R\$...
...	...	R\$...	R\$...	R\$...

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 8/13

Razão Social:
Número do CNPJ:
Endereço Completo com CEP:
Fone/Fax/Celular:
E-mail:
Banco/Nome e nº da Agência/Conta-Corrente:
Prazo de Validade da Proposta:
Prazo para entrega/início da prestação dos serviços:
Local e Data:
(nome e assinatura do representante legal)

Tabela 05 – Formato da Proposta de Preços

Deverá ser informado também o preposto da empresa, bem como o procedimento para acionar o chamado técnico de garantia.

9. PLANO DE AQUISIÇÃO

A aquisição/contratação de todos os itens ocorrerá na sua totalidade quando da assinatura do contrato.

10. DAS OBRIGAÇÕES DA CONTRATADA

Responsabilidade por quaisquer danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato. A fiscalização ou o acompanhamento do contrato pela Administração não exclui ou reduz a responsabilidade do contratado.

Manutenção dos seus empregados devidamente identificados, devendo substituí-los imediatamente caso sejam considerados inconvenientes.

Fornecer em qualquer época, as informações e os esclarecimentos técnicos solicitados pela contratante sobre a execução dos trabalhos.

Sanar em tempo hábil todas as irregularidades apontadas pela fiscalização.

Responsabilidade por despesas decorrentes de infração praticadas por seus empregados nas instalações da Administração.

Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse da contratante ou de terceiros de que tomar conhecimento em razão da execução do objeto, devendo orientar seus empregados nesse sentido.

Caso haja a necessidade de alocar equipamentos de informática de propriedade da empresa contratada nas dependências do TJGO, como notebooks, os mesmos deverão, obrigatoriamente, antes de se conectar com a rede interna, estar de acordo com as políticas de segurança interna do TJGO.

Comunicar à Administração por escrito e em tempo hábil, qualquer anormalidade que esteja impedindo a execução contratual, prestando os esclarecimentos julgados necessários.

Entregar os produtos e serviços de acordo com as características, quantidades e prazos especificados.

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 9/13

11. DAS OBRIGAÇÕES DA CONTRATANTE

Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada.

Exigir o imediato afastamento de qualquer empregado ou representante da contratada, que embarace a fiscalização ou, ainda, que se conduza de modo inconveniente ou incompatível com o exercício das funções que lhe foram atribuídas.

Inspeccionar, dentro dos prazos estabelecidos, os produtos e serviços fornecidos pela contratada e verificar a conformidade dos mesmos com o objeto deste Termo de Referência.

Efetuar os chamados de atendimento técnico e avaliar sua execução, promovendo as medidas cabíveis para que os produtos e serviços sejam executados em conformidade com as especificações técnicas constantes neste Termo de Referência.

Efetuar os pagamentos devidos, nas condições estabelecidas neste Termo de Referência e nos documentos que o integram.

Comunicar imediatamente a contratada via central de serviços ou ainda através de ofício, a respeito de quaisquer incidentes relacionados ao objeto deste Termo de Referência.

12. DO INADIMPLEMENTO

Pela inexecução total ou parcial do contrato, a administração poderá, garantida a defesa prévia, aplicar à contratada, segundo a extensão da falta cometida, as seguintes penalidades:

- I.** Advertência;
- II.** Multa;
- III.** Impedimento de licitar e contratar com a União, Estados, Distrito Federal e Municípios;
- IV.** Descredenciamento do sistema de cadastramento de fornecedores.

§1º. O Tribunal de Justiça, na quantificação da pena de multa, observará o seguinte:

I. 10% (dez por cento) sobre o valor do contrato, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatário em firmar o contrato, dentro de 10 (dez) dias contados da data de sua convocação;

II. multa de até 0,3% (zero vírgula três por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento ou serviço não realizado ou sobre a parte da etapa do cronograma físico de obras não cumprido;

III. multa de até 0,7% (zero vírgula sete por cento) sobre o valor da parte do fornecimento e/ou do serviço não realizado, ou sobre a parte da etapa do cronograma físico de obras não cumprida, por dia subsequente ao trigésimo;

IV. 10% (dez por cento) sobre o valor inadimplente do contrato/saldo remanescente do contrato, em caso de descumprimento parcial da obrigação.

V. Sem prejuízo das multas aplicadas, poderá a Administração, ao seu interesse, rescindir o contrato em caso de atraso superior ao sexagésimo dia sobre o fornecimento parcial ou integral do objeto ou etapa do cronograma físico da obra não cumprido, se for o caso.

VI. As multas serão descontadas de qualquer crédito da empresa contratada. Na inexistência

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 10/13

de créditos que respondam pelas multas, a contratada deverá recolhê-las nos prazos que o Tribunal de Justiça determinar ou, quando for o caso, cobrada judicialmente.

VII. A penalidade de multa, que poderá ser aplicada cumulativamente com as demais sanções, e a sua cobrança, não isentará a obrigação de indenizar eventuais perdas e danos.

§2º. O impedimento de contratar com a União, Estados, Distrito Federal e Municípios será graduado pelos seguintes prazos:

I. 6 (seis) meses, nos casos de:

a. Aplicação de duas penas de advertência, no prazo de 12 (doze) meses, sem que o CONTRATADO tenha adotado as medidas corretivas no prazo determinado pela Administração;

b. Alteração da quantidade ou qualidade da mercadoria/materiais fornecidos.

II. 12 (doze) meses, no caso de retardamento imotivado da execução do objeto, do serviço, de suas parcelas ou do fornecimento de bens.

III. 24 (vinte e quatro) meses, nos casos de:

a. Entregar como verdadeira mercadoria falsificada, adulterada, deteriorada ou danificada;

b. Paralisação de serviço ou do fornecimento de bens sem justa fundamentação e prévia comunicação à Administração;

c. Praticar ato ilícito visando frustrar os objetivos de licitação no âmbito da administração estadual;

d. Sofrer condenação definitiva por praticar, por meio doloso, fraude fiscal no recolhimento de qualquer tributo;

e. Recusar a retirada da nota de empenho ou assinatura do contrato no prazo estabelecido, sem justa causa.

§3º. O fornecedor que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, comportar-se de modo inidôneo ou cometer fraude fiscal, será aplicada penalidade de impedimento de licitar e contratar com a União, os Estados, o Distrito Federal ou Municípios, por prazo não superior a 5 (cinco) anos, sendo descredenciado do Cadastro de Fornecedores, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, aplicadas e dosadas segundo a natureza e a gravidade da falta cometida.

§4º. O contrato, sem prejuízo das multas e demais cominações legais previstas, poderá ser rescindido unilateralmente, por ato formal da Administração, nos casos enumerados no art. 78, incisos I a XII e XVII, da Lei nº 8.666/93.

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 11/13

13. DA SUBCONTRATAÇÃO

É vedada a subcontratação, salvo autorização deste Tribunal.

14. FORMA DE PAGAMENTO

O pagamento do Item 1 será efetuado em parcela única, após entregue e aceito definitivamente a totalidade do objeto.

O pagamento dos serviços do Item 2 será realizado mensalmente, ou seja, à medida que haja utilização dos serviços, com a apresentação pela Contratada de Nota Fiscal, juntamente com os relatórios gerenciais de serviços, quando serão contabilizados os serviços prestados e os pagamentos relacionados, sendo devidamente apurados e atestados pelo Gestor do Contrato e pagos no mês subsequente aos serviços efetivamente prestados.

Em todos os casos, o prazo máximo para pagamento é de 30 (trinta) dias consecutivos, contados a partir da emissão do Termo de Recebimento Definitivo / Termo de Ateste da Nota Fiscal pela Contratante, após as verificações da Nota Fiscal ou Fatura emitida pela Contratada.

O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta-corrente indicados pelo contratado;

- Para execução do pagamento, a contratada deverá fazer constar da nota fiscal correspondente, emitida, sem rasura, em letra bem legível em nome do Fundo de Reparcelamento e Modernização do Poder Judiciário, CNPJ nº 02.050.330/0001-17, o nome do banco, o número de sua conta bancária e a respectiva agência;
- A Nota Fiscal deverá ser emitida pela própria CONTRATADA, obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e das propostas, não se admitindo Notas Fiscais emitidas com outros CNPJ, mesmo aqueles de filiais ou da matriz.
- Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o Tribunal de Justiça atestar a execução do objeto do contrato.
- A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio das certidões previstas no art. 29 da Lei nº 8.666, de 1993.
 - Os documentos referentes à regularidade fiscal deverão apresentar igualdade de CNPJ, ressaltando-se aquele que o próprio órgão emissor declara expressamente no referido documento que ele é válido para todos os estabelecimentos sede e filiais da contratada.
- Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 12/13

- Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento;
- Antes de cada pagamento à contratada, será realizada consulta às certidões de regularidade fiscal para verificar a manutenção das condições de habilitação exigidas neste Termo;
 - Constatando-se a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante;
 - Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas;
 - Não havendo regularização ou sendo a defesa considerada improcedente, o Tribunal de Justiça comunicará aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;
 - Persistindo a irregularidade, serão adotadas as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa e o contraditório;
 - Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao órgão correspondente;
 - Será rescindido o contrato em execução com a contratada inadimplente, salvo por motivo de economicidade ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do Tribunal de Justiça.
- Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
 - A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar;
- Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:
 - $EM = I \times N \times VP$, sendo:
 - EM = Encargos moratórios;

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 13/13

- N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
- VP = Valor da parcela a ser paga.
- I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX) \qquad I = \frac{(6/100)}{365} \qquad I = 0,00016438$$

TX= Percentual da taxa anual = 6%

16. DOCUMENTOS COMPLEMENTARES

Integram este Termo de Referência os documentos relacionados a seguir, os quais estão vinculados à execução do contrato e sendo dele parte integrante, após devidamente ajustados com as informações correspondentes às partes contratantes:

- Anexo I – Características e Especificações do Objeto;
- Anexo II – Modelo de Termo de Compromisso e Sigilo;
- Anexo III – Modelo de Termo de Ciência.

Bárbara Fernandes

Diretora do Núcleo de Segurança e Administração de Dados

Glauco Cintra Parreira

Diretor do Núcleo de Contratos e Aquisições de TIC

Anderson Yagi Costa

Diretor de Tecnologia da Informação

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 1/11

ANEXO I – TERMO DE REFERÊNCIA CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO

1 – SERVIÇOS RELACIONADOS A SOLUÇÃO DE SEGURANÇA CIBERNÉTICA

Trata-se de Solução Integrada de Inteligência Cibernética, incluindo Acesso Ilimitado ao Console para Investigação e Análise de Incidentes Cibernéticos, suporte técnico e análise operacional do ambiente, implantação (instalação) e treinamento.

2 – ESPECIFICAÇÕES TÉCNICAS

2.1 SISTEMA DE MONITORAÇÃO PARA CIBERSEGURANÇA (GRANDE PORTE, COM REDUNDÂNCIA)

2.1.1 Realizar análises, aprendizado de máquina e detecções de eventos de segurança a nível de rede e aplicações (camada 7);

2.1.2 Deve realizar o parse de metadados em tempo real dos seguintes protocolos:

- a) HTTP 1.0 e 1.1;
- b) Apache JServ Protocol (AJP);
- c) Domain Name System (DNS);
- d) Oracle Transparent Network Substrate (TNS);
- e) PostgreSQL (pgsql);
- f) MySQL;
- g) Tabular Data Stream (TDS);
- h) Server Message Block (SMB), nas versões 1 e 2;
- i) Transport Layer Security (TLS), nas versões 1.0, 1.1 e 1.2;
- j) Simple Mail Transfer Protocol (SMTP);
- k) Lightweight Directory Access Protocol.

2.1.3 Instalação em appliance, com hardware e software integrados pelo fabricante;

2.1.4 Deve extrair informações a partir da rede, de forma passiva, em portas espelhadas em switches (ex. SPAN, RSPAN) ou com a utilização de dispositivos passivos (TAPs). Não serão aceitas soluções intrusivas, que requeiram a instalação de softwares em servidores ou que atuem de forma ativa na rede;

2.1.5 Extrair metadados de requisições e respostas de todas as transações analisadas, inclusive lentas e/ou com erros, efetuadas nos protocolos suportados, exportando os detalhes de cada transação executada, de forma granular (sem sumarizar/agregar);

2.1.6 Reconstruir o conteúdo (*body HTML*) de requisições e respostas em protocolos HTTP e AJP;

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 2/11

2.1.7 Deve calcular métricas de performance de cada transação coletada, informando:

- a) Tempo para abertura da conexão TCP;
- b) Tempo para execução da requisição pelo cliente, após início da conexão TCP;
- c) Tempo para resposta da requisição pelo servidor;
- d) Tempo para transmissão dos dados da resposta;
- e) Quantidade de retransmissões TCP (pelo cliente e pelo servidor).

2.1.8 Quantidade de pacotes Zero Window (pelo cliente e pelo servidor);

2.1.9 Todos os dados extraídos pelo appliance devem ser estruturados em formato JSON ou XML e transmitidos utilizando protocolo de mensageria;

2.1.10 A reconstrução das transações/eventos nos protocolos suportados deve ser executada em tempo real. Não serão aceitas soluções que primeiro armazenam os dados (em PCAP ou qualquer outro formato de armazenamento de pacotes de rede) e depois executam a extração de metadados;

2.1.11 Executar *Deep Packet Inspection (DPI)* em todo tráfego que chega às interfaces de coleta, identificando aplicações através de assinaturas. O DPI deve identificar as seguintes aplicações automaticamente: FTP, POP, SMTP, IMAP, DNS, HTTP, NFS, SMB, PostgreSQL, MySQL, Oracle (SGBD), MS SQL, RTSP, GRE, SSH, HTTPS, HTTP Proxy, SIP, VNC, Telnet, RDP, Websocket, Bittorrent, Youtube, Skype, Whatsapp. Não serão aceitas soluções que identificam aplicações apenas a partir do número da porta TCP/UDP;

2.1.12 Possuir 2 (duas) portas exclusivas e dedicadas para coleta de dados, em interfaces 1/10 Gigabit Ethernet, utilizando placa aceleradora com 4GB de RAM integrada. Deve executar em hardware a marcação de timestamp nos pacotes coletados e a sincronização de tempo com placas similares, com precisão de microssegundos;

- a) As interfaces devem suportar transceivers SFP e SFP+, multimodo e monomodo;
- b) Deve acompanhar 2 (dois) transceivers 10GBASE-SR.

2.1.13 Possuir 2 (duas) portas Ethernet 10GBase-T RJ45, capazes de receber tráfego espelhado via túnel GRE (Generic Routing Encapsulation), proveniente de espelhamento remoto (ex: ERSPAN), extraído em tempo real metadados de eventos contidos no túnel;

2.1.14 Possuir porta Gigabit Ethernet RJ45 dedicada para serviço Intelligent Platform Management Interface (IPMI);

2.1.15 Permitir configuração de bloqueio de pacotes nas interfaces de coleta, utilizando informações de IP e portas TCP/UDP;

2.1.16 Fazer a coleta contínua de fluxos e pacotes completos, em formato PCAP. Esses dados devem ser relacionados em interface com os demais metadados extraídos dos protocolos de rede em camada de aplicação, permitindo assim filtrar os dados que serão analisados por flow ou transação de rede;

- a) Prover capacidade de armazenamento de 100TB (cem terabytes), em drives NVMe, exclusivos para armazenamento de arquivos PCAP;
- b) Deve licenciar funcionalidade integrada para reconstrução completa de arquivos, a partir dos PCAPs capturados, inclusive de arquivos anexos a e-mails, trafegados na web ou

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 3/11

compartilhados entre usuários.

2.1.17 Performance:

a) Deve suportar a análise de tráfego Ethernet com throughput contínuo de 6 (seis) Gigabits por segundo, sem perda de pacotes;

b) Caso se julgue necessário, a performance do sistema deverá ser comprovada em demonstração executada no laboratório do fabricante, no prazo máximo de 15 dias, utilizando equipamento similar ao ofertado. Não serão aceitos equipamentos que deixem de atender a qualquer requisito de performance.

2.1.18 Permitir a procura em transações e eventos armazenados, através de filtro textual. O sistema deve indexar as informações coletadas;

2.1.19 O armazenamento de metadados e a interface de gestão devem estar instalados em cluster de dispositivos similares para alta-disponibilidade, com escalabilidade horizontal, distribuição de carga e redundância dos dados armazenados;

a) Deve armazenar os dados de forma redundante e com alta-disponibilidade, prevendo pelo menos 3 (três) cópias de cada dado, distribuídas igualmente nos appliances da solução de forma automática, suportando assim falhas em drives de armazenamento, processadores, memória ou mesmo a perda de um appliance por completo, sem que isso comprometa a disponibilidade da solução e o acesso aos dados;

b) Prover capacidade de armazenamento de 90TB (noventa Terabytes) brutos, em drives NVMe, dedicados para armazenamento de metadados provenientes da rede e logs.

2.1.20 Deve contemplar todo o processo de instalação e atualização, incluindo serviços e equipamentos, a ser realizado nas dependências do CONTRATANTE somente por profissionais autorizados pelo fabricante da solução;

2.1.21 Todos equipamentos instalados deverão ser homologados pelo fabricante original da solução;

2.1.22 As versões de firmwares e softwares instaladas deverão estar de acordo com os termos de garantia do fabricante;

2.1.23 Permitir a criação de dashboards customizados, contendo apenas gráficos e tabelas escolhidas pelo usuário.

2.1.24 Permitir a criação de alarmes customizados pelo usuário, utilizando qualquer metadado armazenado como parâmetro para envio de alertas;

2.1.25 Permitir o envio dos alertas para sistema de SIEM, utilizando formato CEF (Common Evento Format);

2.1.26 Possuir interface web em HTML5;

2.1.27 Utilizar técnicas de Machine Learning ou similares para identificar não apenas ataques amplamente divulgados, mas também ataques novos ou desconhecidos (zero day);

2.1.28 Aprender os comportamentos de usuários e dispositivos de rede para identificar anomalias que possam estar envolvidas em ataques.

a) O aprendizado deve ser supervisionado, permitindo ao administrador do sistema confirmar ou rejeitar eventuais comportamentos, com posterior inclusão de tal classificação no

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 4/11

aprendizado;

2.1.29 Detectar, pelo menos, as seguintes atividades maliciosas:

- a) Acesso a endereços IP e URLs conhecidamente maliciosas;
 - 1. As informações sobre a reputação dos recursos acessados devem ser fornecidas por entidades especializadas em inteligência;
 - 2. Acessos a aplicações realizados por mecanismos automatizados (bots).
- b) Inundações de pacotes (floods);
- c) Ataques a usuários e senhas de aplicações mediante tentativas sucessivas (brute force and dictionary attacks);
- d) Varreduras de redes para mapeamento de ativos e descoberta de vulnerabilidades;
- e) Anomalias em comportamentos de usuários da rede interna para identificação de Insider Threats;
- f) Injeções de comandos em aplicações;
- g) Movimento Lateral.

2.1.30 Na ocorrência de eventos detectados com características de ataques, alertas devem ser produzidos com informações de contexto, comportamento e assinaturas pertinentes à detecção;

2.1.31 Monitorar o status de risco de segurança e computar reputação de usuários e endpoints IP, incluindo os seguintes tipos de dispositivos:

- a) Estações de trabalho;
- b) Impressoras;
- c) Servidores de aplicação;
- d) Banco de dados;
- e) Servidores DNS;
- f) Dispositivos IOT;
- g) Celulares;
- h) Sistemas de armazenamento;
- i) Sistemas de autenticação, autorização (AAA) e acesso (IAM) à rede.

2.1.32 Deve incluir subscrição (assinatura a serviço) de API de ameaças conhecidas (Threat Intelligence), totalmente compatível com o sistema ofertado, permitindo acesso durante o período do contrato de suporte/garantia às seguintes informações:

- a) Lista de endereços IP identificados como maliciosos;
- b) Lista de URL (Uniform Resource Locator) classificadas como maliciosas;
- c) Classificação de conteúdo de serviços Web;
- d) Listas de hashes MD5 de arquivos classificados como maliciosos;
- e) Modelo de Machine Learning treinado especificamente para detecção de Malwares.

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 5/11

1. O algoritmo de detecção de Malware deve permitir a análise de pelo menos cinco mil arquivos por minuto, através da análise do conteúdo do arquivo (sem a necessidade de utilização de sandbox);

2. Esse módulo deverá ser executado localmente, sem necessidade do envio de arquivos para nuvem.

2.1.33 A lista com classificação de reputação de serviços Web deve conter pelo menos 25 (vinte cinco) bilhões de URLs;

2.1.34 As informações providas devem ser atualizadas dinamicamente, à medida que novas ameaças são detectadas na Internet;

2.1.35 O acesso aos dados da subscrição deve ser feito via HTTP REST API, de forma totalmente integrada e orquestrada pelo sistema, para correlação automatizada de metadados com as bases de ameaças conhecidas;

2.1.36 Deve fornecer informações de Whois e Geolocalização para os endereços IP e URL classificadas como ameaças;

2.1.37 A API deve fornecer o histórico de ameaça de um determinado endereço IP;

2.1.38 As informações sobre endereços IP devem incluir quais tipos de ameaças foram identificadas, com pelo menos as seguintes classificações: exploits, phishing, botnet, DoS, scanners de portas, proxies anônimos e origens de spam;

2.1.39 O provedor desses serviços deve possuir ciclo contínuo de tratamento das informações, utilizando fontes de detecção espalhadas por todo o mundo.

2.2 – SERVIÇO DE RESPOSTA A INCIDENTES DE SEGURANÇA

2.2.1 Tem por objetivo analisar eventos, orientar a resposta e documentar os incidentes de segurança da informação. Tal serviço deverá ser executado obedecendo aos *frameworks* do NIST (National Institute of Standards and Technology) e SANS Institute para resposta a incidente de segurança da informação;

2.2.2 As equipes de ataque (*RED TEAM*) e defesa (*BLUE TEAM*) devem interagir e funcionar de maneira integrada. A equipe de ataque deve compartilhar seu conhecimento no sentido de indicar soluções para vulnerabilidades encontradas e a equipe de defesa deve possuir conhecimento das táticas e técnicas de ataque para que, por meio da atuação conjunta (*PURPLE TEAM*), aumente-se a efetividade da proteção do ambiente;

2.2.3 Um incidente de segurança é definido como qualquer evento adverso em sistemas computacionais, feito de forma intencional ou acidental, levando a violação de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade;

2.2.4 O início do processo de resposta a incidente de segurança se dará das seguintes formas:

a) Sempre que um evento adverso for submetido à Contratada, pelo corpo técnico da Contratante, a qualquer tempo;

b) A partir de consultas diárias ao **Sistema de monitoração para cibersegurança**, deve identificar situações onde endpoints IP, sistemas ou usuários apresentem comportamentos

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 6/11

comprovadamente ou potencialmente nocivos a segurança dos dados.

2.2.5 Após o incidente de segurança ser aberto, será de responsabilidade do grupo de resposta a incidente de segurança (*Blue Team*) da Contratada, analisar os logs, pacotes, flows e demais artefatos coletados, a fim de no primeiro instante identificar do que se trata o incidente e avaliar o risco do mesmo;

2.2.6 Uma vez realizadas as análises iniciais do incidente, o grupo de resposta a incidente de segurança (*Blue Team*) da Contratada, deverá trabalhar para identificar quais foram os principais vetores de ataque ao ambiente do Contratante;

2.2.7 Como próximo passo o grupo de resposta a incidente de segurança (*Blue Team*) da Contratada, deverá comunicar ao time de segurança da informação do Contratante as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente;

2.2.8 A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente;

2.2.9 Após análises iniciais do incidente, caberá ao grupo de resposta a incidente de segurança (*Blue Team*), realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e todos os seus artefatos coletados;

2.2.10 Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança (*Blue Team*) da Contratada, deverá definir uma estratégia para a mitigação e contenção do ataque em questão;

2.2.11 Ao longo do processo de resposta ao incidente de segurança, a Contratada através do grupo de resposta a incidente de segurança (*Blue Team*), deve documentar toda e quaisquer evidências e identificação dos serviços e usuários envolvidos. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso. A análise deve ser realizada com o objetivo de identificar pessoas, locais e/ou eventos relacionados, correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão;

2.2.12 Caso seja necessária a reconstrução do ataque, este deve ser realizado pela Contratada em ambiente controlado, usando-se, por exemplo, de sandbox (mecanismo de segurança para separar programas em execução, geralmente utilizado em um esforço para mitigar falhas de sistema ou vulnerabilidades de segurança da informação). Tal ambiente deve ser de propriedade e controle da Contratada;

2.2.13 O grupo de resposta a incidente de segurança (*Blue Team*) da Contratada, deve documentar as lições aprendidas no incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos;

2.2.14 O serviço de resposta a incidentes será responsável por monitorar, configurar e operar o **Sistema de monitoração para cibersegurança**, visando a análise de logs, flows e pacotes de rede;

2.2.15 O regime de execução deste serviço deverá ser 24x7x365 (vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano);

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 7/11

2.2.16 A Contratada deverá prover inteligência de proteção contra ataques cibernéticos e serviços de pesquisa e desenvolvimento de inteligência de proteção contra ataques cibernéticos, sendo responsável por:

- a) Pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança fornecidos pela Contratada;
- b) Criar e revisar periodicamente regras (casos de uso) para detecção de ataques no **Sistema de monitoração para cibersegurança**, realizando as adaptações e evoluções necessárias;
- c) Implementar procedimentos para triagem de alertas e resposta a incidentes.

2.3 – SERVIÇO DE ANÁLISE DA QUALIDADE OPERACIONAL

2.3.1 Deve ser executado por profissionais especializados e certificados na ferramenta **Sistema de monitoração para cibersegurança**;

2.3.2 Os dados de performance e capacidade a serem analisados deverão ser providos unicamente pelas ferramentas de Network Performance Management (NPM) e Application Performance Management (APM), utilizados pela Contratante. Não cabe a Contratada a instalação ou manutenção dessas ferramentas, apenas o consumo de dados;

2.3.3 O serviço deve ser prestado por equipe em regime de teletrabalho, com acesso remoto às ferramentas de monitoração;

2.3.4 Cabe ao Contratante o assegurar o acesso remoto aos recursos de monitoração, via VPN ou outras tecnologias, para viabilizar o serviço de análise de performance;

2.3.5 O serviço será prestado em horário comercial, em dias úteis, conforme calendário local da Contratante;

2.3.6 Esse serviço prevê a execução de análise profissional quanto a performance e qualidade de serviço de aplicações Web, banco de dados e infraestrutura;

2.3.7 As análises de performance serão feitas de acordo com a prioridade definida pela Contratante;

2.3.8 A Contratada terá um prazo de 24 (vinte e quatro) horas corridas para iniciar o serviço de análise após a solicitação formal;

2.3.9 Após o início da análise, a Contratada deverá concluir as atividades num prazo máximo de 48 (quarenta e oito) horas corridas;

2.3.10 As análises deverão ser realizadas na ordem em que foram solicitadas e, caso a Contratante indique mais de um item por vez, deverá indicar a ordem de prioridade;

2.3.11 As análises serão realizadas sequencialmente, respeitando os prazos previstos para início e fim das atividades;

2.3.12 Cabe à Contratante definir o escopo da análise, detalhando:

- a) Endereços IP dos servidores onde estão os serviços que serão analisados;
- b) Nome dos serviços e portas TCP/UDP;
- c) Topologia de rede.

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 8/11

2.3.13 A análise deve incluir os seguintes aspectos:

- a) Performance de resposta dos servidores de aplicação, banco de dados, webservices e outros componentes da aplicação;
- b) Melhoria do tempo de resposta e experiência do usuário final;
- c) Requisições com maiores tempos de resposta e sugestões de melhorias;
- d) Requisições que apresentaram erros em execução e sugestões de melhorias;
- e) Problemas relativos à gargalos em rede e interfaces de comunicação (ex. retransmissões e zero window);
- f) Falhas em balanceamento de carga;
- g) Falhas em DNS;
- h) Erros de autenticação;
- i) Lentidão no acesso a FTP ou sistemas NAS (Network Attached Storage), SMB e NFS;
- j) Possíveis razões de erros em HTTP, com análise do conteúdo das transações;
- k) Queries lentas ou com erros em sistemas de banco de dados, com sugestões de melhorias;
- l) Otimização de objetos estáticos (imagens, PDF, vídeos, textos), com melhores práticas de uso de cache e compressão;
- m) Latência da comunicação em rede e Round Trip Time;
- n) Erros e performance de comunicações criptografadas em SSL/TLS.

2.3.14 O resultado das análises deve ser fornecido através de documentação formal e personalizada, contendo todas os levantamentos executados, inclusive com gráficos e tabelas explanatórias e análises da causa-raiz dos problemas encontrados;

2.3.15 Toda a documentação produzida deve conter o contato (telefone e e-mail) do especialista responsável pela análise;

2.3.16 A Contratante poderá entrar em contato com os especialistas em horário comercial para sanar eventuais dúvidas;

2.3.17 A Contratada terá um prazo de 4 (quatro) horas úteis para responder às dúvidas colocadas e fazer possíveis ajustes na documentação produzida.

3 – REQUISITOS DE NEGÓCIOS

3.1 Requisitos e Manutenção e Garantia

3.1.1 A Contratada assegurará garantia integral e perfeito funcionamento da solução pelo período de vigência do contrato, a partir do Termo de Aceito Provisório;

3.1.2 Durante o período de garantia da solução, a Contratada deverá:

- a) prestar suporte técnico de forma ininterrupta, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive feriados, sem ônus adicional para o Contratante;

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 9/11

b) disponibilizar Portal de Serviços, no padrão Web, que permita o acompanhamento de todos os chamados técnicos do Contratante, seu gerenciamento e a geração de relatórios gerenciais;

c) disponibilizar número telefônico e correio eletrônico para abertura de chamados de suporte técnico.

3.1.3 O prazo de início de atendimento para os chamados de suporte técnico e manutenção corretiva não poderá exceder 2 (duas) horas, a contar da abertura do chamado telefônico ou registro em sistema Web para os dias úteis, de 08:00 às 18:00, e 12 (doze) horas para os demais horários, exceto se o problema impactar na disponibilidade de todo o ambiente interno ou externo;

3.1.4 A cada nova liberação de versão e *release*, mesmo em caso de mudança de designação do nome do software, a Contratada devesse apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem;

3.1.5 As atualizações deverão estar disponibilizadas via Web ou fornecida em mídia magnética, caso solicitada pela Contratante, sem custo adicional para a Contratante;

3.1.6 Sempre que for necessária, a Contratada fará operação assistida da solução nas instalações do Contratante.

3.2 Requisitos Temporais

3.2.1 A Contratada assegurará garantia integral e perfeito funcionamento da solução pelo período de vigência do contrato, a partir do Termo de Recebimento Provisório;

3.2.2 Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos (ou horas corridas, quando definido em horas).

3.2.3 Todos os eventos de trabalho que envolvam participação de integrantes do Contratante deverão ser realizados das 08:00 às 12:00 e 14:00 às 18:00, exceto feriados, salvo acordo entre as partes.

3.2.4 Os esclarecimentos solicitados pela fiscalização do contrato deverão ser prestados imediatamente pela Contratada, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 4 (quatro) horas úteis.

3.3 Requisitos de Segurança

3.3.1 A Contratada deverá tratar como segredos comerciais e confidenciais quaisquer informações, dados e processos do Contratante obtidos em consequência ou por necessidade da execução do contrato, utilizando-os apenas para as finalidades previstas contratualmente, não podendo revelá-los ou facilitar sua revelação a terceiros, devendo todos os seus funcionários que tiverem acesso a essas informações, no decorrer da execução dos serviços contratados, assinarem termo de responsabilidade e sigilo, que deverão ser entregues ao Contratante em até 10 (dez) dias úteis contados da assinatura do contrato, e, após, sempre que necessário;

3.3.2 O Termo de Compromisso contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se no **Anexo II – Termo de Compromisso e Sigilo** e no **Anexo III – Termo de Ciência** deste Termo de Referência.

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 10/11

3.4 Requisitos de Implantação e Metodologia de Trabalho

3.4.1 O prazo de implantação é de no máximo 30 (trinta) dias, contados do recebimento da Ordem de Serviço - OS.

3.4.2 A execução do projeto será realizada de acordo com o cronograma abaixo. Os prazos estabelecidos são os prazos máximos de duração de cada fase:

Item	Descrição do evento	Prazo Máximo	Responsável
1	Envio da ordem de serviço	D1	CONTRATANTE
2	Reunião Inicial de Projeto	D2 = D1 + 5	CONTRATANTE e CONTRATADA
3	Plano de Implementação e de Testes	D3 = D2 + 10	CONTRATADA
4	Entrega da solução	D4 = D3 + 15	CONTRATADA
5	Treinamento	D5 = D4 + 10	CONTRATADA
6	Instalação, configuração e implantação	D6 = D5 + 30	CONTRATADA

3.4.3 A Contratada deverá elaborar e entregar Plano de Implementação descrevendo a estratégia de implementação da solução, incluindo descrição das atividades e estratégia de implementação, dentro do prazo estipulado na tabela acima;

3.4.4 O Contratante deverá fornecer todas as informações necessárias à implantação da solução;

3.4.5 O Contratante emitirá Termo de Recebimento Provisório, conforme previsto neste Termo de Referência;

3.4.6 Após 30 (trinta) dias corridos da emissão do Termo de Recebimento Provisório, sendo confirmada sua operação e desempenho a contento, nos termos deste Termo de Referência, o Contratante emitirá o Termo de Recebimento Definitivo.

3.4.7 A comunicação entre a Contratante e a Contratada dar-se-á por meio de canais de internet, correio eletrônico, telefone e em reuniões de acompanhamento e de suporte técnico por meio de visitas de técnico(s) da Contratada.

3.5 Requisitos de Capacitação

3.5.1 A Contratada deverá fornecer treinamento para a solução, com carga mínima de 20 (vinte) horas, para capacitar os usuários no que tange à perfeita compreensão e operação de todas as ferramentas e recursos da solução;

3.5.2 O treinamento deverá ser ministrado para equipe de servidores do Contratante por técnico qualificado da Contratada;

3.5.3 A transferência de conhecimento poderá ser realizado presencialmente ou em formato EAD (Ensino à Distância);

3.5.4 Ao final do treinamento, deverá ser fornecido certificado de conclusão, contendo as seguintes informações mínimas: nome do curso e do instrutor, carga horária total e ementa do treinamento;

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO I CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 11/11

3.5.5 A capacitação somente será tida por aceite no caso de uma avaliação média desta pelos alunos for igual ou superior de 80% (oitenta por cento). No caso de avaliação abaixo do percentual previsto, deverão ser realizados os seguintes procedimentos:

Item	Avaliação média capacitação (A)	Procedimento a ser realizados
1	$80\% > A \geq 70\%$	Ministrar aulas de reforço de 2 (duas) horas-aulas.
2	$70\% > A \geq 60\%$	Ministrar aulas de reforço de 4 (quatro) horas-aulas.
3	$A < 60\%$	Realizar nova capacitação

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	<p>TERMO DE REFERÊNCIA - ANEXO II MODELO DE TERMO DE COMPROMISSO E SIGILO</p>		
	<p>Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC</p>		
	<p>Revisão: 004</p>	<p>Código/Versão: NCA-003</p>	<p>Página: 1/5</p>

ANEXO II – TERMO DE REFERÊNCIA MODELO DE TERMO DE COMPROMISSO E SIGILO

O <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ n.º<CNPJ>, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.º<CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE; Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e os Decretos nº 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO 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 do

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO II		
	MODELO DE TERMO DE COMPROMISSO E SIGILO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 2/5

CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO II MODELO DE TERMO DE COMPROMISSO E SIGILO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 3/5

INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

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

III – Comunicar ao CONTRATANTE, 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; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretroatável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

A vigência deste Termo independe do prazo de vigência do contrato assinado.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – 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.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, a CONTRATADA assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do CONTRATANTE.

Parágrafo Quarto – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	<p>TERMO DE REFERÊNCIA - ANEXO II MODELO DE TERMO DE COMPROMISSO E SIGILO</p>		
	<p>Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC</p>		
	<p>Revisão: 004</p>	<p>Código/Versão: NCA-003</p>	<p>Página: 4/5</p>

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, 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, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro da <CIDADE DO CONTRATANTE>, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

_____, _____ de _____ de 20____

De acordo.

CONTRATANTE

CONTRATADA

<Nome>
Matrícula: <Matr.>

<Nome>
<Qualificação>

 PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação	TERMO DE REFERÊNCIA - ANEXO II MODELO DE TERMO DE COMPROMISSO E SIGILO		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 5/5

Testemunhas

_____ <Nome> <Qualificação>	_____ <Nome> <Qualificação>
-----------------------------------	-----------------------------------

 <p>PODER JUDICIÁRIO Tribunal de Justiça do Estado de Goiás Diretoria de Tecnologia da Informação</p>	TERMO DE REFERÊNCIA - ANEXO III MODELO DE TERMO DE CIÊNCIA		
	Processo de Planejamento de Aquisições e de Contratações de Soluções de TIC		
	Revisão: 004	Código/Versão: NCA-003	Página: 1/1

**ANEXO III – TERMO DE REFERÊNCIA
MODELO DE TERMO DE CIÊNCIA**

Contrato Nº			
Objeto			
Contratante			
Gestor do Contrato		Matrícula	
Contratada		CNPJ	
Preposto da Contratada		CPF	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes no Contratante.

Goiânia, _____ de _____ de _____

Ciência

CONTRATADA	
Funcionários	
<hr/> <Nome> Matrícula: <Matr.>	<hr/> <Nome> Matrícula: <Matr.>
<hr/> <Nome> Matrícula: <Matr.>	<hr/> <Nome> Matrícula: <Matr.>
<hr/> <Nome> Matrícula: <Matr.>	<hr/> <Nome> Matrícula: <Matr.>
<hr/> <Nome> Matrícula: <Matr.>	<hr/> <Nome> Matrícula: <Matr.>

ASSINATURA(S) ELETRÔNICA(S)

Tribunal de Justiça do Estado de Goiás

Para validar este documento informe o código 457344264719 no endereço <https://proad-v2.tjgo.jus.br/proad/publico/validacaoDocumento>

Nº Processo PROAD: 202109000294564 (Evento nº 4)

BARBARA FERNANDES

AUXILIAR JUDICIÁRIO

NÚCLEO DE SEGURANÇA E ADMINISTRAÇÃO DE DADOS

Assinatura CONFIRMADA em 02/10/2021 às 23:27

ANDERSON YAGI COSTA

DIRETOR DE TECNOLOGIA DA INFORMAÇÃO

DTI - PRESIDÊNCIA

Assinatura CONFIRMADA em 01/10/2021 às 19:10

GLAUCO CINTRA PARREIRA

ANALISTA JUDICIÁRIO

NUCLEO DE CONTROLE DE CONTRATOS E AQUISIÇÕES - NCCA

Assinatura CONFIRMADA em 04/10/2021 às 14:17

