PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO ELETRÔNICO nº: 202200047003608

MODALIDADE: Pregão Eletrônico

OBJETO: Contratação de empresa especializada para fornecimento de serviços gerenciados de segurança da informação ao Tribunal de Contas Estado de Goiás (TCE-GO).

DATA DA REALIZAÇÃO: 22/12/2022 às 09h00min – Horário de Brasília

LOCAL: Sistema Eletrônico Licitações-e – acesso: www.licitacoes-e.com.br

O **TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS – TCE-GO**, pessoa jurídica de direito público interno, inscrito no CNPJ/MF sob o nº 02.291.730/0001-14, com sede em Goiânia, capital do Estado de Goiás, na Avenida Ubirajara Berocan Leite, nº 640, Setor Jaó, telefone: (62) 3228-2696, CEP – 74.674-015, por intermédio do Pregoeiro e da Equipe de Apoio, instituídos pela **Portaria nº 449/2021**, tornam público o edital de **PREGÃO ELETRÔNICO Nº 036/2022**, processo eletrônico nº **202200047003608**, do tipo **MENOR PREÇO GLOBAL**, em regime de empreitada por preço global, licitação que será regida pela Lei Federal nº 10.520/2002, Lei Complementar nº 123/2006, e demais legislações correlatas, aplicando-se, subsidiariamente, no que couber, o Decreto Estadual nº 9.666/2020, a Lei Federal nº 8.666/1993 e a Lei Estadual nº 17.928/2012, com suas alterações, e demais exigências deste Edital.

Na data, horário e endereço eletrônico abaixo indicado far-se-á a abertura da Sessão Pública do **PREGÃO ELETRÔNICO**, por meio de Sistema Eletrônico Licitações-e, acessado por meio do site **www.licitacoes-e.com.br.**

I - Início de acolhimento de propostas:

09/12/2022 às 08h00min – Horário de Brasília;

II – Limite de acolhimento de propostas:

22/12/2022 às 08h00min – Horário de Brasília;

III – Abertura das propostas:

22/12/2022 às 08h00min – Horário de Brasília;

IV – Data e hora do Pregão:

22/12/2022 às 09h00min – Horário de Brasília;

Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e local (endereço eletrônico) estabelecidos no preâmbulo deste Edital, desde que não haja comunicação do Pregoeiro em contrário.

1. DO OBJETO

1.1. A presente licitação tem por objeto a contratação de empresa especializada, em regime de empreitado por preço globlal para fornecimento de serviços gerenciados de segurança da informação ao Tribunal de Contas Estado de Goiás (TCE-GO), compreendendo: Serviço de gestão de vulnerabilidades, Serviço de monitoramento, triagem, tratamento e resposta a incidentes de segurança e Serviço de operação e resposta a requisições, por 12 (doze) meses, de acordo com as especificações constantes do Termo de Referência, dos seguintes itens:

DESCRIÇÃO	QTD	AFERIÇÃO	MÉTRICA	PERÍODO
SERVIÇO DE GESTÃO DE VULNERABILIDADES	1.000	Mensal	Por Ativo	12 meses
SERVIÇO GERENCIADO DE MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA	3.500	Mensal	EPS	12 meses
SERVIÇO DE OPERAÇÕES E RESPOSTAS AS REQUISIÇÕES	2	Mensal	Por solução de SI	12 meses

1.2. Em caso de discordância existente entre as especificações e quantidades deste objeto descritas no Edital e as especificações e quantidades constantes no Termo de Referência, prevalecerão as últimas.

1.3. Acompanham este Edital os seguintes Anexos:

Anexo I: Termo de Referência
Anexo II: Minuta de Contrato
Anexo III: Modelo de Proposta de Preços
Anexo IV: Modelo de Declaração de Inexistência de Fato Impeditivo à Habilitação
Anexo V: Modelo de Declaração de não empregar menor
Anexo VI: Modelo de Declaração de Micro Empresa-ME ou Empresa de Pequeno Porte-EPP
Anexo VII: Modelo de Declaração que não possui parentesco
Anexo VIII: Modelo de Declaração de Sustentabilidade Ambiental.

2. DA IMPUGNAÇÃO AO EDITAL

2.1. **Até 03 (três) dias úteis que antecederem à abertura da sessão pública**, qualquer licitante poderá impugnar o ato convocatório do Pregão Eletrônico, exclusivamente na forma eletrônica, no e-mail: **cpl@tce.go.gov.br,** no horário das 08h00min às 12h00min e das 14h00mm às 18h00mm.

2.1.1. Caberá ao Pregoeiro, auxiliada pela Equipe de Apoio e o setor responsável pela elaboração deste Edital, decidir sobre a petição no prazo de 2 (dois) dias úteis, contados da data de recebimento da impugnação.

2.1.2. Acolhida a impugnação contra o ato convocatório e, em caso de alteração na formulação da proposta de preços, será definida e publicada nova data para realização do certame, com reabertura do prazo inicialmente concedido.

3. DA SOLICITAÇÃO DE INFORMAÇÕES

3.1**.** Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao Pregoeiro, impreterivelmente, **até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública**, exclusivamente por meio eletrônico via internet, no e-mail cpl@tce.go.gov.br.

3.2. O pregoeiroresponderá aos pedidos de esclarecimentos no prazo de 2 (dois) dias úteis, contados da data de recebimento do pedido.

3.3. As informações e/ou esclarecimentos serão prestados pelo pregoeiropor meio do site www.tce.go.gov.br e www.licitacoes-e.com.br, e vincularão os participantes e a administração, ficando todos os licitantes obrigados a acessá-los para obtenção das informações prestadas pelo pregoeiro .

4. DAS CONDIÇÕES PARA PARTICIPAÇÃO

4.1. Poderão participar deste **PREGÃO ELETRÔNICO** as empresas que:

4.1.1. Atendam às condições deste Edital e seus Anexos, inclusive quanto à documentação exigida para habilitação constante do item 12 deste Edital, e estiverem devidamente credenciadas nas agências do Banco do Brasil, através do site www.licitacoes-e.com.br, e apresentem os documentos por ele exigidos, em original ou por qualquer processo de cópia autenticada por Cartório de Notas e Ofício competente.

4.1.2. As empresas estrangeiras deverão solicitar o seu credenciamento junto ao Banco do Brasil no *site* **<http:// www.licitacoes-e.com.br>,** até 03 (três) dias úteis antes da abertura da sessão. Para seu credenciamento deverão fornecer: nome, endereço físico, telefone e endereço eletrônico (e-mail).

4.1.3. Não tenham sido declaradas inidôneas por qualquer Órgão da Administração Pública direta ou indireta, Federal, Estadual, Municipal ou do Distrito Federal, bem como as que estejam punidas com suspensão do direito de contratar ou licitar com a Administração Pública e com o Tribunal de Contas do Estado de Goiás.

4.2. Como requisito para participação no **PREGÃO ELETRÔNICO** o licitante deverá manifestar, em campo próprio do Sistema Eletrônico, que **cumpre plenamente os requisitos de habilitação e que sua proposta de preços está em conformidade com as exigências do instrumento convocatório**, bem como as especificações e quantitativos constantes **no Termo de Referência.**

4.3. O Banco do Brasil atua como Órgão provedor do Sistema Eletrônico.

4.4. Não poderá concorrer direta ou indiretamente nesta Licitação, servidor de qualquer Órgão ou Entidade vinculada ao Órgão promotor da Licitação, bem assim a empresa da qual tal servidor seja sócio, dirigente ou responsável técnico.

4.5. O licitante arcará integralmente com todos os custos de preparação e apresentação de sua proposta de preços, independente do resultado do procedimento licitatório.

4.6. Um licitante, ou grupo, suas filiais ou empresas que fazem parte de um mesmo grupo econômico ou financeiro, somente poderá apresentar uma única proposta de preços.

4.6.1. Para tais efeitos entendem-se que fazem parte de um mesmo grupo econômico ou financeiro, as empresas que tenham diretores, acionistas (com participação em mais de 5%), ou representantes legais comuns, e aquelas que dependam ou subsidiem econômica ou financeiramente a outra empresa.

4.7. Caso um licitante participe em mais de uma proposta de preços, estas propostas de preços não serão levadas em consideração e serão rejeitadas pelo comprador.

4.8. Nenhuma empresa ou instituição vinculada ao TCE-GO poderá ser elegível para participar deste processo licitatório.

4.9. Não poderão participar desta licitação os interessados que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666/1993.

5. DA PARTICIPAÇÃO DE MICROEMPRESA E EMPRESA DE PEQUENO PORTE

5.1. A disputa deste certame é aberta a quaisquer empresas que preencham as condições revistas no Item 9 – DA HABILITAÇÃO.

5.2. Por ocasião da participação neste certame, será assegurado às microempresas - ME e empresas de pequeno porte - EPP, como critério de desempate, o direito de preferência para ofertar o menor preço em relação àquele lançado pelo licitante não qualificado nessas categorias.

5.2.1. As microempresas (ME) e empresas de pequeno porte (EPP) que quiserem usufruir dos benefícios concedidos pela Lei Complementar nº 123/2006 e pela Lei Estadual nº 7.928/2012 deverão declarar em campo próprio do sistema eletrônico, a sua condição de ME ou EPP. Essa declaração é necessária para o processamento do tratamento diferenciado no procedimento licitatório.

5.2.2. Essa identificação das microempresas ou empresas de pequeno porte na Sessão pública do Pregão Eletrônico só deve ocorrer após o encerramento dos lances.

5.3. As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa entre as interessadas, observados os direitos dos participantes.

6. DO CREDENCIAMENTO

6.1. Para participar do pregão eletrônico o licitante deverá se credenciar no Banco do Brasil.

6.1. O credenciamento do licitante e a sua manutenção dependerão de registro prévio e atualizado no Licitações-e.

6.2. Os licitantes interessados deverão proceder ao credenciamento antes da data marcada para início da sessão pública via Internet.

6.3. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao Sistema Eletrônico, no site www.licitacoes-e.com.br.

6.4. O credenciamento junto ao Banco do Brasil implica na responsabilidade legal única e exclusiva da licitante ou de seu representante legal e na presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

6.5. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao Banco do Brasil ou à entidade promotora da Licitação, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

6.6. A perda da senha ou a quebra de sigilo deverão ser comunicadas ao Banco do Brasil para imediato bloqueio de acesso.

7. DA VISITA TÉCNICA

7.1. É facultada aos licitantes a vistoria nas dependências da CONTRATANTE, para proporcionar conhecimento necessário à elaboração da proposta comercial.

7.2. Tendo em vista a faculdade da realização da vistoria, o licitante vencedor não poderá alegar o desconhecimento das condições e grau de dificuldades existentes como justificativa para se eximir das obrigações assumidas e/ou prejuízos em virtude de sua omissão na realização da vistoria.

7.3. Fica a critério das licitantes realizar visita ao local onde serão realizados os serviços, no prédio sede do Tribunal de Contas do Estado de Goiás, localizado na Av. Ubirajara Berocan Leite, Nº 640. Setor Jaó, na cidade de Goiânia – GO.

7.4. As visitas destinam-se à vistoria, avaliação e ciência das empresas interessadas acerca das condições do local e peculiaridades atinentes à realização dos serviços que compõem o objeto da licitação, para fins de elaboração da proposta.

7.5. O agendamento das vistorias deverá ser previamente efetuado por intermédio do e-mail: informatica@tce.go.gov.br, cujo campo “assunto” da mensagem deverá conter o texto “Vistoria – CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

7.6. As visitas deverão ser feitas por profissional qualificado da empresa interessada, o qual deverá estar munido de documento de identificação e de instrumento que o habilite à representação legal da empresa.

7.7. No dia e hora a ser agendado, o servidor designado pelo TCE-GO acompanhará a visita das empresas interessadas, com o objetivo de esclarecer as possíveis dúvidas dos serviços que compõem o objeto da licitação.

7.8. O TCE-GO emitirá atestado de vistoria técnica que deverá ser anexado junto à documentação de habilitação.

7.9. A vistoria deverá ser pré-agendada com pelo menos 1 (um) dia útil de antecedência e poderá ser realizada até 02 (dois) dias úteis antes da data prevista para a realização do certame.

8. DA APRESENTAÇÃO DAS PROPOSTAS DE PREÇOS E DOS DOCUMENTOS DE HABILITAÇÃO

8.1. A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha privativa da licitante e subsequente encaminhamento da Proposta de Preços **contendo o valor total da proposta**, a partir da data da liberação deste Edital no site www.licitacoes-e.com.br**, 09/12/2022 às 08:00h**, até o horário limite de acolhimento de proposta, ou seja, até às **08:00h** do dia **22/12/2022**, horário de Brasília, exclusivamente por meio do Sistema Eletrônico, quando, então, encerrar-se-á, automaticamente, a fase de recebimento da proposta de preços. Durante este período a licitante poderá incluir ou excluir proposta de preços.

8.1.1. Ao término do prazo estipulado para a fase de encaminhamento e registro de Propostas o Sistema Eletrônico bloqueará automaticamente o envio de novas propostas.

8.1.2. As propostas de preços deverão ser anexadas juntamente com os documentos de habilitação exigidos no item 12 do Edital e demais documentos exigidos no Termo de Referência anexo do edital de forma exclusiva por meio do sistema.

8.1.3. O envio da proposta, acompanhada dos documentos de habilitação exigidos no presente edital, ocorrerá por meio de chave de acesso e senha.

8.1.4. Caso não seja anexado documentos de habilitação, ou na falta de algum dos documentos exigidos no Edital e ou ausência de proposta conforme anexo III do Edital, o licitante será automaticamente desclassificado.

8.2. O licitante se responsabilizará por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras as suas propostas, assim como os lances inseridos durante a sessão pública de oferta de lances.

8.3. Incumbirá ao licitante acompanhar as operações no Sistema Eletrônico durante a sessão pública do Pregão Eletrônico, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo Sistema ou de sua desconexão.

8.4. As Propostas de Preços deverão atender as especificações e quantidades contidas no Anexo I - Termo de Referência e as demais condições deste Edital.

8.5. No preenchimento da proposta eletrônica poderão ser informadas, ainda, no campo “INFORMAÇÕES ADICIONAIS”, as especificações do objeto ofertado.

8.6. Os licitantes deverão cotar seus preços com todos os tributos cabíveis inclusos, bem como todos os demais custos diretos e indiretos necessários ao atendimento das exigências deste Edital e seus anexos.

8.7. Quaisquer tributos, custos e despesas diretas ou indiretas omitidos na proposta ou incorretamente cotados serão considerados como inclusos nos preços, não sendo aceitos pleitos de acréscimos a esse ou a qualquer outro título.

8.7.1. Todas as empresas deverão cotar seus preços com todos os tributos cabíveis inclusos, bem como os demais custos diretos e indiretos necessários ao atendimento do Edital e seus anexos. Entretanto, as empresas enquadradas no regime normal de tributação (empresas não optantes do simples), estabelecidas em Goiás, deverão registrar a proposta com preços desonerados do ICMS conforme disposições do Art. 6º, Inc. XCI do Regulamento do Código Tributário do Estado de Goiás - RCTE, que concede isenção de ICMS nas operações e prestação internas, relativas à aquisição de bem, mercadoria e serviço por órgãos da Administração Pública Estadual Direta e suas fundações e autarquias, ficando mantido o crédito, observado, dentre outras coisas, à transferência do valor correspondente ao ICMS ao adquirente mediante a redução do preço do bem, mercadoria e serviço, devendo a redução ser demonstrada no documento fiscal.

8.7.2. Para as empresas estabelecidas em Goiás, isentas do ICMS, conforme item 7.7.1 acima, as propostas comerciais, enviadas pelas empresas detentoras das melhores ofertas após a fase de lances, deverão conter, obrigatoriamente, além do preço normal de mercado dos produtos ou serviços ofertados (valor bruto), o preço resultante da isenção do ICMS conferida (valor líquido), que deverá ser o preço considerado como base de julgamento. O valor líquido será aquele registrado no sistema como proposta e será

considerado como base para etapa de lances. O valor bruto (com ICMS) servirá apenas para efeito de análise do desconto concedido e para que as ordens de fornecimento possam apresentar os dois valores, facilitando a execução do contrato ou instrumento equivalente.

8.7.3 Para o licitante que não estiver obrigado a promover a desoneração do ICMS, deverá apresentar na proposta, no campo referente ao valor desonerado, o mesmo valor onerado, porém, com alíquota zero.

8.8. Fica vedado ao licitante qualquer tipo de identificação quando do registro de sua Proposta de Preços inicial, planilha ou outros anexos exigidos neste Edital, sob pena de desclassificação do certame pelo pregoeiro .

8.9. A **Proposta de Preços** da licitante arrematante, atualizada com o último lance, e, se necessário, os documentos complememtares, deverão ser anexados no **sistema, no prazo de 2 (duas) horas**, a partir da solicitação do pregoeirono sistema, observando o disposto no item 7.12 deste Edital.

8.10. A Proposta de Preços original, devidamente atualizada com o último lance ofertado, caso seja solicitada, deverá ser enviada para o Tribunal de Contas do Estado de Goiás, localizado na Av. Ubirajara Berocan Leite, n° 640, Setor Jaó, Goiânia/GO, CEP 74.674-015 (1º Andar – Corredor B - Sala da Secretaria Administrativa), no prazo máximo de 03 (três) dias úteis da indicação do(s) licitante(s) vencedor(es). Caso o vencedor seja uma empresa estrangeira, este prazo poderá ser prorrogado para até 15 (quinze) dias.

8.10.1. Ao término do prazo estipulado para a fase de encaminhamento e registro de Propostas o Sistema Eletrônico bloqueará automaticamente o envio de novas propostas.

8.11. O licitante que se enquadrar no que estabelece a Lei Complementar n.º 123/2006, deverá declarar que atende os requisitos do Artigo 3º, no ato de envio de sua proposta, em campo próprio do Sistema, para fazer jus aos benefícios previstos na referida lei.

8.12. Na proposta de preços anexada em campo próprio do sistema, deverão constar, pelo menos, as seguintes condições, conforme modelo constante do **Anexo III deste Edital (ESTE CAMPO SERÁ VISUALIZADO SOMENTE APÓS A FASE DE DISPUTA):**

a) razão social e CNPJ da empresa, endereço completo, telefone, fax e endereço eletrônico (e-mail), este último se houver, para contato, bem como nome do proponente ou de seu representante legal, CPF, RG e cargo na empresa, Banco, agência, número da conta corrente e praça de pagamento;

b) prazo de validade, não inferior a 60 (sessenta) dias corridos, contados da data do envio da proposta atualizada em conformidade com o último lance ofertado no Sistema Eletrônico;

c) planilha com o valor do dos serviços a serem fornecidos para o do TCE-GO, sendo **vedada a apresentação de apenas propostas com valor global sem a apresentação da composição dos itens citados**;

d) valor total da proposta, de acordo com o(s) preço(s) praticado(s) no mercado, conforme estabelece o inciso IV do art. 43 da Lei Federal nº. 8.666/93, em algarismo e por extenso, expresso em moeda corrente nacional (R$), com no máximo 02 (duas) casas decimais, INCLUSIVE NA ETAPA DE LANCES;

e) nos preços ofertados deverão estar incluídos todos os insumos que os compõem, tais como as despesas com mão-de-obra, impostos, encargos sociais e previdenciários, taxas,

transportes, seguros e quaisquer outros que incidam direta ou indiretamente na execução do objeto desta licitação;

f) data e assinatura do responsável.

8.13. A proposta de preços enviada implicará em plena aceitação, por parte da licitante, das condições estabelecidas neste Edital e seus Anexos.

8.14. Não serão admitidas retificações ou alterações nas propostas apresentadas, uma vez aceito o lance vencedor ou negociado e finalizada a Sessão Eletrônica.

8.15. O licitante arcará integralmente com todos os custos de preparação e apresentação de sua Proposta de Preços, sendo que o TCE-GO não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do procedimento licitatório.

8.16. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiroe para acesso ao público após encerramento do envio de lances.

9. DA CLASSIFICAÇÃO DAS PROPOSTAS

9.1. O Pregoeiro verificará as Propostas de Preços apresentadas, antes da abertura da fase de lances, desclassificando aquelas que não estejam em conformidade com os requisitos e condições estabelecidos neste Edital.

9.2. Serão desclassificadas também as Propostas de Preços que forem omissas ou que apresentarem irregularidades insanáveis, informando este fato ao licitante desclassificado.

9.3. A desclassificação de Proposta de Preços será sempre fundamentada e registrada no Sistema Eletrônico, com o acompanhamento em tempo real por todos os participantes.

9.4. Para fins de julgamento das propostas, sob pena de desclassificação, as licitantes devem apresentar planilha, conforme modelo disposto no **Anexo III deste Edital**.

9.5. O sistema ordenará, automaticamente, as Propostas de Preços classificadas pelo pregoeiro , sendo que somente estas participarão da fase de lance, dando início à fase competitiva.

10. DA SESSÃO PÚBLICA PARA FORMULAÇÃO DE LANCES

10.1. A partir das **09:00h do dia 22/12/2022** e em conformidade com o estabelecido neste Edital, terá início à sessão pública do presente Pregão Eletrônico, com a divulgação das Propostas de Preços recebidas em conformidade com o **Item 8 - DA APRESENTAÇÃO DAS PROPOSTAS DE PREÇOS E DOS DOCUMENTOS DE HABILITAÇÃO** e que deverão estar em perfeita consonância com as especificações detalhadas no presente Edital e seus Anexos.

10.2. A partir desta mesma data e horário ocorrerá o início da etapa de lances, via Internet, única e exclusivamente no site **www.licitacoes-e.com.br**, conforme previsto neste Edital.

10.3. Somente os licitantes que apresentaram Proposta de Preços em consonância com o **Item 8 - DAS PROPOSTAS DE PREÇOS**, poderão apresentar lances para o objeto deste Pregão, exclusivamente por meio do Sistema Eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

10.3.1. Assim como as Propostas de Preços, os lances serão ofertados pelo **MENOR PREÇO GLOBAL.**

10.4. Os licitantes poderão oferecer lances sucessivos, observado o horário fixado para abertura da sessão e as regras de sua aceitação.

10.4.1. O licitante somente poderá oferecer lances inferiores ao último por ele ofertado e registrado no Sistema Eletrônico.

10.4.2. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

10.4.3. O Sistema Eletrônico rejeitará automaticamente os lances em valores superiores aos anteriormente apresentados pelo mesmo licitante.

10.5. **Caso o licitante não realize lances, permanecerá o valor da proposta eletrônica apresentada para efeito da classificação final.**

10.6. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes, vedada a identificação do detentor do lance.

10.7. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o Sistema Eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

10.7.1. O Pregoeiro, quando possível, dará continuidade a sua atuação no certame, sem prejuízo dos atos realizados.

10.7.2. Quando a desconexão persistir por tempo superior a **10 (dez) minutos**, a sessão do Pregão Eletrônico será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes, no sítio eletrônico utilizado para divulgação.

10.8. A etapa de envio de lances na sessão pública durará 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

10.8.1. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta será de R$ 100,00 (cem reais).

10.8.2. A prorrogação automática da etapa de envio de lances, de que trata o item anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários.

10.8.3. Na hipótese de não haver novos lances na forma estabelecida nos itens anteriores, a sessão pública será encerrada automaticamente.

10.8.4. Encerrada a sessão pública sem prorrogação automática pelo sistema, nos termos do disposto no item 9, o pregoeiro poderá, assessorado pela equipe de apoio, admitir o reinício da etapa de envio de lances em prol da consecução do melhor preço, mediante justificativa.

10.9. A desistência em apresentar lance implicará exclusão do licitante da etapa de lances e na manutenção do último preço por ele apresentado, para efeito de ordenação das propostas de preços, conforme subitem 10.5.

11. DO ENCERRAMENTO DA ETAPA DOS LANCES E DA NEGOCIAÇÃO

11.1. Após o encerramento da etapa de lances, o pregoeirodeverá encaminhar pelo sistema eletrônico contraproposta diretamente ao licitante que tenha apresentado o lance de menor valor, para que seja obtido melhor preço, observando o critério de julgamento e o valor máximo estimado do Termo de Referência – Anexo I deste Edital, bem como decidir sobre sua aceitação, não se admitindo negociar condições diferentes das previstas no instrumento convocatório.

11.2. A negociação será realizada por meio do Sistema Eletrônico, podendo ser acompanhada pelos demais licitantes.

11.3. O Pregoeiro anunciará o licitante vencedor, imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após a negociação e decisão da mesma, acerca da aceitação do lance de menor valor.

11.4. Encerrada a etapa de lances, o pregoeiroexaminará a Proposta de Preços classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para contratação.

11.4.1. Caso não ocorram lances deverá ser verificado o valor estimado do objeto e a especificação técnica prevista, para efeito de comparação com a Proposta de Preços enviada e registrada.

11.4.2. O valor total proposto para o objeto deste Pregão superior ao estimado para a contratação, constante do Termo de Referência – Anexo I deste Edital, poderá não ser aceito e adjudicado.

11.4.3. O Pregoeiro, com o auxílio de sua Equipe de Apoio, para formalizar sua decisão em relação a este item, poderá valer-se também do que estabelece o inciso IV do art. 43 da Lei nº 8.666/93.

11.5. Após a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte, e houver proposta de microempresa ou empresa de pequeno porte que seja igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, proceder-se-á da seguinte forma:

11.5.1. A microempresa ou a empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos, apresentar proposta de preço inferior à do licitante mais bem classificado e, se atendidas as exigências deste Edital, ser contratada.

11.5.2. Não sendo contratada a microempresa ou empresa de pequeno porte mais bem classificada na forma do subitem anterior e, havendo outros licitantes que se enquadram na condição prevista no caput, estes, serão convocados, na ordem classificatória, para o exercício do mesmo direito.

11.5.3. O convocado que não apresentar proposta dentro do prazo de 5 (cinco) minutos, controlados pelo Sistema, decairá do direito previsto nos arts. 44 e 45 da Lei Complementar nº123/2006 e no art. 6º da Lei Estadual nº 17.928/2012.

11.5.4. Na hipótese de não contratação nos termos previstos nestes subitens, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.

11.6. O disposto no subitem 10.5 somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte.

11.7. Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente desistente às penalidades estabelecidas neste Edital.

11.8. A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do Pregão Eletrônico constarão de Ata divulgada no Sistema Eletrônico, sem prejuízo das demais formas de publicidade previstas na legislação pertinente.

11.9. Na hipótese de a proposta classificada em primeiro lugar não for aceitável ou o licitante não atender às exigências para a habilitação, o pregoeirodeverá restabelecer a etapa competitiva de lances entre os licitantes.

12. DA ACEITABILIDADE E DO JULGAMENTO DAS PROPOSTAS DE PREÇOS

12.1. A proposta de preços deverá conter, no mínimo, os seguintes documentos:

12.1.1. Planilha de custos unitários e totais ofertados de todos os custos diretos, conforme Anexo I do Termo de Referência;

12.1.2. Para fins de julgamento das propostas, sob pena de desclassificação, as licitantes devem apresentar planilha orçamentária de custos unitários, conforme modelo disposto no Anexo deste Termo de Referência.

12.2. Não serão aceitas propostas com custos unitários manifestamente inexequíveis.

12.2.1. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, na forma do § 3º do art. 43 da Lei nº 8.666/93, para efeito de comprovação de sua exequibilidade.

12.2.2. Também será desclassificada a proposta que, após as diligências, não corrigir ou justificar eventuais irregularidades apontadas pelo Pregoeiro.

12.2.3. A adequação da proposta na forma dos itens anteriores não poderá acarretar em majoração de seu valor global.

12.3. Encerrada a etapa de lances e concluída a negociação, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade com as condições e especificações estabelecidas no Termo de Referência e neste Edital, inclusive quanto ao valor estimado para a contratação, para efeito de aceitabilidade.

12.4 O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de servidores do TCE-GO, ou, ainda, caso seja necessário, de outras pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.

12.5. Havendo aceitação da proposta classificada em primeiro lugar, o pregoeiropoderá promover diligência destinada a obter esclarecimentos complementares, caso seja necessário.

12.6. O julgamento das Propostas de Preços dar-se-á pelo critério de **MENOR PREÇO GLOBAL**, observadas as condições definidas no Termo de Referência, seus anexos e neste Edital.

12.7. O empate entre dois ou mais licitantes somente ocorrerá quando houver igualdade de preços entre a Proposta de Preços e quando não houver lances para definir o desempate.

12.7.1. Havendo empate no caso de todos os licitantes desistirem da fase de lances e se negarem a negociar com o Pregoeiro, serão utilizados para fins de desempate os seguintes critérios:

1º. O disposto no § 2º do art. 3º da Lei nº 8.666/1993;

2º. Sorteio, a ser realizado pelo sistema eletrônico entre as propostas empatadas.

3º. Será assegurada, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte, no caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos §§ 1º e 2º do art. 44 da Lei Complementar 123/06, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

12.9. Será admitido apenas 01 (um) licitante vencedor.

12.9. Não será motivo de desclassificação simples omissões que sejam irrelevantes para o entendimento da Proposta de Preços, que não venham causar prejuízo para o comprador e nem firam os direitos dos demais licitantes.

12.10. Será rejeitada a Proposta de Preços que apresentar valores irrisórios ou de valor zero, incompatíveis com os preços de mercado acrescidos dos respectivos encargos.

12.11. O licitante classificado provisoriamente em primeiro lugar deverá encaminhar a proposta atualizada conforme disposto no item 8 deste Edital e, quando necessário, os documentos complementares à proposta e à habilitação.

12.12. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de erros ou falhas no julgamento das propostas ou da habilitação, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com no mínimo 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

13. DA HABILITAÇÃO

13.1. Para habilitação neste Pregão Eletrônico, as empresas nacionais deverão apresentar os seguintes documentos abaixo listados, EXCLUSIVAMENTE por meio do sistema *licitacoes-e*, concomitantemente com a proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

13.1.1. Deverão ser apresentados todos os documentos exigidos no item 9 do Termo de Referência – Anexo I do presente Edital, ainda:

13.1.2. Documentação relativa a habilitação jurídica, conforme o caso, incisos I a V do artº 28 da Lei 8.666/93;

13.1.3. Registro comercial, no caso de empresa individual;

13.1.4. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedades por ações, documentos de eleição de seus administradores;

13.1.5. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

13.1.6. Certificado de Regularidade do FGTS - CRF, perante o Fundo de Garantia por Tempo de Serviço, atualizado;

13.1.7. Prova de regularidade para com as Fazendas Federal/INSS (Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União), Estadual e Municipal do domicílio ou sede do licitante, e **da Fazenda Pública do Estado de Goiás (exigência prevista no art. 88 da Lei nº 17.928/12) atualizadas;**

13.1.8. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, tendo em vista o disposto no art. 3º da Lei nº 12.440, de 7 de julho de 2011;

13.1.8.1. É permitida a apresentação de Certidão Positiva com Efeitos de Negativa de Débitos Trabalhistas instituída pela Lei n° 12.440/2011.

13.1.9. Documentos contábeis e financeiros que demonstrem a capacidade econômico-financeira da CONTRATADA para assumir os compromissos do Contrato, por meio de comprovação de patrimônio líquido não inferior a 10% (dez por cento) do valor estimado da contratação, quando qualquer dos índices Liquidez Geral, Liquidez Corrente e Solvência Geral, for igual ou inferior a 1;

13.1.9.1. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

13.1.10. Certidão negativa de falência ou recuperação judicial e extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física;

13.1.10.1 No caso de certidão positiva de recuperação judicial ou extrajudicial, o licitante deverá apresentar a comprovação de que o respectivo plano de recuperação foi acolhido judicialmente, na forma do art. 58, da Lei n.º 11.101, de 09 de fevereiro de 2005, sob pena de inabilitação, devendo, ainda, comprovar todos os demais requisitos de habilitação, que comprovem a sua viabilidade econômica.

13.1.11. Apresentar declaração de inexistência de fato superveniente impeditivo de sua habilitação, atestando a inexistência de circunstâncias que impeçam a empresa de participar do processo licitatório, nos termos do modelo constante do **Anexo IV** deste edital, assinada por sócio, dirigente, proprietário ou procurador da licitante, com o número da identidade do declarante;

13.1.12. Apresentar declaração da licitante de que não possui em seu quadro de pessoal empregado (s) menor (es) de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e menor (es) de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do inciso XXXIII, do art. 7º, da Constituição Federal de 1988, conforme modelo constante do **Anexo V** deste edital;

13.1.13. Apresentar declaração, para todos os fins de direito e sob as penas da lei que não possui em seus quadros de empregados e em seu corpo societário/acionário cônjuges, companheiros ou parentes em linha reta ou colateral, até o terceiro grau, ou por afinidade, até o segundo grau, de Conselheiros, Auditores, e Procuradores de Contas do Tribunal de

Contas do Estado de Goiás, e ainda, com os servidores detentores de cargo em comissão ou função de confiança que atuem diretamente na realização do certame e/ou na posterior formalização contratual, conforme modelo do **Anexo VII** deste Edital;

13.1.14. Apresentar declaração, sob as penas da lei, a ser apresentada pela microempresa ou empresa de pequeno porte de que se enquadra nas condições do Estatuto Nacional da Microempresa e Empresa de Pequeno Porte, instituído pela Lei Complementar nº 123, de 14.12.2006, de que cumprem os requisitos legais para a qualificação como microempresa ou empresa de pequeno porte, estando aptas a usufruir do tratamento favorecido estabelecido por aquela Lei, conforme modelo constante do **Anexo VI** deste edital.

13.1.14.1. Apresentar certidão que ateste o enquadramento, expedida pela Junta Comercial ou, alternativamente, documento gerado pela Receita Federal, por intermédio de consulta realizada no sítio www.receita.fazenda.gov.br/simplesnacional, podendo ser confrontado com as peças contábeis apresentadas no certame licitatório;

13.1.15. Apresentar declaração, sob as penas da lei, de sustentabilidade ambiental, conforme modelo constante do **Anexo VIII** deste Edital.

13.2. A apresentação da documentação exigida neste edital estende-se às Microempresas ou Empresas de Pequeno Porte.

13.2.1. Se a documentação enviada nos termos dos subitens anteriores for proveniente de microempresa ou de empresa de pequeno porte e apresentar alguma restrição quanto à regularidade fiscal, ser-lhe-á assegurado o prazo de **05 (cinco) dias úteis**, cujo termo inicial corresponderá ao momento em que a licitante for declarada vencedora do certame, prorrogáveis por igual período, a critério da Administração, para regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas, com efeito de certidão negativa.

13.2.2. A não regularização da documentação no prazo previsto acima implicará decadência do direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei nº 8.666/93, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação, conforme previsto no art. 43, § 2º, da Lei Complementar nº 123/2006 e do art.4º, § 5º, do Decreto nº. 8.538/2015 e no art. 5º, § 3º da Lei Estadual nº 17.928/2012.

13.3. Os documentos complementares à proposta e à habilitação, quando forem necessários à confirmação daqueles exigidos no edital e já apresentados, serão encaminhados pelo licitante melhor classificado após o encerramento do envio de lances, no próprio sistema no prazo de 2 (duas) horas, a partir da solicitação do pregoeirono sistema.

13.4. O licitante, que for declarado vencedor apenas encaminhará os documentos de habilitação, por via de e-mail (cpl@tce.go.gov.br), dentro do prazo de 2 (duas) horas, se autorizado ou solicitado pelo Pregoeiro .

13.4.1. A empresa declarada vencedora na hipótese de autorização dada pelo Pregoeiro, **poderá** encaminhar documentação via e-mail, para o referido endereço, desde que possua certificado digital, ou seja, a empresa deverá possuir assinatura eletrônica para que a documentação enviada eletronicamente tenha validade.

13.5. O licitante regularmente cadastrado e habilitado parcialmente perante a Administração Pública poderá apresentar o CRC (Certificado de Registro Cadastral), emitido pelo Cadastro de Fornecedores do Estado de Goiás – CADFOR.

13.6. Os documentos necessários à habilitação poderão ser apresentados em original, cópia autenticada em Cartório competente ou assinados eletrônicamente.

13.7. Os documentos remetidos por meio eletrônico, poderão ser solicitados em original ou por cópia autenticada, a qualquer momento, em prazo a ser estabelecido pelo pregoeiro , salvo se assinado eletronicamente (assinatura eletônica - *token*).

13.8. Os originais ou cópias autenticadas, **caso sejam solicitados**, deverão ser encaminhados para o Tribunal de Contas do Estado de Goiás, localizado na Av. Ubirajara Berocan Leite, n° 640, Setor Jaó, Goiânia/GO, CEP 74.674-015 – Sala da Secretaria Administrativa (1º andar – Bloco B).

13.9. Sob pena de inabilitação, os documentos encaminhados deverão estar em nome do licitante, com indicação do número de inscrição no CNPJ.

13.10. Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz.

13.11. Caso a participação no certame se dê através da matriz, com possibilidade de que a execução contratual se dê por filial, ou vice-versa, a prova de regularidade fiscal deverá ser de ambas.

13.12. O licitante estrangeiro deverá apresentar todos os documentos equivalentes aos exigidos dos licitantes brasileiros, no caso de ser considerado vencedor.

13.12.1. Na hipótese de o licitante vencedor ser estrangeiro, para a assinatura do contrato ou da ata de registro de preços, os documentos de que trata o *caput* deste artigo serão traduzidos por tradutor juramentado no País e apostilados.

13.12.2. O licitante deverá ter procurador residente e domiciliado no País, com poderes para receber citação, intimação e responder administrativa e judicialmente por seus atos, juntando os instrumentos de mandato com os documentos de habilitação.

13.13. Não serão aceitos “protocolos de entrega” ou “solicitação de documento” em substituição aos documentos requeridos no presente Edital e seus Anexos.

12.14. O pregoeiropoderá consultar sítios oficiais de órgãos e entidades emissores de certidões, para verificar as condições de habilitação dos licitantes.

13.15 Serão consultados os bancos de dados CEIS (Cadastro Nacional de Empresas Inidôneas e Suspensas) e CNEP (Cadastro Nacional de Empresas Punidas), seja para fins de participação, seja como condição prévia para análise da habilitação da empresa melhor classificada.

13.16 A existência de registro no CADIN estadual constituirá impedimento à contratação do licitante, no termos do art. 6º, I e §1º da Lei estadual nº 19.754, de 17 de julho de 2017, devendo o mesmo, nesta hipótese, ser desclassificado, já que tal impedimento inviabiliza o resultado útil da licitação.

13.17 Relativo ao tratamento diferenciado às microempresas e empresas de pequeno porte serão consultados o Portal da Transparência estadual e o sistema SIOFI a fim de verificar se o somatório dos valores das ordens de pagamento, recebidas por licitante, ME ou EPP, detentor da proposta classificada em primeiro lugar, ultrapassou, no exercício anterior, os limites

previstos no artigo 3°, incisos I e II, da LC n° 123/2006, ou o limite proporcional de que trata o artigo 3°, § 2°, do mesmo diploma, em caso de início de atividade no exercício considerado.

13.18 A consulta também abrangerá o exercício corrente, para verificar se o somatório dos valores das ordens bancárias, recebidas pela referida licitante até o mês anterior ao da sessão pública da licitação, extrapola os limites acima referidos, acrescidos do percentual de 20% (vinte por cento) de que trata o artigo 3°, §§ 9°-A e 12, da LC n° 123/2006.

13.19. O não atendimento de qualquer das condições aqui previstas provocará a inabilitação do licitante.

14. DOS RECURSOS

14.1. Qualquer licitante poderá, de forma imediata e motivada, explicitando sucintamente suas razões, **no prazo de 10 (dez) minutos após declaração do vencedor**, em campo próprio do Sistema Eletrônico, manifestar sua intenção de recorrer.

> 14.1.1. Será concedido ao licitante que manifestar a intenção de interpor recurso o prazo de **03 (três) dias** para apresentar as razões de recurso, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

14.2. **A ausência de manifestação imediata e motivada do licitante quanto à itenção de recurso, importará a decadência do direito de recurso** e o pregoeiroestará autorizado para adjudicar o objeto ao licitante declarado vencedor.

14.3. O acolhimento do recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

14.4. A decisão do pregoeirodeverá ser motivada e submetida à apreciação da autoridade competente pela licitação, se não aceito o recurso interposto.

14.5. Decididos os recursos e constatada a regularidade dos atos praticados, **a autoridade competente adjudicará o objeto e homologará o resultado da licitação.**

15. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

15.1. A adjudicação do objeto do presente certame será viabilizada pelo Pregoeiro sempre que não houver recurso.

15.2. A homologação da licitação é de responsabilidade da autoridade competente e só poderá ser realizada depois da adjudicação do objeto à licitante vencedora pelo pregoeiro .

15.3. Quando houver recurso e o pregoeiromantiver sua decisão, deverá esta ser submetida à autoridade competente para decidir acerca dos atos do pregoeiro.

15.4. Após a homologação, o adjudicatário será convocado para assinar o contrato no prazo definido neste Edital.

16. DA FISCALIZAÇÃO, DO PAGAMENTO E GERENCIAMENTO DO CONTRATO

16.1. A gestão e a fiscalização do contrato competirão respectivamente aos servidores Licardino Siqueira Pires (Gerente de Tecnologia da Informação) e Bruno Henrique de Oliveira Peixoto (Chefe do Serviço de Sistemas da Informação), conforme designado no inciso I do art. 1º da Portaria nº 128/2021 do Tribunal de Contas do Estado de Goiás.

16.2. À fiscalização caberá ainda:

16.2.1. assegurar-se da boa prestação dos serviços, verificando sempre o bom desempenho dos mesmos;

16.2.2. Documentar as ocorrências havidas e fiscalizar o cumprimento das obrigações contratuais assumidas pela CONTRATADA, inclusive quanto à não interrupção dos serviços prestados;

16.2.3. Emitir pareceres em todos os atos relativos à execução do Contrato, em especial quando da necessidade de aplicação de sanções, alterações e repactuações do Contrato.

16.3. A fiscalização nos moldes deste Termo de Referência não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados ao Tribunal de Contas do Estado de Goiás ou a terceiros, resultantes de imperfeições técnicas, vícios ou defeitos ocultos de serviços que os desqualificam para o uso normal e rotineiro e, na ocorrência destes, não implica corresponsabilidade do TCE-GO ou de seus agentes e prepostos.

16.4. Ao Tribunal de Contas do Estado de Goiás caberá:

16.4.1. Apresentar à CONTRATADA as observações, reclamações e exigências que se impuserem em decorrência da Fiscalização;

16.4.2. Notificar à CONTRATADA, por escrito, sobre a ocorrência de eventuais imperfeições na execução dos serviços, fixando prazo para sua correção, conforme sua conveniência.

16.5. À CONTRATANTE não caberá qualquer ônus pela rejeição de serviços ou materiais considerados inadequados pelo Fiscal.

16.6 A Nota Fiscal dos serviços prestados deverá ser remetida, tanto em papel quanto em arquivo eletrônico, com antecedência mínima de 10 (dez) dias úteis em relação à data de seu vencimento, para que o Gestor do Contrato possa realizar sua verificação e, não havendo problemas, emitir o Aceite Definitivo;

16.7 A CONTRATADA deverá fornecer as faturas mensais no endereço do CONTRATANTE;

16.8 Sendo identificada cobrança indevida, os fatos serão informados à CONTRATADA e a contagem do prazo para pagamento será reiniciada a partir da reapresentação da Nota Fiscal devidamente corrigida;

16.9 Sendo identificada cobrança indevida após o pagamento da Nota Fiscal, os fatos serão informados à CONTRATADA, para que seja feita glosa do valor correspondente no próximo documento de cobrança;

16.10 O aceite dos serviços prestados por força desta contratação, será feito mediante ateste das Notas Fiscais;

16.11 Havendo erro na apresentação da Nota Fiscal/Fatura 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 o CONTRATANTE;

16.12. Será emitida nota de empenho em favor da empresa adjudicatária, após a homologação da licitação, caso se efetive a contratação.

16.13. O pagamento será efetuado de acordo com os valores estipulados no Contrato Administrativo firmado com a CONTRATADA, sendo realizado de acordo com as Ordens de Serviço ou de Fornecimento de Bens;

16.14. Os serviços entregues serão homologados pelos Fiscais e Gestor do Contrato;

16.15. A Aceitação dar-se-á após a assinatura do TERMO DE RECEBIMENTO DEFINITIVO;

16.16. O Tribunal de Contas do Estado de Goiás - efetuará o pagamento até o 30º (trigésimo) dia do mês subsequente à entrega definitiva devidamente atestada pela Gerência de Tecnologia da Informação.

16.17. O pagamento será creditado em favor da adjudicatária, por meio de Ordem Pagamento, em qualquer instituição bancária indicada na Nota Fiscal, devendo, para isto, ficar especificado o nome do banco, agência com a qual opera, localidade e número da conta corrente em que deverá ser efetivado o crédito.

16.18. O TCE-GO não efetuará pagamento por meio de títulos de cobrança bancária.

16.19. Qualquer erro ou omissão ocorrido na documentação fiscal será motivo de correção por parte da adjudicatária e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente sanado.

16.20. Quando do pagamento a ser efetuado pelo Tribunal de Contas do Estado de Goiás, a adjudicatária deverá comprovar sua regularidade no tocante à Documentação Obrigatória (Receita Federal, Dívida Ativa da União, Estado e Município, FGTS, INSS e Justiça do Trabalho). Tal comprovação será objeto de confirmação “ON LINE”, sendo suspenso o pagamento, caso esteja irregular.

16.21. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação das obrigações, em virtude de penalidades impostas à CONTRATADA ou inadimplência total ou parcial referente à contratação.

16.22. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação das obrigações, em virtude de penalidades impostas à CONTRATADA ou inadimplência total ou parcial referente à contratação.

16.23. O TCE/GO reserva-se o direito de suspender o pagamento se o produto entregue estiver em desacordo com as especificações constantes no Edital e em seus Anexos.

16.24. No caso de atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, serão devidos pela CONTRATANTE encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples;

16.25. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

16.26. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável;

16.27. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, 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;

16.28. Para fazer jus ao pagamento, a empresa deverá manter, durante toda a execução contratual e em compatibilidade com as obrigações assumidas, todas as condições de habilitação exigidas no Termo de Referência;

16.29. Nenhum pagamento será efetuado à empresa, enquanto houver pendência de liquidação de obrigação financeira, em virtude de penalidade ou inadimplência contratual.

17. PRAZO E FORMA DE ENTREGA

17.1. Em conformidade com os artigos 73 a 76 da Lei nº 8.666/1993, os itens objeto da prestação dos serviços serão recebidos da seguinte forma:

17.1.1. Provisoriamente, no ato da entrega, para efeito de posterior verificação de sua conformidade com as especificações e com a proposta;

17.1.2. Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para a perfeita execução efetiva da prestação dos serviços.

17.1.3. O dimensionamento da equipe para a execução adequada do serviço contratado é de responsabilidade exclusiva do Fornecedor de Serviço, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência e seus anexos. Dependendo da complexidade, criticidade e do prazo do projeto, os serviços poderão ser realizados nas instalações da CONTRATADA ou do TCE-GO.

17.1.4. Todos os custos com licenças de simuladores e softwares devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extras, seja a que título for.

17.1.5. O período de prestação dos serviços, a partir da emissão do termo de recebimento definitivo, será o estabelecido na tabela abaixo, observadas as etapas previstas no item EXECUÇÃO DOS SERVIÇOS do Anexo IV do presente Termo de Referência. As quantidades da tabela abaixo foram baseadas no ambiente especificado no Anexo III deste Termo de Referência e em estimativa de fluxo de dados no *switch* principal do TCE-GO.

DESCRIÇÃO	QTD	AFERIÇÃO	MÉTRICA	PERÍODO
SERVIÇO DE GESTÃO DE VULNERABILIDADES	1.000	Mensal	Por Ativo	12 meses
SERVIÇO GERENCIADO DE MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA	3.500	Mensal	EPS	12 meses
SERVIÇO DE OPERAÇÕES E RESPOSTAS AS REQUISIÇÕES	2	Mensal	Por solução de SI	12 meses

17.1.6. A partir da assinatura do contrato, correrão os seguintes prazos:

17.1.7. Reunião de início do projeto (kick-off): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pelo TCE-GO com 02 (dois) dias úteis de antecedência.

17.1.8. Entrega do Projeto Executivo: até 30 (trinta) dias corridos, contados a partir da reunião de início do projeto (kick-off);

17.1.9. O TCE-GO se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;

17.1.10. Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo TCE-GO, a respeito da manifestação sobre o Projeto Executivo;

17.1.11. A conclusão da fase de implantação dos serviços é de até 60 (sessenta) dias corridos, contados a partir da data de início da vigência do contrato, mediante a emissão do termo de recebimento definitivo pelo TCE-GO.

17.1.12. O termo de recebimento definitivo obedecerá os seguintes critérios:

17.1.13. O TCE-GO terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo, depois de finalizado o planejamento, customização e a instalação do ambiente;

17.1.14. A prestação dos serviços mensais iniciará somente a partir da emissão do termo de recebimento definitivo pelo TCE-GO;

17.1.15. Para todos os bens importados, caso necessários por parte da CONTRATADA, que sejam instalados nas dependências do TCE-GO, será necessária a apresentação dos respectivos comprovantes de origem.

17.1.16. Os Centros de Operações de Segurança da CONTRATADA deverão estar em pleno funcionamento, operando em regime 24x7x365, em até – no máximo – 90 (noventa) dias corridos, contados da data de início da vigência contratual.

18. DO VALOR ESTIMADO E RECURSOS ORÇAMENTÁRIOS

18.1. O valor global máximo aceito para a contratação é de R$ 1.651.045,08 (Um milhão e seiscentos e cinquenta e um mil e quarenta e cinco reais e oito centavos).

SERVIÇOS CONTINUADOS SOB PROGRAMAÇÃO				
Item	**Descrição**	**Parcelas**	**Valor Mensal**	**Valor Total**
1	Serviço de Gestão de Vulnerabilidades	12	R$ 45.738,54	R$ 548.862,43
2	Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança	12	R$ 64.990,13	R$ 779.881,53
3	Serviço de Operação e Resposta a Requisições	12	R$ 26.858,43	R$ 322.301,12
		TOTAL:	**R$ 137.587,09**	**R$ 1.651.045,08**

18.2. As despesas decorrentes do certame tem adequação orçamentária e financeira com a Lei Orçamentária Anual e compatibilidade com o Plano Plurianual e com a Lei de Diretrizes Orçamentárias, podendo ser enquadrada, na seguinte Classificação Orçamentária 2022.0201.01.032.4200.4215.03.15000100.90 na Natureza de Despesa 3.3.90.40.28 - Outros Serviços Técnicos Especializados de Tecnologia da Informação, sendo o valor total de R$ 1.651.045,08 (um milhão, seiscentos e cinquenta e um mil e quarenta e cinco reais e oito centavos), sendo que para o exercício de 2022 o valor de R$ 137.587,09 (cento e trinta e sete mil, quinhentos e oitenta e sete reais e nove centavos).

19. DO TERMO DE CONTRATO

19.1. As condições contratuais constam da Minuta de Contrato, Anexo II deste Edital.

19.2. Homologada a licitação pela autoridade competente, o TCE/GO emitirá a(s) nota(s) de empenho e firmará o Contrato com a empresa adjudicatária, visando o fornecimento do objeto desta licitação, nos termos da Minuta que integra este Edital.

19.3. A empresa adjudicatária deverá comparecer para firmar o contrato, **no prazo máximo de 03 (três) dias úteis**, contados da data da convocação. Caso a adjudicatária seja uma empresa estrangeira, este prazo poderá ser adiado até 15 (quinze) dias.

19.4. Na hipótese de a empresa adjudicatária não atender a condição acima ou recusar a assinar o contrato e não apresentar justificativa porque não o fez, decairá o direito à contratação, conforme preceitua o art. 4º, inciso XVI e XXIII, da Lei nº. 10.520/02, e o pregoeiroconvocará outro licitante classificado e, assim, sucessivamente, na ordem de classificação, sem prejuízo da aplicação das sanções cabíveis observados o disposto no artigo 7º da mesma lei.

19.5. A execução do contrato será acompanhada e fiscalizada por servidor indicado pelo TCE-GO.

19.6. Como condição para celebração do Contrato, a empresa adjudicatária deverá manter as mesmas condições de habilitação exigidas na licitação.

19.7. O presente Edital e seus anexos, bem como a proposta de preços da empresa adjudicatária, farão parte integrante do Contrato a ser firmado, independentemente de transcrição.

19.8. Pela inexecução total ou parcial do Contrato, a Administração poderá, garantida a prévia defesa, aplicar à CONTRATADA as sanções de que tratam a Lei Federal nº 10.520/2002 c/c com os arts. 77 a 83 da Lei de Licitações e Contratos do Estado de Goiás nº 17.928/2012.

20. DA VIGÊNCIA CONTRATUAL

20.1. A vigência da contratação será de 12 (DOZE) meses à partir da assinatura do contrato, podendo ser prorrogado até o limite de 60 (sessenta) meses.

20.2. Para efeitos de continuidade da vigência contratual, a cada 12 (doze) meses, todos os itens são considerados como serviços de natureza continuada, e poderão ser renovados anualmente até o limite de 60 (sessenta) meses.

20.3. A CONTRATADA deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei nº 8.666/93.

21. DOS CRITÉRIOS DE REAJUSTE

21.1 A periodicidade para eventual reajuste de preços do contrato será anual, contando-se a partir da data da limite para apresentação da proposta comercial pela CONTRATADA e aceita pela CONTRATANTE, ou do último reajuste, adotando-se como parâmetro o Índice de Custo da Tecnologia da Informação (ICTI), ocorrido nos últimos 12 (doze) meses, e ainda, os preços praticados no mercado e a negociação entre as partes.

22. DAS SANÇÕES ADMINISTRATIVAS

22.1 Ficará impedido de licitar e de contratar com o Estado e será descredenciado no CADFOR, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato, além das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

a) não assinar o contrato ou a ata de registro de preços;

b) não entregar a documentação exigida no edital;

c) apresentar documentação falsa;

d) causar o atraso na execução do objeto;

e) não mantiver a proposta;

f) falhar na execução do contrato;

g) fraudar a execução do contrato;

h) comportar-se de modo inidôneo;

i) declarar informações falsas; e

j) cometer fraude fiscal.

22.2. As sanções serão registradas e publicadas no CADFOR.

22.3. As sanções descritas no item 24.1, também se aplicam aos integrantes do cadastro de reserva em pregão para registro de preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.

22.4. A multa poderá ser descontada dos pagamentos eventualmente devidos ou ainda, quando for o caso, cobrada judicialmente.

22.5. Pela inexecução parcial ou total das condições pactuadas, garantida a prévia defesa, ficará a CONTRATADA sujeita às seguintes sanções:

a) Advertência;

b) Multa sobre o valor total do contrato, observados os seguintes limites:

I - 10% (dez por cento) sobre o valor do contrato ou instrumento equivalente, em caso de descumprimento total da obrigação, inclusive no caso de recusa do adjudicatário em assinar o Contrato ou retirar o instrumento equivalente, dentro de 10 (dez) dias contados da data de sua convocação;

II - 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do serviço não realizado;

III - 0,7% (sete décimos por cento) sobre o valor da parte do serviço não realizado, por cada dia subsequente ao trigésimo.

c) Impedimento de licitar e contratar com a Administração Pública Estadual e descredenciamento do CADFOR pelo prazo de até 5 (cinco) anos.

22.5.1. A inexecução contratual também poderá dar causa à rescisão contratual, nos moldes da Lei n° 8.666/93.”

22.6. A multa, aplicada após regular processo administrativo, será recolhida em favor do CONTRATANTE, no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente, ou será descontada dos pagamentos devidos à CONTRATADA ou, ainda, quando estas não ocorrerem ou não forem suficientes, o saldo será inscrito na Dívida Ativa do Estado e cobrado judicialmente.

22.7. A critério da Administração poderão ser suspensas as penalidades, no todo ou em parte, quando o atraso no fornecimento dos itens ou da prestação dos serviços for devidamente justificado pela CONTRATADA e aceito pela Administração da CONTRATANTE, que fixará novo prazo, improrrogável, para a completa execução das obrigações assumidas.

22.8. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isolada ou cumulativamente, sem prejuízo de sanções de que tratam a Lei Federal n° 10.520/2002” e na Lei Estadual nº 17.928/2012.

22.9. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, com oportunidade de defesa prévia da interessada, no respectivo processo, no prazo de 5 (cinco) dias úteis, observando-se o procedimento previsto na Lei nº 8.666, de 1993 e, subsidiariamente, na Lei Estadual nº 13.800, de 2001.

22.10. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

23. DA FRAUDE E DA CORRUPÇÃO

23.1. Os licitantes deverão observar os mais altos padrões éticos durante o processo licitatório e a execução do Contrato, estando sujeitos às sanções previstas na legislação aplicável.

24. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

24.1. A CONTRATANTE e a CONTRATADA deverão cumprir integralmente as obrigações estabelecidas nos item **10** e **11** do Termo de Referência e nas Cláusulas Terceira e Quarta da Minuta Contratual, que fazem parte integrante do presente Edital.

25. DAS DISPOSIÇÕES GERAIS

25.1. Esta Licitação poderá ser revogada por interesse do contratante, em decorrência de fato superveniente devidamente comprovado, pertinente e suficiente para justificar o ato, ou anulada por vício ou ilegalidade, a modo próprio ou por provocação de terceiros, sem que o licitante tenha direito a qualquer indenização.

25.2. Qualquer modificação no presente Edital será divulgada pela mesma forma que se divulgou o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação da proposta de preços.

25.3. O pregoeiroou à Autoridade Competente, é facultada, em qualquer fase desta Licitação a promoção de diligência, destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documentos ou informações que deveriam constar do mesmo desde a realização da sessão pública.

25.4. Os licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase desta Licitação.

25.5. Após apresentação da proposta de preços não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro .

25.6. A homologação do resultado desta Licitação não implicará direito à contratação do objeto pelo TCE-GO.

25.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento, vencendo-se os prazos somente em dias de expedientes normais.

25.8. O desatendimento de exigências formais não essenciais, não importará no afastamento do licitante, desde que sejam possíveis a aferição da sua qualificação, e a exata compreensão da sua proposta de preços, durante a realização da sessão pública do Pregão Eletrônico.

25.9. Para fins de aplicação das sanções administrativas constantes no presente Edital, o lance é considerado proposta de preços.

25.10. As normas que disciplinam este Pregão Eletrônico serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento do interesse do comprador, a finalidade e a segurança da contratação.

25.11. O objeto da presente Licitação poderá sofrer acréscimos ou supressões, conforme previsto no § 1° do Art. 65 da Lei Federal n.º 8.666/93.

25.12. Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do CONTRATADO de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do Contrato.

25.13. O Edital e seus Anexos, além de poderem ser visualizados nos sites www.licitacoes-e.com.br e www.tce.go.gov.br, poderão ser obtidos na sede do Tribunal de Contas do Estado de Goiás (com prévio recolhimento de taxas limitado ao valor do custo efetivo de reprodução gráfica da documentação fornecida, conforme art. 32, § 5° da Lei 8.666/93 e Decreto Estadual n° 5.721/03), localizado na Avenida Ubirajara Berocan Leite, nº 640, Setor Jaó, telefone: (62) 3228-2852/2616, CEP 74.674-015.

25.14. Em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais e Lei Complementar nº 131 – Lei da Transparência, a participação no presente certame pressupõe a aceitação de que os dados pessoais fornecidos pelos licitantes no decorrer do procedimento licitatório serão de conhecimento público, podendo ser divulgados no Portal do TCE-GO.

25.15. Quaisquer informações complementares sobre o presente Edital e seus Anexos poderão ser obtidas pelos telefones (62) 3228-2852/2616 (Tribunal de Contas do Estado de Goiás – Comissão Permanente de Licitação) ou pelo e-mail: *cpl@tce.go.gov.br.*

25.16. Na hipótese de procedimento judicial, fica eleito o Foro da Comarca de Goiânia - Goiás, para dirimir eventuais pendências oriundas do presente pregão, com renúncia de qualquer outro, por mais privilegiado que seja.

Goiânia, 23 de novembro de 2022.

Luis Carlos de Gouveia Coelho
PREGOEIRO

Lídia Laborão Meirelles
EQUIPE DE APOIO

Artur Eduardo Lopes da Silva
EQUIPE DE APOIO

Rafael do Nascimento Moreira
EQUIPE DE APOIO

ANEXO II

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO Nº 202200047003608

TERMO DE REFERÊNCIA

CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

1. OBJETO

A presente licitação tem por objeto a contratação de empresa especializada para fornecimento de serviços gerenciados de segurança da informação ao Tribunal de Contas Estado de Goiás (TCE-GO), compreendendo: Serviço de gestão de vulnerabilidades, Serviço de monitoramento, triagem, tratamento e resposta a incidentes de segurança e Serviço de operação e resposta a requisições, por 12 (doze) meses, de acordo com as especificações constantes deste Termo de Referência e seus anexos.

2. DETALHAMENTO DO OBJETO

2.1. Os Serviços Gerenciados de Segurança da Informação envolvem a prestação dos seguintes serviços:

2.1.1. **Serviço de gestão de vulnerabilidades**, que tem por objetivo, de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação na infraestrutura e aplicações do TCE-GO, a fim de evitar que ataques cibernéticos direcionados a este Tribunal obtenham sucesso explorando vulnerabilidades conhecidas.

2.1.2. **Serviço gerenciado de monitoramento, triagem, tratamento e resposta a incidentes de segurança**, que visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao TCE-GO, através do fornecimento de solução de correlacionamento de logs, pacotes de rede e/ou comportamento anômalo de aplicações, serviços e infraestrutura que possam gerar eventos/incidentes de segurança da informação, os quais devem ser analisados, remediados, contidos e documentados. Tais serviços deverão ser executados através de um Centro de Operações de Segurança, obedecendo os principais frameworks de resposta a incidentes de segurança da informação e boas práticas de mercado já conhecidas.

2.1.3. **Serviço de operação e resposta a requisições**, que tem por objetivo sustentar, operar e gerenciar as soluções de Firewall e Antivírus, definir e realizar de forma periódica, ações proativas de acompanhamento de todo o parque computacional, a fim de mantê-lo sempre estável, disponível, íntegro e confiável.

2.2. Todos os serviços descritos pertencem a um único objeto e bloco de contratação denominado SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

3. REQUISITOS E ESPECIFICAÇÕES DOS SERVIÇOS

3.1. Os requisitos e especificações dos serviços objetos desta contratação constam no Anexo IV deste Termo de Referência.

4. MOTIVAÇÃO E JUSTIFICATIVA

4.1. De acordo com a Resolução Administrativa 19/2022, publicada no Diário Eletrônico de Contas do TCE-GO em 11 de outubro de 2022, compete à Diretoria de Tecnologia da Informação, dentre outros pontos, planejar, organizar, dirigir e controlar a política de segurança da informação, bem como gerir e operacionalizar a segurança da informação por meio da gestão dos ativos de informação do Tribunal.

4.2. O TCE-GO possui uma infraestrutura de Tecnologia da Informação e Comunicação (TIC) bem heterogênea, com ativos de vários tipos: rede de comunicação de dados, telefonia, banco de dados, servidores de aplicação, sistemas operacionais, sistemas de backup e recursos de armazenamento e processamento de dados distribuídos. Além de todos esses ativos, existe também os que sustentam e garantem a confiabilidade e integridade dos demais ativos de TIC, os ativos de segurança.

4.3. Buscando entregar serviços com adequado nível de qualidade e eficiência, a área de TI do TCE-GO investe no aprimoramento das práticas de gestão desse ambiente tecnológico com base em modelos de melhores práticas internacionalmente reconhecidos, sendo relevante citar aqui a necessidade de aplicar recomendações e controles presentes na norma ABNT NBR ISO/IEC 27001:2013.

4.4. A infraestrutura de segurança atualmente implantada no TCE-GO é composta por diversas tecnologias de hardware e software, as quais fornecem serviços de segurança com o objetivo de proteger o ambiente computacional de ataques cibernéticos e outras ameaças externas e internas. Entre as tecnologias e soluções em uso, destacam-se: solução de firewall, proxy/web filter, antivírus e sistema antispam.

4.5. No entanto, considerando a importância vital que os sistemas e serviços de TI adquiriram para as organizações e que se observa a constante diversificação e desenvolvimento de novas ameaças cibernéticas, são mandatórios a constante evolução, o aprimoramento dos mecanismos de segurança, bem como o desenvolvimento de equipes e de métodos de segurança cada vez mais complexos.

4.6. Portanto, verifica-se que o atual modelo de contratações, por meio da compra de produtos, não é suficiente para fazer frente à velocidade com que surgem novos tipos de ameaças, e principalmente a velocidade com que o mercado de segurança evolui e lança novos produtos. Para endereçar tais desafios desenvolveu-se internacionalmente (Gartner) o conceito de Managed Security Services – MSS. Neste modelo, empresas especialistas de segurança atuando por meio de Centros de Operações de Segurança (Security Operations Center – SOC), ofertam diversas soluções de segurança na modalidade de serviço. As maiores vantagens desta modalidade são:

- Maior flexibilidade com relação à aquisição de produtos;

- Os serviços podem ser contratados sob demanda, conforme a necessidade e disponibilidade financeira do cliente;
- Maior velocidade de inserção de novas tecnologias;
- Utilização de profissionais altamente capacitados e especialistas em cibersegurança, que dificilmente atuariam em um único cliente de pequeno porte;
- Menor custo total de propriedade (Total Cost of Ownership – TCO), tendo em vista os custos de compra, operação e capacitação contínua a longo prazo.

4.7. Além disso, é primordial aprimorar a atuação preventiva, elevar o grau de detecção de comportamentos anômalos e desenvolver o processo de gestão de incidentes de segurança, agilizar a resposta a esses incidentes e melhorar a percepção de segurança perante os usuários do TCE-GO e a sociedade. Estes objetivos serão perseguidos nesta contratação pela criação e revisão dos níveis de serviço, para que estes estejam condizentes com a importância que a segurança da informação possui para a instituição.

4.8. O uso de serviços gerenciados de segurança (MSSs) é uma abordagem cada vez mais popular para atingir as metas de segurança da informação, reduzir riscos e suprir a lacuna de habilidades de segurança da organização e assim, aprimorar a qualidade e a percepção de entrega de valor dos serviços prestados pelo Serviço de Infraestrutura e Segurança em TI da Diretoria de Tecnologia da Informação.

4.9. Com base no exposto e na Análise Técnica Preliminar (Anexo I), o TCE-GO entende como necessária a contratação de empresa especializada em prover serviços de operação e monitoramento de segurança da informação para atuar em seu ambiente de forma padronizada, tendo como principais atividades:

- Operar e gerir os ativos de segurança da informação;
- Monitorar o ambiente de tecnologia da informação em regime 24x7x365;
- Executar todo o processo de triagem de eventos, informando ao TCE-GO os eventos de exceção que se transformam em incidentes;
- Responder aos incidentes cibernéticos ocorridos no ambiente do TCE-GO.

5. CRITÉRIOS DE AGRUPAMENTO EM LOTE ÚNICO

5.1. Um ponto fundamental para se garantir a viabilidade técnico-administrativa de tal aquisição é o de que o conjunto dos serviços gerenciados de segurança da informação sejam licitados em lote único, portanto com adjudicação para um único licitante vencedor. Os principais balizadores desta definição estão descritos a seguir:

5.1.1. A definição pela contratação dos serviços em lote único levou em consideração o prejuízo de ordem técnica que poderiam ocorrer casos os serviços fossem prestados por diferentes empresas, uma vez que os serviços a serem contratados guardam estreita relação entre si e dependem de forte integração para que sejam efetivos e alcancem os resultados pretendidos.

5.1.2. O agrupamento de itens em um único lote, na realização dos pregões eletrônicos, é orientação constante do Acórdão nº 861/2013 - Plenário, do Tribunal de Contas da União: “São lícitos os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si”.

5.1.3. Destaca-se que a contratação de forma global, garante tanto a unicidade dos processos, aferição dos níveis de serviços, como a otimização dos recursos necessários à gerência e fiscalização do contrato.

5.1.4. A contratação global também evita o risco de contratações conflituosas entre si, pois os serviços especificados dependem também do fornecimento de equipamentos e softwares que necessitarão de total integração, evitando-se que os produtos apresentem problemas de incompatibilidade.

5.1.5. As contratações em separado apresentariam também o alto risco de ocorrer, no decorrer da vigência do contrato, conflitos entre diferentes prestadoras de serviço em que as contratadas atribuam culpa a terceiros por descumprimentos de suas responsabilidades.

5.1.6. 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 tácticas e técnicas de ataque para que, por meio da atuação conjunta (Purple Team), aumente-se a efetividade da proteção do ambiente.

6. INSPEÇÕES E DILIGÊNCIAS

6.1. O TCE-GO reserva-se o direito de efetuar inspeções e diligências para sanar quaisquer dúvidas existentes, podendo efetuá-las previamente à contratação.

6.2. O TCE-GO poderá realizar diligência nos Centros de Operações de Segurança da CONTRATADA antes do início da prestação do serviço, in loco, a fim de validar e aferir se TODOS os itens solicitados neste Termo de Referência serão atendidos.

6.3. A contratação não será formalizada caso não haja o atendimento de quaisquer itens previstos neste Termo de Referência e seus anexos.

7. VISITA TÉCNICA

7.1. É facultada aos licitantes a vistoria nas dependências do TCE-GO, para proporcionar conhecimento necessário à elaboração da proposta comercial.

7.2. A visita técnica é facultativa, sendo de responsabilidade da empresa contratada eventuais prejuízos em virtude de sua omissão na verificação do local de implantação da solução contratada.

7.3. Fica a critério das licitantes realizar visita ao local onde serão realizados os serviços, no prédio sede do Tribunal de Contas do Estado de Goiás, localizado na Av. Ubirajara Berocan Leite, Nº 640. Setor Jaó, na cidade de Goiânia – GO.

7.4. As visitas destinam-se à vistoria, avaliação e ciência das empresas interessadas acerca das condições do local e peculiaridades atinentes à realização dos serviços que compõem o objeto da licitação, para fins de elaboração da proposta.

7.5. O agendamento das vistorias deverá ser previamente efetuado por intermédio do e-mail: informatica@tce.go.gov.br, cujo campo “assunto” da mensagem deverá conter o texto “Vistoria – CONTRATAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

7.6. As visitas deverão ser feitas por profissional qualificado da empresa interessada, o qual deverá estar munido de documento de identificação e de instrumento que o habilite à representação legal da empresa.

7.7. No dia e hora a ser agendado, o servidor designado pelo TCE-GO acompanhará a visita das empresas interessadas, com o objetivo de esclarecer as possíveis dúvidas dos serviços que compõem o objeto da licitação.

7.8. O TCE-GO emitirá atestado de vistoria técnica que deverá ser anexado junto à documentação de habilitação.

A vistoria deverá ser pré-agendada com pelo menos 1 (um) dia útil de antecedência e poderá ser realizada até 02 (dois) dias úteis antes da data prevista para a realização do certame.

8. VIGÊNCIA DO CONTRATO

8.1. A vigência da contratação será de 12 (DOZE) meses à partir da assinatura do contrato, podendo ser prorrogado até o limite de 60 (sessenta) meses.

8.2. Para efeitos de continuidade da vigência contratual, a cada 12 (doze) meses, todos os itens são considerados como serviços de natureza continuada, e poderão ser renovados anualmente até o limite de 60 (sessenta) meses.

8.3. A CONTRATADA deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei nº 8.666/93.

9. HABILITAÇÃO TÉCNICA

9.1. A LICITANTE deverá apresentar Cópia Autenticada de Atestado(s) de Capacidade Técnica, ou original fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) a experiência na prestação de Serviços Gerenciados de Segurança da Informação similares aos especificados neste Termo de Referência e seus anexos, por pelo menos 6 meses, em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana.

9.2. Serão considerados compatíveis os atestados que comprovem a prestação de SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, com as seguintes parcelas de maior relevância:

9.2.1. Serviço de Gestão de Vulnerabilidades, por meio do fornecimento, instalação, prestação de serviços de suporte, administração e operação da solução para no mínimo 500 (quinhentos) ativos de TI. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado como SERVIÇO DE GESTÃO VULNERABILIDADES exigido neste certame.

9.2.2. Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança, utilizando tecnologia de SIEM (Security Information and Event Management) para gerenciamento e correlação de eventos de segurança através da análise de logs e pacotes, em redes com, no mínimo, 500 (quinhentos) ativos de TI. Este item visa atestar a capacidade da licitante para o fornecimento do serviço especificado como SERVIÇO GERENCIADO DE MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA exigido neste certame.

9.2.3. Serviço de Gestão e Operação de soluções de coleta e proteção contra riscos digitais, incluindo o fornecimento e prestação de serviços, administração e operação da solução para no mínimo 100 (cem) ativos. Este item visa atestar a capacidade da licitante para o fornecimento do SERVIÇO DE OPERAÇÃO E RESPOSTA A REQUISIÇÕES exigido neste edital.

9.3. Será permitido o somatório de atestado(s) de capacidade técnica para efeito de comprovação de experiência na prestação dos serviços de características técnicas semelhantes ao objeto desta contratação, não se exigindo que todos tenham sido prestados a uma única pessoa jurídica de direito público ou privado.

9.4. Para confirmação da qualificação técnica das empresas o TCE-GO poderá a seu critério, sem comunicação prévia visitar as instalações da proponente, devendo na ocasião serem comprovadas as informações documentais.

9.5. O Atestado de Capacidade Técnica apresentado deverá conter, no mínimo, as seguintes informações:

a) Dados da empresa licitante: nome e CNPJ;
b) Dados da empresa cliente: nome e CNPJ;
c) Descrição dos serviços/fornecimento com dados que permitam o amplo entendimento dos trabalhos realizados e identifiquem a compatibilidade e semelhança com objeto da licitação;
d) Dados do emissor do atestado: nome e contato;
e) Data de emissão e assinatura do emissor;

9.6. Não serão aceitos atestados/declarações emitidos pela própria LICITANTE.

9.7. O TCE-GO realizará diligências objetivando comprovar a veracidade das informações prestadas pela LICITANTE.

10. OBRIGAÇÕES DA CONTRATADA

10.1. Fornecer os produtos e prestar os serviços requeridos nas condições e prazos estipulados neste Termo de Referência e seus anexos;

10.2. Observar os processos de trabalho, políticas e normas internas do TCE-GO;

10.3. Assumir a responsabilidade, sem qualquer espécie de solidariedade por parte do TCE-GO, pelos encargos previdenciários e obrigações sociais previstas na legislação em vigor, obrigando-se a saldá-los na época própria, bem como pelos encargos fiscais e comerciais resultantes da contratação e pelos decorrentes de eventual demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência;

10.4. Manter-se, durante o período de vigência do contrato, em compatibilidade com as condições de habilitação e qualificação exigidas na licitação;

10.5. Planejar, desenvolver, implantar, executar e manter os serviços de acordo com os níveis de serviço estabelecidos neste Termo de Referência e seus anexos;

10.6. Reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no todo ou em parte, serviços efetuados nos quais se verificar vícios, defeitos ou incorreções;

11. OBRIGAÇÕES DO TCE-GO

11.1. Respeitar a titularidade do direito autoral, patrimonial e comercial da CONTRATADA sobre os produtos fornecidos, seus componentes de software, suas adaptações, derivações e customizações resultantes da execução dos serviços objeto deste Termo de Referência, comprometendo-se a não doar, ceder, disponibilizar e permitir o manuseio e utilização dos códigos-fonte e componentes de software por terceiros ou praticar qualquer outra forma de transferência dos aplicativos sem anuência da CONTRATADA, conforme legislação específica;

11.2. Acompanhar e fiscalizar os serviços, quanto aos aspectos qualitativos e quantitativos, anotando em registro próprio as falhas e solicitando as medidas corretivas;

11.3. Tomar providências necessárias para que sejam seguidas as recomendações da CONTRATADA, concernentes às condições de uso correto da solução;

12. ORÇAMENTO ESTIMADO

12.1. O valor global máximo aceito para a contratação é de R$ 1.651.045,08 (Um milhão e seiscentos e cinquenta e um mil e quarenta e cinco reais e oito centavos).

SERVIÇOS CONTINUADOS SOB PROGRAMAÇÃO

Item	Descrição	Parcelas	Valor Mensal	Valor Total
1	Serviço de Gestão de Vulnerabilidades	12	R$ 45.738,54	R$ 548.862,43
2	Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança	12	R$ 64.990,13	R$ 779.881,53
3	Serviço de Operação e Resposta a Requisições	12	R$ 26.858,43	R$ 322.301,12
		TOTAL:	**R$ 137.587,09**	**R$ 1.651.045,08**

13. CONDIÇÕES DE PAGAMENTO

13.1. Será emitida nota de empenho em favor da empresa adjudicatária, após a homologação da licitação, caso se efetive a contratação.

13.2. O pagamento será efetuado mensalmente de acordo com os valores estipulados no Contrato Administrativo firmado com a CONTRATADA, sendo realizado de acordo com as Ordens de Serviço ou de Fornecimento de Bens;

13.3. Os serviços entregues serão homologados pelos Fiscais e Gestor do Contrato;

13.4. A Aceitação dar-se-á após a assinatura do TERMO DE RECEBIMENTO DEFINITIVO;

13.5. O Tribunal de Contas do Estado de Goiás - efetuará o pagamento até o 30º (trigésimo) dia do mês subsequente à entrega definitiva devidamente atestada pela Diretoria de Tecnologia da Informação.

13.6. O pagamento será creditado em favor da adjudicatária, por meio de Ordem Pagamento, em qualquer instituição bancária indicada na Nota Fiscal, devendo, para isto, ficar especificado o nome do banco, agência com a qual opera, localidade e número da conta corrente em que deverá ser efetivado o crédito.

13.7. O TCE-GO não efetuará pagamento por meio de títulos de cobrança bancária.

13.8. Qualquer erro ou omissão ocorrido na documentação fiscal será motivo de correção por parte da adjudicatária e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente sanado.

13.9. Quando do pagamento a ser efetuado pelo Tribunal de Contas do Estado de Goiás, a adjudicatária deverá comprovar sua regularidade no tocante à Documentação

Obrigatória (Receita Federal, Dívida Ativa da União, Estado e Município, FGTS, INSS e Justiça do Trabalho). Tal comprovação será objeto de confirmação “ON LINE”, sendo suspenso o pagamento, caso esteja irregular.

13.10. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação das obrigações, em virtude de penalidades impostas à CONTRATADA ou inadimplência total ou parcial referente à contratação.

13.11. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação das obrigações, em virtude de penalidades impostas à CONTRATADA ou inadimplência total ou parcial referente à contratação.

13.12. O TCE/GO reserva-se o direito de suspender o pagamento se o produto entregue estiver em desacordo com as especificações constantes no Edital e em seus Anexos.

14. ESCOPO, PRAZOS E FORMA DE ENTREGA

14.1. Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para a perfeita execução efetiva da prestação dos serviços.

14.2. O dimensionamento da equipe para a execução adequada do serviço contratado é de responsabilidade exclusiva do Fornecedor de Serviço, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência e seus anexos.

14.3. Dependendo da complexidade, criticidade e do prazo do projeto, os serviços poderão ser realizados nas instalações da CONTRATADA ou do TCE-GO.

14.4. Todos os custos com licenças de simuladores e softwares devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extras, seja a que título for.

14.5. O período de prestação dos serviços, a partir da emissão do termo de recebimento definitivo, será o estabelecido na tabela abaixo, observadas as etapas previstas no item EXECUÇÃO DOS SERVIÇOS do Anexo IV do presente Termo de Referência. As quantidades da tabela abaixo foram baseadas no ambiente especificado no Anexo III deste Termo de Referência e em estimativa de fluxo de dados no *switch* principal do TCE-GO.

DESCRIÇÃO	QTD	AFERIÇÃO	MÉTRICA	PERÍODO
SERVIÇO DE GESTÃO DE VULNERABILIDADES	1.000	Mensal	Por Ativo	12 meses
SERVIÇO GERENCIADO DE MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA	3.500	Mensal	EPS	12 meses
SERVIÇO DE OPERAÇÕES E RESPOSTAS AS REQUISIÇÕES	2	Mensal	Por solução de SI	12 meses

14.6. A partir da assinatura do contrato, correrão os seguintes prazos:

14.7. Reunião de início do projeto (kick-off): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pelo TCE-GO com 02 (dois) dias úteis de antecedência.

14.8. Entrega do Projeto Executivo: até 30 (trinta) dias corridos, contados a partir da reunião de início do projeto (kick-off);

14.9. O TCE-GO se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;

14.10. Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo TCE-GO, a respeito da manifestação sobre o Projeto Executivo;

14.11. A conclusão da fase de implantação dos serviços é de até 60 (sessenta) dias corridos, contados a partir da data de início da vigência do contrato, mediante a emissão do termo de recebimento definitivo pelo TCE-GO.

14.12. O termo de recebimento definitivo obedecerá os seguintes critérios:

14.13. O TCE-GO terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo, depois de finalizado o planejamento, customização e a instalação do ambiente;

14.14. A prestação dos serviços mensais iniciará somente a partir da emissão do termo de recebimento definitivo pelo TCE-GO;

14.15. Para todos os bens importados, caso necessários por parte da CONTRATADA, que sejam instalados nas dependências do TCE-GO, será necessária a apresentação dos respectivos comprovantes de origem.

14.16. Os Centros de Operações de Segurança da CONTRATADA deverão estar em pleno funcionamento, operando em regime 24x7x365, em até – no máximo – 90 (noventa) dias corridos, contados da data de início da vigência contratual.

15. SIGILO E PROPRIEDADE

15.1. A CONTRATADA deve manter a mais absoluta confidencialidade a respeito de quaisquer informações, dados, processos, modelos ou outros materiais de propriedade do TCE-GO ou de terceiros, aos quais tiver acesso em decorrência da prestação dos serviços objeto do contrato, ficando terminantemente proibida de fazer uso ou revelar estes, sob qualquer justificativa.

15.2. A CONTRATADA deverá observar, na condução de suas atividades, as diretrizes estabelecidas pela Política de Segurança da Informação do TCE-GO.

16. CONDIÇÕES GERAIS

16.1. Independente de declaração expressa, a simples participação nesta licitação implica a aceitação das condições estipuladas no presente Termo de Referência e submissão total às normas nele contidas.

16.2. Todos os produtos deverão ser fornecidos em sua versão/release mais recente.

16.3. A proposta comercial deverá conter o quantitativo, preço total para os 12 meses.

16.4. Os equipamentos deverão ser novos, sem instalações anteriores, em linha de produção, e sem previsão de encerramento, na data de entrega.

16.5. Por ocasião da entrega, a empresa CONTRATADA poderá entregar configuração superior à proposta apresentada e/ou equipamento aprovado, respeitando a qualidade de todos os componentes do equipamento, bem como as condições comerciais e técnicas previstas no Edital.

16.6. O proponente arrematante deverá enviar junto com a proposta, documentação do fabricante impressa (como por exemplo manuais, planilhas de especificações técnicas, cópias de páginas publicadas no site do fabricante, entre outros), que comprove o atendimento aos itens solicitados neste formulário de especificações técnicas.

16.7. Deverão ser fornecidos manuais em português ou inglês, cabos de energia, acessórios e programas de configuração necessários à operacionalização do equipamento.

ANEXO I – ESTUDO TÉCNICO PRELIMINAR

As organizações, sejam elas de qualquer segmento ou tamanho, cada vez mais utilizam os serviços da TIC - Tecnologia da Informação e Comunicação como meio para atingirem seus objetivos. Com a transformação digital cada vez mais presente nas organizações, riscos, ameaças e vulnerabilidades que antes não existiam, começaram a surgir. Dados e informações na nuvem, transações feitas através da Internet (acesso remoto) e redes sem fio (wi-fi) facilitam o dia a dia, mas também abrem brechas de segurança para ataques de hackers, roubo de informações e outras ameaças à segurança digital.

De acordo com o último relatório de violação de dados da Identity Theft Resource Center (ITRC), houve um aumento geral de 68% na exposição de registros, sensíveis ou não, nos EUA de 2020 para 2021. As violações de dados relacionadas a Ransomware dobraram em cada um dos últimos dois anos. Também segundo o relatório, na taxa de crescimento atual, os ataques de Ransomware passarão o Phishing como a principal causa de comprometimento de dados em 2022.

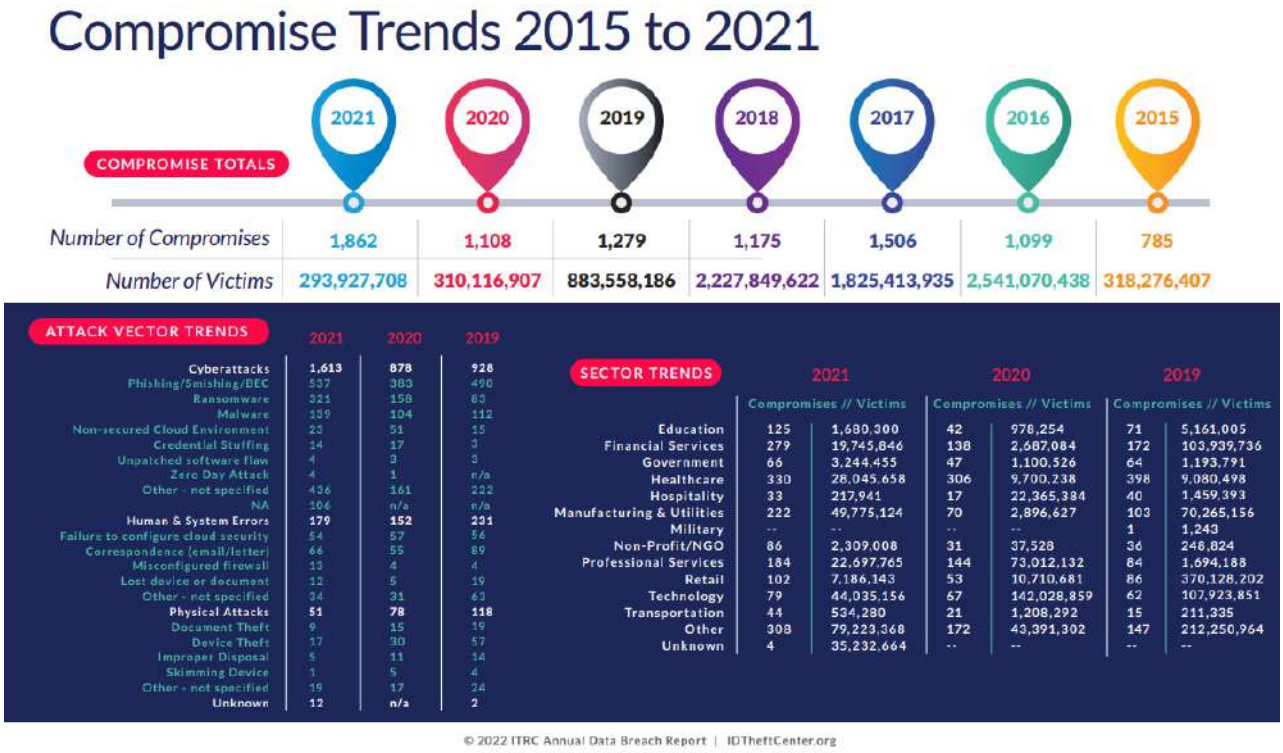


Figura 1 - Comprometimentos entre 2015 e 2021 - ITRC Annual Data Breach Report.

No Brasil, o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança), entidade responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira, mantém estatísticas sobre notificações de incidentes a ele espontaneamente reportadas, conforme Figura 2.

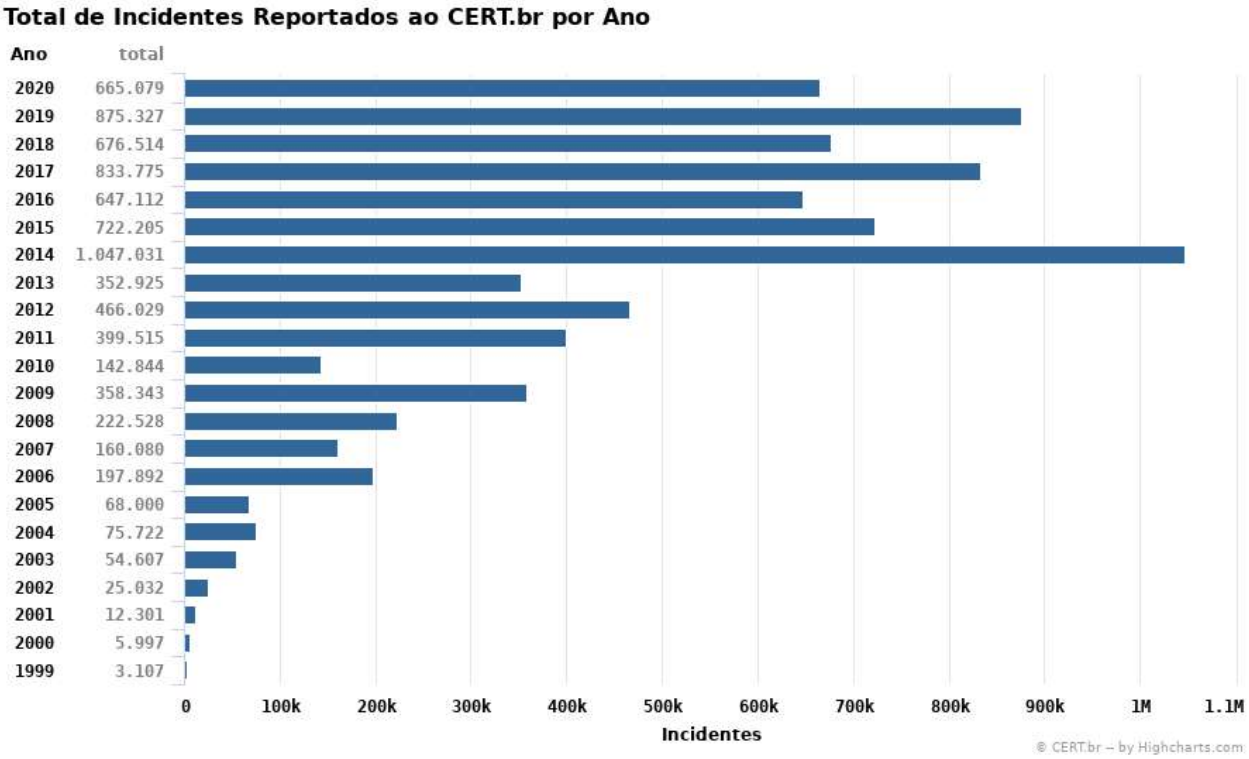


Figura 2 – Total de Incidentes Reportados ao CERT.br por Ano,

disponível em https://cert.br/stats/incidentes/ (acessado em 21/10/2022).

Na Figura 3 temos uma visão dos tipos de ataques reportados durante o ano de 2020.

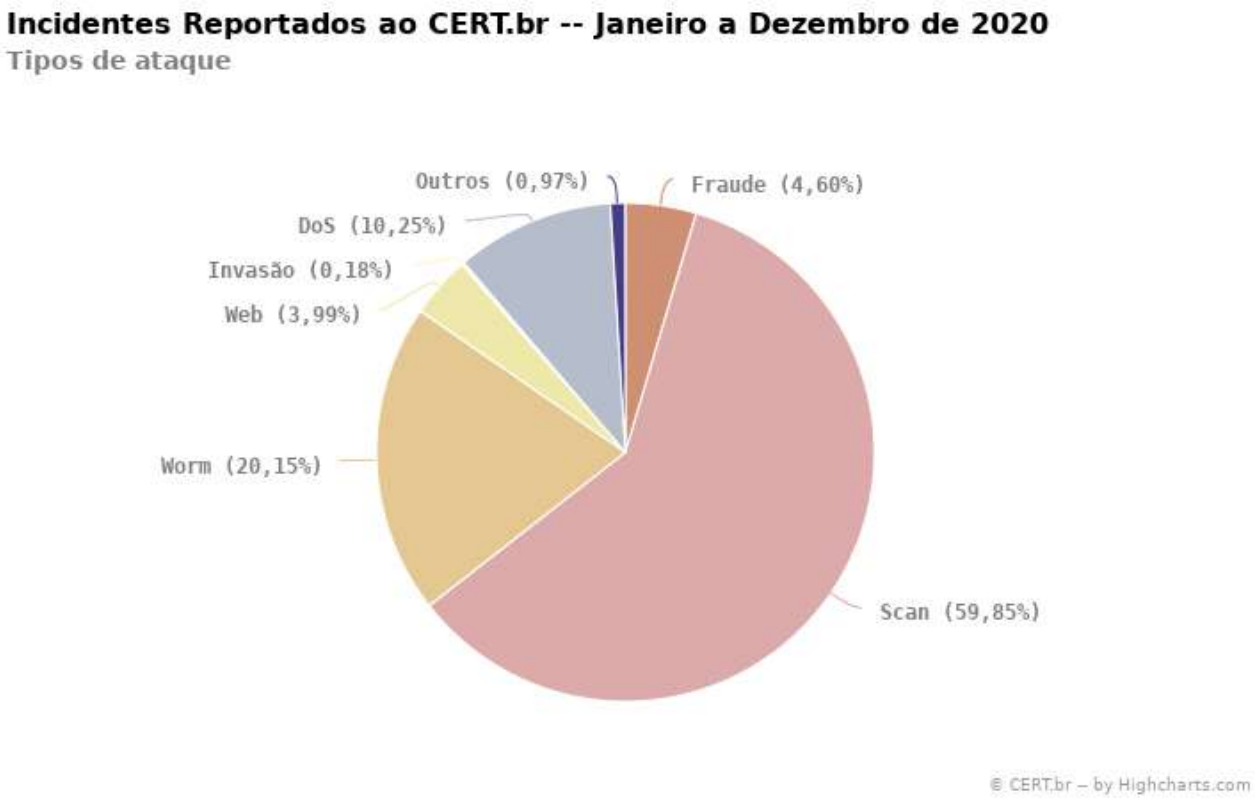


Figura 3- Tipos de Ataques Reportados ao CERT.br em 2020,

disponível em https://cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html (acessado em 21/10/2022).

Legenda:

- ***Worm:*** *notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.*
- ***DoS (Denial of Service):*** *notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.*
- ***Invasão:*** *um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.*
- ***Web:*** *um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.*
- ***Scan:*** *notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.*
- ***Fraude:*** *segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.*
- ***Outros:*** *notificações de incidentes que não se enquadram nas categorias anteriores.*
- ***Obs.:*** *Vale lembrar que não se deve confundir scan com scam. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.*

Na Figura 4 a seguir temos os percentuais de Scans reportados por porta.

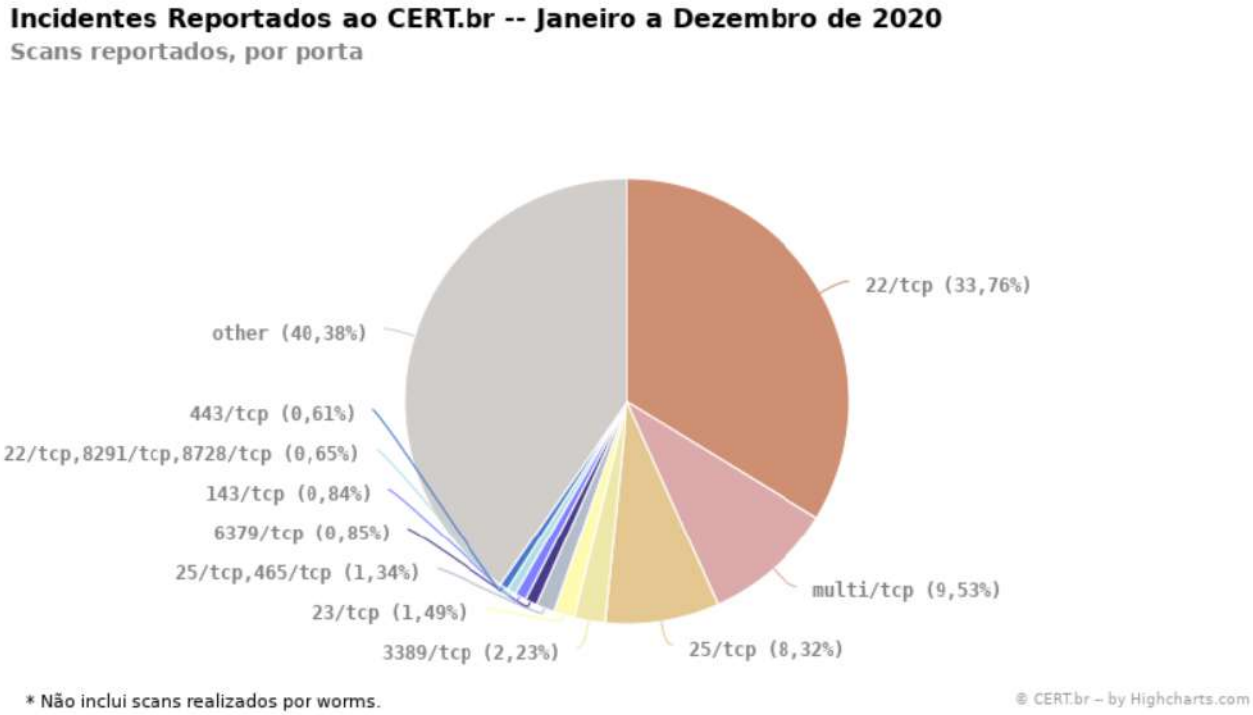


Figura 4 - Porcentagem de Scans por porta reportados em 2020,

disponível em https://cert.br/stats/incidentes/2020-jan-dec/scan-portas.html (acessado em 24/10/2022).

A Figura 5 a seguir apresenta os totais de notificações reportadas sobre equipamentos participando de ataques de negação de serviço (DoS – Denial of Service).

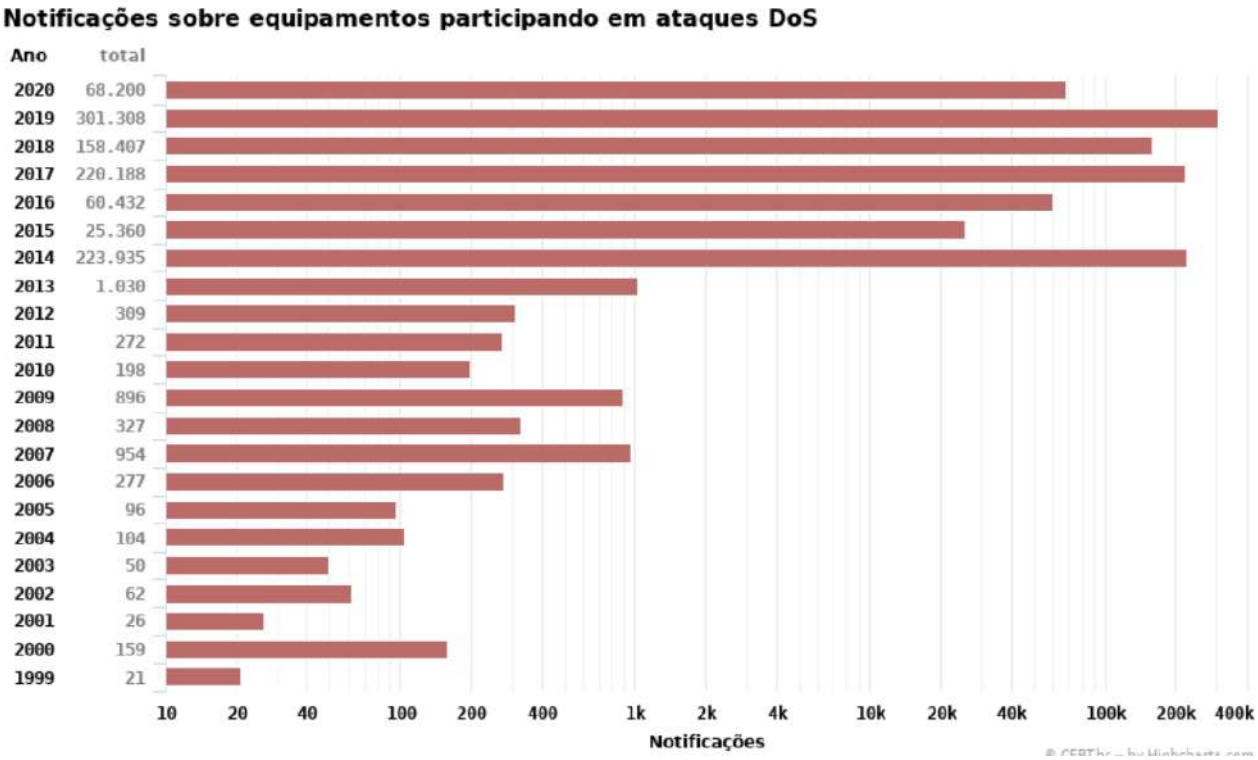


Figura 5 - Equipamentos participando de ataques DoS,

disponível em https://cert.br/stats/incidentes/2020-jan-dec/dos.html (acessado em 24/10/2022).

Já o gráfico a seguir apresenta os percentuais por tipo de tentativa de fraude no período analisado.

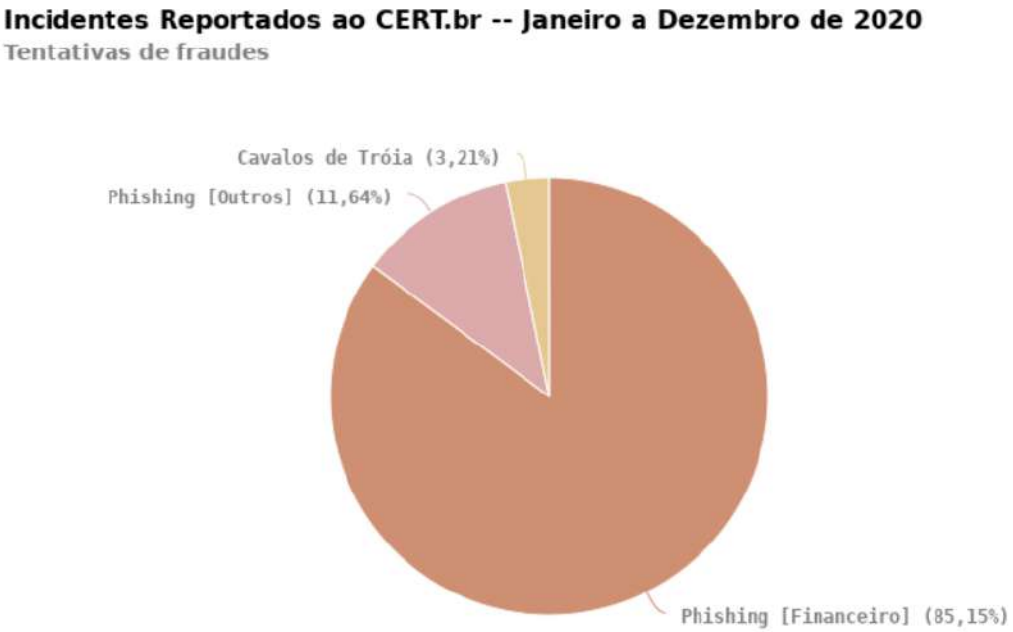


Figura 6 - Porcentagem por tipo de tentativa de fraude,

disponível em https://www.cert.br/stats/incidentes/2020-jan-dec/fraude.html (acessado em 25/10/2022).

Legenda:

- ***Cavalos de Tróia:*** *Tentativas de fraude com objetivos financeiros envolvendo o uso de cavalos de tróia.*
- ***Páginas Falsas:*** *Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.*
- ***Outras:*** *Outras tentativas de fraude.*

Na Figura 7 são apresentados os totais de incidentes reportados ao CERT.br considerando a origem do ataque.

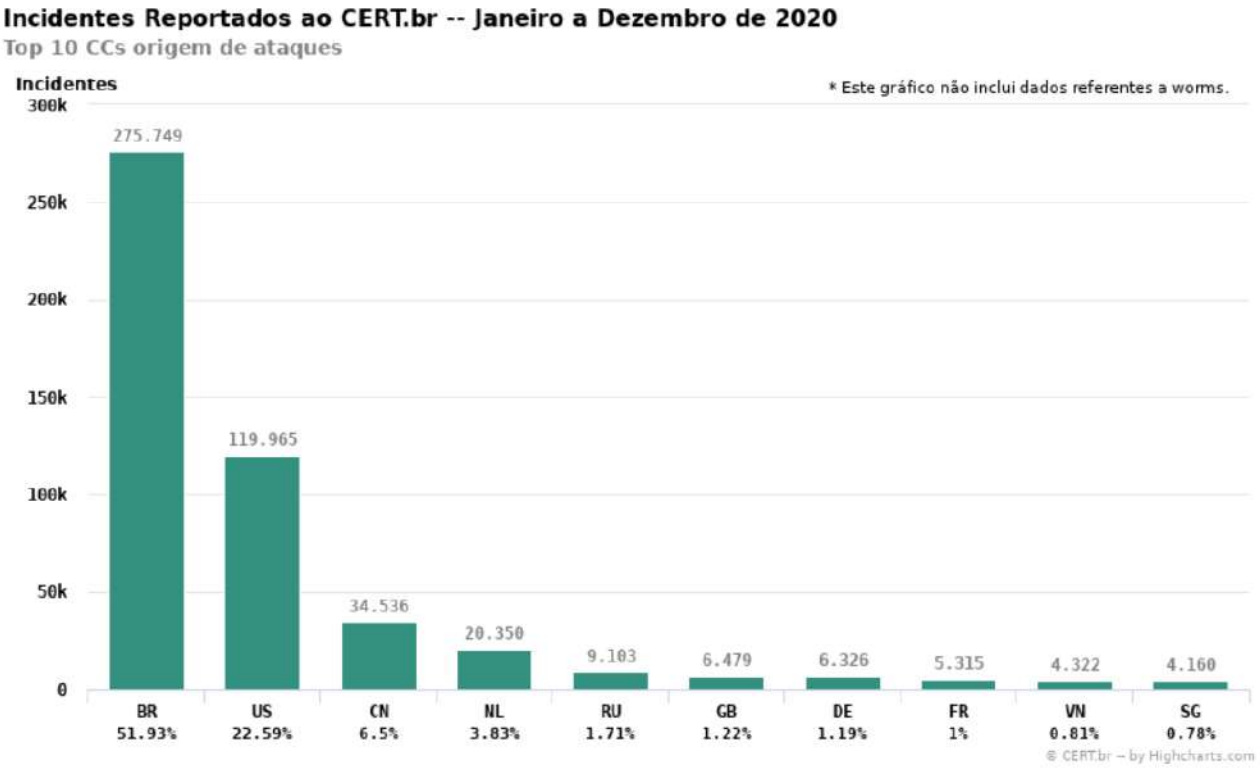


Figura 7 - Totais de incidentes reportados considerando a origem do ataque,

disponível em https://www.cert.br/stats/incidentes/2020-jan-dec/top-cc.html (acessado em 25/10/2022).

Diante desse cenário complexo e misto, a contratação de uma equipe dedicada ao monitoramento, prevenção e resposta a incidentes de segurança se torna imprescindível.

É possível perceber a função de um Security Operations Center (SOC), a partir do trecho extraído da brochura do Kaspersky for Security Operations Center (*https://media.kaspersky.com/en/business-security/enterprise/brochure-soc-powered-by-kl-eng.pdf*), conforme a seguir:

> *"As businesses learn to better protect themselves, criminals are simultaneously devising increasingly sophisticated techniques to penetrate their security barriers. Attracted by the unprecedented financial rewards that cyberattacks can deliver, growing numbers of threat actors are actively seeking and targeting undiscovered security flaws. In this environment, many organizations are establishing Security Operations Centers (SOCs) to combat security issues as they arise, providing a swift response and a decisive resolution."*

> *"À medida que as empresas aprendem a se proteger melhor, os criminosos estão simultaneamente planejando cada vez mais técnicas sofisticadas para penetrar em suas barreiras de segurança. Atraídos pelas recompensas financeiras sem precedentes que os ciberataques podem oferecer, um número crescente de atores de ameaças está ativamente buscando e direcionando falhas de segurança não descobertas. Nesse ambiente, muitas organizações estão estabelecendo Centrais de Operações de Segurança (SOCs) para combater os problemas de segurança à medida que surgem, fornecendo uma resposta rápida e uma resolução decisiva." (tradução livre)*

Partindo dessa percepção, um SOC (utilizaremos o acrônimo em inglês), é um ente centralizado com a função de monitoramento contínuo de ameaças, análise dessas ameaças, bem como, para prevenção e mitigação de incidentes de cibersegurança.

A crescente demanda pela eficiência na segurança da informação fez com que as organizações passassem a lidar com o assunto de forma mais estratégica. A formação de um Blue Team e um Red Team é um bom exemplo disso. Com atribuições específicas, as equipes promovem um trabalho de cibersegurança em nível mais elevado nas empresas. Cada uma delas tem sua importância e o alinhamento entre as duas traz inúmeros benefícios.

O Red Team é formado com o objetivo de realizar testes de ciberataque. Estamos falando de profissionais com alto conhecimento sobre as principais ameaças e ataques existentes, sendo capazes de simular tentativas de penetrar na rede e ou sistemas da organização. Com isso, eles se tornam capazes de identificar vulnerabilidades e, consequentemente, eliminá-las.

Resumidamente, eles assumem o papel de alguém que tentaria atacar a instituição — o que geralmente pode envolver a contratação de alguém de fora, sem o olhar acostumado àquele ambiente. Os ataques podem envolver engenharia social para enviar phishing aos funcionários, por exemplo.

O papel do Blue Team é justamente se opor aos ataques, inclusive aqueles ensaiados pelo Red Team. Assim, ele deve desenvolver estratégias para aumentar as defesas, modificando e reagrupando os mecanismos de proteção da rede para que eles se tornem mais fortes.

Um time desse tipo deve ter também um alto nível de conhecimento sobre a natureza das ameaças da rede. Entretanto, eles devem ser capazes não só de eliminar brechas, mas de reformular a infraestrutura de defesa como um todo.

Podemos extrair o que se entende por Blue Team, Red Team e Purple Team a partir das definições da autoridade mundial no tema, SANs:

- Blue Team:

> *"[...] focus is to defend the organization from digital/cyber attacks. In truth, while everything that improves the defensive security posture could be construed as Blue Team, there is an overt emphasis on discovering and defending against attacks". (https://wiki. sans.blue/#!index.md)*

"[...] focado em defender a organização de digital/cyber ataques. Na verdade, enquanto tudo que melhore a postura defensiva de segurança possa ser entendida como Blue Team, há uma ênfase na descoberta e defesa contra esses ataques". (tradução livre)

- Red Team:

"[...] would be those playing the role of the adversary. [...] So Red Team acts as Offense and Blue Team as Defense." (https://wiki.sans.blue/#!index.md)

"[...] seriam aqueles que atuam no papel de adversários. [...] Então o Red Team atua como ofensiva e Blue Team como defensiva." (tradução livre)

- Purple Team:

"[...] They typically report to a as a "third" team; think of it as a concept aimed at bringing the red and blue teams together to create purple team exercises. Red teams and blue teams should be encouraged to work as a joint team, to share insights beyond just reporting, to create a strong feedback loop, and to look for detection and prevention controls that can realistically be implemented for immediate improvement. " (https://www.sans.org/purple-team?msc=ptcourse- faq-lp)

"[...] Eles denominam-se como o "terceiro" time; pense nisso como um conceito que visa reunir as equipes vermelhas e azuis para criar exercícios de purple team. Equipes vermelhas e azuis devem ser incentivadas a trabalhar como uma equipe conjunta, para compartilhar ideias e não somente gerar relatórios, a criar um forte ciclo de feedback, e a procurar controles de detecção e prevenção que possam ser implementados realisticamente para melhoria imediata." (tradução livre)

A SANS (System Administration, Networking and Security) é uma empresa especializada em segurança da informação e treinamento em cybersegurança.

*"**SANS is the most trusted and by far the largest source for cybersecurity training in the world.** We offer training through several delivery methods including OnDemand (self paced) and instructor-led both Live Online (virtual) and In-Person. Our cybersecurity courses are developed by industry leaders in numerous fields including network security, digital forensics, offensive operations, cybersecurity leadership, industrial control systems, and cloud security. Courses are taught by real-world practitioners who are the best at ensuring you not only learn the material, but that you can apply it immediately when you return to the office. In addition to top-notch training, we offer certification via GIAC, an affiliate of the SANS Institute featuring over 35 hands-on, technical certifications in cyber security. We offer a Master's Degree, graduate and undergraduate certificate programs through SANS Technology Institute, as well as numerous free resources including newsletters, whitepapers and webcasts."*

*"**SANS é a mais confiável e de longe a maior fonte de treinamento em segurança cibernética do mundo.** Oferecendo treinamento por meio de vários métodos de entrega,*

incluindo OnDemand (individualizado) e ministrado por instrutor ao vivo online (virtual) e presencial. Os cursos de segurança cibernética são desenvolvidos por líderes do setor em diversos campos, incluindo segurança de rede, análise forense digital, operações ofensivas, liderança em segurança cibernética, sistemas de controle industrial e segurança em nuvem. Os cursos são ministrados por profissionais do mundo real que são os melhores em garantir que você não apenas aprenda o material, mas também que possa aplicá-lo imediatamente ao retornar ao escritório. Além do treinamento de alto nível, oferece certificação via GIAC, uma afiliada do SANS Institute com mais de 35 certificações técnicas práticas em segurança cibernética. Oferece programas de certificado de mestrado, pós-graduação e graduação por meio do SANS Technology Institute, bem como diversos recursos gratuitos, incluindo boletins, white papers e webcasts." (tradução livre)

Considerando as definições acima inseridas para Blue Team, Red Team e Purple Team, podemos afirmar, simplificadamente que o Blue Team é o elo de defesa e sua operação, o Red Team seria o ente de ataque o qual checa as defesas implementadas pelo Blue Team. O Purple Team seria o esforço coordenado envolvendo os dois grupos para examinar novas técnicas de invasão, desenvolver defesas melhoradas e enfrentar ataques de equipe vermelha.

De acordo com o modelo de arquitetura de segurança adaptativa proposto pelo Gartner, uma organização somente obterá sucesso na luta contra os crimes cibernéticos se seu SOC for capaz de predizer, prever, detectar e responder efetivamente as ameaças, conforme podemos visualizar na Figura 8.

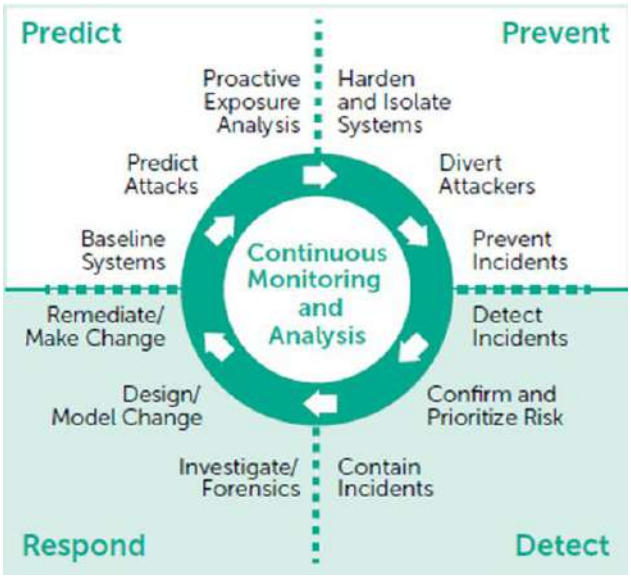


Figura 8 - Gartner, Designing an Adaptive Security Architecture for Protection From Advanced Attacks, February 2014.

(retirado da brochura do Kaspersky for Security Operations Center)

Levando esse modelo em consideração o TCE-GO tem por objetivo contratar serviços de segurança da informação para operação, monitoramento e defesa de seu ambiente.

ANEXO II – CATÁLOGO DE SERVIÇOS

1. INTRODUÇÃO

1.1. Este catálogo de serviços de apoio ao planejamento visa estabelecer e caracterizar grande parte dos serviços contemplados no objeto da contratação.

1.2. A estrutura deste catálogo é separada em três partes, de acordo com o tema da atividade:

a) Serviço de Gestão de Vulnerabilidades;

b) Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta A Incidentes de Segurança;

c) Serviço de Operação e Respostas a Requisições.

1.3. Cada demanda possui uma prioridade pré-estabelecida. Após o término da demanda, na fase de encerramento, a CONTRATADA poderá propor ao TCE-GO a atualização do catálogo. Se, por exemplo, uma determinada atividade vier a apresentar escopo maior do que o originalmente previsto no catálogo, esse processo permitirá medição mais precisa para demandas futuras. O TCE-GO poderá, assim, alterar a dimensão do escopo de determinado item no catálogo, tanto por provocação da CONTRATADA, como por iniciativa própria. O catálogo só poderá ser atualizado antes do início do desenvolvimento de determinada demanda.

1.4. A seguir apresentamos os itens do catálogo de serviços.

2. CATÁLOGO DE SERVIÇOS

Serviço de Gestão de Vulnerabilidades

Grupo de Serviço	ID	Serviço	ANS
Gestão de Vulnerabilidades	1	Checagem (Scan) e varredura diária	P4
	2	Checagem (Scan) e varredura semanal	P7
	3	Checagem (Scan) e varredura Mensal	P8

Serviço Gerenciado de Monitoramento, Triagem, Tratamento e Resposta a Incidentes de Segurança

Grupo de Serviço	ID	Serviço	ANS

Monitoramento de Ataques Cibernéticos	1	Eventos de Informação	P4
	2	Eventos de Aviso	P3
	3	Eventos de Exceção	P2
Resposta a Incidentes de Segurança	1	Resposta a Incidente Crítico - Sistema totalmente inoperante com impacto nas operações críticas de negócio	P1
	2	Resposta a Incidente Alto - Sistema parcialmente inoperante com impacto nas operações críticas de negócio	P2
	3	Resposta a Incidente Médio - Sistema parcialmente inoperante sem impacto nas operações críticas de negócio	P3
	4	Resposta a Incidente Baixo - Informacional, ajustes na configuração, dúvidas e/ou esclarecimentos	P4

Serviço de Operação e Resposta a Rquisições

Grupo de Serviço	ID	Serviço	ANS
Firewall	1	Update/Upgrade de firmware ou software	P3
	2	Backup de configuração	P2
	3	Configuração sistema (NTP, SNMP, password, users, privileges, names, DNS, Syslog, SMTP, administration setting ...)	P3
	4	Configuração conectividade e segurança (Interfaces, SD-WAN, PBR, OSPF, Route, NAT, Zones, L4 Policy, Object, ...)	P2
	5	Implementação de IPS, WebFilter, Antivírus e Antibot	P3
	6	Configuração de VPN	P2
	7	Configuração IPS, WebFilter, Antivírus e Antibot	P2
	8	Falha ou problema de sistema (NTP, SNMP, password, users, privileges, names, DNS, Syslog, SMTP,	P2

		administration setting ...)	
	9	Falha ou problema de conectividade e segurança (Interfaces, SD-WAN, PBR, OSPF, Route, NAT, Zones, L4 Policy, IPS, WebFilter, Antivírus e Antibot ....)	P2
	10	Análise de logs e geração de relatórios;	P3
	11	Análise de atividade maliciosa;	P3
	12	Ativação de firewall	P2
	13	Desativação de firewall	P2
	14	Monitoramento	P3
Antivírus	1	Health Check – Antivírus	P2
	2	Gerenciamento centralizado dos clientes	P2
	3	Instalação de clientes via console	P2
	4	Atualização da Solução	P3
	5	Configuração de políticas Firewall/AV/IPS/Integridade	P2
	6	Configuração de scans customizados	P2
	7	Configuração de políticas de controle de aplicação	P2
	8	Configuração de instalação de agentes via pacotes customizados	P2
	9	Configuração de políticas de grupo	P2
	10	Configuração de integração	P2

ANEXO III – AMBIENTE TECNOLÓGICO DO TCE-GO (HARDWARE E SOFTWARE)

Solução	Qtd.	Marca
Solução de Next Generation Firewall	1	Fortinet
Solução de IPS	1	Fortinet
Solução Wireless	2	Cisco
Solução Segurança Estações	770	Trend Micro
Solução Segurança Servidores	100	Trend Micro
Solução de E-mail	800	Google
Solução AD/DNS	2	Microsoft
Solução DNS	2	ISC - Internet Systems Consortium
Solução DHCP	2	Cisco
Servidores de Banco de Dados Oracle	2	Oracle
Servidores de Banco de Dados Microsoft SQL Server	1	Microsoft
Servidores de Banco de Dados MySQL	1	Oracle
Servidores de Banco de Dados PostgreSQL	1	PostgreSQL
Servidores de Virtualização (168 VMs)	6	VMware
Sistemas Operacionais	**	Microsoft
	**	Oracle

** CentOS

** Debian

** Rocky

ANEXO IV – REQUISITOS E ESPECIFICAÇÕES DOS SERVIÇOS

1. REQUISITOS DOS SERVIÇOS

1.1. São apresentadas, a seguir, as especificações técnicas mínimas dos serviços a serem ofertados referentes ao objeto. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

1.2. O objeto de contratação SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO consiste na prestação dos seguintes serviços: Serviço de gestão de vulnerabilidades, Serviço gerenciado de monitoramento, triagem, tratamento e resposta a incidentes de segurança e Serviço de operação e resposta a requisições.

1.3. REQUISITOS GERAIS DOS SERVIÇOS

1.3.1. Os requisitos gerais dos serviços, define os requisitos obrigatórios para todos os serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

1.3.2. CANAIS DE COMUNICAÇÃO - Para abertura de solicitações, a CONTRATADA deverá disponibilizar 03 (três) tipos de canais de comunicação, a saber:

Canais de Comunicação	Classificação
Linha de telefonia gratuita (0800).	Tipo 1
E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
Sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI).	Tipo 3

Tabela 1 - Tipos de Canais de Comunicação

1.3.3. Independentemente do canal de comunicação utilizado pela CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM, do inglês Information Technology Service Management (Gerenciamento de Serviços de TI). Ou seja, imaginando que a CONTRATANTE realize a abertura de uma nova solicitação de serviço via linha telefônica gratuita, no

segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2 (e-mail).

1.3.4. Sobre o canal de comunicação do tipo 1: via linha telefonia gratuita (0800), tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitida a utilização de URA (Unidade de Resposta Audível), e/ou qualquer uso de atendimento eletrônico.

1.3.5. Para um eventual cenário de crise, ou seja, onde o negócio fim do TCE-GO estiver sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.

1.3.6. Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL (Secure Socket Layer), com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os canais de comunicação, utilizados pela sala de videoconferência utilizem protocolos para criptografia dos dados trafegados.

1.3.7. A sala virtual deve ainda ter capacidade para 10 (dez) pessoas do TCE-GO simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

1.4. HORÁRIO DE ATENDIMENTO

1.4.1. Os SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO devem obrigatoriamente ser executados, ofertados e estar acessíveis ao TCE-GO em regime de 24 (vinte quatro) horas por dia, 07 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

1.5. GESTÃO DE CATÁLOGO DE SERVIÇO DO AMBIENTE DE SEGURANÇA DA INFORMAÇÃO

1.5.1. A fim de fornecer uma única fonte de informação sobre os SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, disponíveis para cada grupo de tecnologia dos itens de configuração do parque de segurança da informação do TCE-GO, definiu-se previamente um catálogo de serviços, o qual obrigatoriamente a CONTRATADA deverá ser capaz de entregar. Tal definição pode ser consultada através do anexo II do presente termo de referência.

1.5.2. É de responsabilidade da CONTRATADA manter, atualizar e revisar os serviços disponíveis para cada grupo de serviço. As responsabilidades do TCE-GO estão

relacionadas a aprovação de um novo serviço ou a inativação de um ou mais serviços existentes.

1.5.3. O catálogo de serviços deverá ser mantido e administrado através do sistema de ITSM de responsabilidade da CONTRATADA, estando este disponível de forma on-line para o TCE-GO, onde o mesmo poderá consultar a qualquer tempo os serviços disponíveis. Este sistema deve ser o mesmo descrito no tópico SOBRE O SISTEMA DE ITSM A SER UTILIZADO, do presente termo de referência, e obviamente deve seguir os mesmos requisitos técnicos supracitados.

1.5.4. Apesar de já existir uma definição prévia dos serviços a serem ofertados pela CONTRATADA, através do catálogo de serviço do anexo II do presente termo de referência, o TCE-GO a qualquer tempo poderá solicitar a inclusão de novos serviços, ou a retirada de um serviço em comum acordo com a CONTRATADA.

1.5.5. Também se espera que tais revisões de continuidade de um serviço no catálogo de serviços seja sugerido por parte da CONTRATADA durante a execução do contrato. Todavia, não é de responsabilidade da CONTRATADA a retirada ou inclusão de um serviço, cabendo apenas ao TCE-GO tal ação.

1.6. MODALIDADE DE ATENDIMENTO

1.6.1. A modalidade principal de atendimento será do tipo remota, ou seja, a ser realizada nas dependências da CONTRATADA, obedecendo obrigatoriamente os critérios estabelecidos para execução do mesmo, conforme previstos neste termo de referência.

1.6.2. Eventualmente o TCE-GO poderá solicitar uma visita técnica, para que um atendimento qualquer possa ser realizado e/ou acompanhado em suas dependências físicas.

1.6.3. Os atendimentos referentes ao objeto contratado, denominado SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, são ilimitados durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas e/ou quantidade de atendimentos realizados, se limitando apenas ao escopo.

1.7. ACESSIBILIDADE E CONFIDENCIALIDADE

1.7.1. Para garantir a qualidade e disponibilidade dos serviços remotos entre o TCE-GO e os Centros de Operações de Segurança da CONTRATADA, deverá haver dois tipos de conexões digitais, sendo uma do tipo internet ou do tipo MPLS (Multi-Protocol Label Switching) para cada Centro de Operações de Segurança.

1.7.2. Ambas as conexões digitais devem ter velocidade de upload e download mínima de 50 (cinquenta) Mbps, serem contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO do TCE-GO.

1.7.3. Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com links xDSL (excetuada a tecnologia HDSL). Também a fim de garantir a disponibilidade da conexão, deverá a CONTRATADA garantir que tal conexão esteja protegida contra ataques de DDoS (Distributed Denial of Service).

1.7.4. Em qualquer que seja o tipo de conexão, será de responsabilidade da CONTRATADA, a contratação junto as devidas operadoras, bem como seus devidos custos durante todo o período de vigência do contrato.

1.7.5. A fim de garantir a segurança do tráfego bidirecional entre o TCE-GO e os Centros de Operações de Segurança da CONTRATADA, ambas as conexões (Internet e MPLS) devem ser criptografadas. Ou seja, a CONTRATADA deverá estabelecer duas VPN's (Virtual Private Network), do tipo "site to site", para cada Centro de Operações de Segurança.

1.7.6. A fim de garantir a segurança entre o TCE-GO e os Centros de Operações de Segurança da CONTRATADA, não será permitido Centro de Operações de Segurança terceirizado ou consórcio de empresas. A CONTRATADA deve ter e manter os Centros de Operações de Segurança.

1.7.7. Será de responsabilidade e propriedade da CONTRATADA as soluções para estabelecer as VPN's. Caberá ao TCE-GO apenas a disponibilidade de infraestrutura física no seu Data Center, onde infraestrutura física entende-se: energia elétrica, espaço no rack, climatização adequada, e sistemas de combate a incêndio. Tais equipamentos e/ou soluções devem possuir contratos de garantia junto ao seu respectivo fabricante, com suporte em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.

1.7.8. Tais exigências visam proteger o TCE-GO contra o uso indevido de informações sob sua custódia, por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

1.8. CENTRO DE OPERAÇÕES DE SEGURANÇA

1.8.1. Os serviços gerenciados de segurança devem ser executados por meio de 02 (dois) Centros de Operações de Segurança (SOC – Security Operation Center) redundantes, próprios da CONTRATADA, sendo ambos obrigatoriamente no Brasil, de modo que a indisponibilidade de um deles não afete a prestação dos SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, e a no mínimo 300 (trezentos) km de distância geodésica um do outro e em estados distintos.

1.8.2. Ambos os centros devem atender os mesmos requisitos mínimos, a saber:

1.8.2.1. Funcionar em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

1.8.2.2. Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;

1.8.2.3. Filmar toda a área, mantendo as imagens armazenadas por, no mínimo, 90 (noventa) dias;

1.8.2.4. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao Centro de Operações de Segurança;

1.8.2.5. Possuir solução de monitoramento de disponibilidade e desempenho;

1.8.2.6. O perímetro físico dos Centros de Operações de Segurança deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;

1.8.2.7. Ser vigiado de forma ininterrupta por segurança física especializada em regime de 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;

1.8.2.8. Ter controle de acesso físico com pelo menos 02 (dois) dos seguintes fatores de autenticação, a saber: cartão de identificação magnético, biometria de leitura digital ou análise de retina;

1.8.2.9. Possuir registro de entrada e saída de pessoas, mantido por pelo menos 90 (noventa) dias;

1.8.2.10. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia;

1.8.2.11. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, durante todo o período de vigência contratual;

1.8.2.12. Ser configurado de forma que a falha de um dos equipamentos, isoladamente, NÃO interrompa a prestação dos serviços;

1.8.2.13. Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs (Uninterruptible Power Supply), para garantir a transição entre o fornecimento normal da energia e o grupo gerador;

1.8.2.14. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

1.8.2.15. Não possuir campo físico visual externo das suas instalações, a fim de garantir que as informações exibidas em monitores, estejam inacessíveis a leituras e a capturas externas desautorizadas;

1.8.2.16. Possuir ambiente dedicado único e exclusivo para laboratório, onde seja possível reproduzir os incidentes e problemas da CONTRATANTE, sem que haja impacto na operação do Centro de Operações de Segurança e/ou da própria CONTRATANTE;

1.8.2.17. Possuir no Centro de Operações de Segurança processos consistentes e objetivos de monitoramento e detecção de ameaças, gestão de dispositivos, gestão de incidentes, inteligência de ameaças, investigação de ameaças e gestão de conformidade de segurança;

1.8.2.18. Possuir nativamente solução de SecOps para gerenciamento de incidentes de segurança da informação;

1.8.2.19. Deverá possuir processos implementados que garantam a segurança das normas ABNT NBR ISO/IEC 27001. Tal certificação deverá garantir controles rígidos e auditáveis de acesso físico e lógico às informações e monitoramento.

1.8.3. Ao menos 01 (um) Centro de Operações de Segurança da CONTRATADA deverá possuir as características das certificações listadas na Tabela 2. Tais características garantem que a CONTRATADA segue os principais controles de segurança da informação, bem como também possui processos para tratamento de incidente e problemas bem estabelecidos, além de boa qualidade de atendimento e interface com o cliente.

Certificações
ABNT NBR ISO/IEC 27001
ABNT NBR ISO/IEC 20000
ABNT NBR ISO/IEC 9001

Tabela 2 - Certificações do Centro de Operações de Segurança.

1.8.4. A fim de garantir a disponibilidade das ferramentas e soluções utilizadas para a execução do objeto do presente termo de referência, ambos os CENTROS DE OPERAÇÕES DE SEGURANÇA devem utilizar infraestruturas de Data Center distintas, ou seja, dois ou mais datacenters.

1.8.5. Ao menos um dos Data Centers deve possuir as seguintes certificações ou normas, a saber:

Certificações	Descrição
ABNT NBR ISO/IEC 27001, 20000 e 9001	Norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um

	SGSI (Sistema de Gestão de Segurança da Informação) documentado dentro do contexto dos riscos de negócio globais da organização.

Tabela 3 - Certificações do Data Center 1.

1.8.6. O segundo datacenter pode estar situado fora dos ambientes dos CENTROS DE OPERAÇÕES DE SEGURANÇA, e deve possuir as seguintes certificações ou normas, a saber:

Certificações	Descrição
ABNT NBR ISO/IEC 27001	Norma que especifica os requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um SGSI (Sistema de Gestão de Segurança da Informação) documentado dentro do contexto dos riscos de negócio globais da organização.
ABNT NBR ISO/IEC 22301	Norma de gestão da continuidade de negócios especifica os requisitos para planejar, estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente um sistema de gestão documentado para se proteger, reduzir a possibilidade de ocorrência, preparar-se, responder a e recuperar-se de incidentes de interrupção quando estes ocorrerem.

Tabela 4 - Certificações do Data Center 2.

2. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS

2.1. Todas as soluções e/ou ferramentas utilizadas para prestação dos serviços deverão obrigatoriamente seguir os requisitos especificados a seguir.

2.2. Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre);

2.3. Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA;

2.4. Devem englobar a alocação de equipamentos (quando exigido) hardware e/ou softwares necessários à consecução das atividades de segurança da informação e ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção, atualização dos produtos e monitoramento de segurança em

regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano;

2.5. Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço. Da mesma maneira, os equipamentos fornecidos para a prestação dos serviços devem estar cobertos por contratos de garantia do fabricante;

2.6. O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança, em termos de integridade, confidencialidade ou disponibilidade;

2.7. PORTAL DE INDICADORES DE SERVIÇO

2.7.1. O portal de indicadores deverá ser disponibilizado ao TCE-GO contemplando, no mínimo, os requisitos abaixo.

2.7.2. A CONTRATADA deverá disponibilizar um sistema em modelo SaaS (Software as a Service), denominado portal de indicadores, para consolidação dos dados gerados pelas soluções que compõem o objeto.

2.7.3. O portal deverá estar acessível ao TCE-GO via internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, e 365 (trezentos e sessenta e cinco) dias por ano, de maneira segura utilizando protocolo de criptografia SSL.

2.7.4. O TCE-GO terá direito a criação de usuários ilimitados com a função de criação de perfis para cada usuário, disponibilizando assim visões diferentes para cada nível de acesso.

2.7.5. Deverá disponibilizar para os usuários do TCE-GO, a função de mudança de visão gráfica a critério de cada usuário. Isso quer dizer que apesar de um gráfico estar disposto em modelo de barras, caso o usuário identifique uma melhor visualização do modelo gráfico em forma de pizza, o sistema deve oferecer tal funcionalidade ou opção.

2.7.6. O portal ainda deverá disponibilizar pelo menos os seguintes modelos gráficos para os usuários: gráfico do tipo pizza, gráfico do tipo barra, gráfico do tipo linha, gráfico do tipo área, gráfico do tipo funil e gráfico do tipo bolha.

2.7.7. INDICADORES DE RISCO – KRI

2.7.7.1. Deverá ser exibido no portal a quantidade de Vulnerabilidades que estavam presentes na última auditoria realizada através de gráfico(s) com separação dos tipos/quantidades com a opção de “Drill Down”, possibilitando assim visualização de forma mais detalhada das vulnerabilidades listadas;

2.7.7.2. O portal deverá possuir recurso para filtrar apenas as vulnerabilidades relevantes, excluindo as de severidade média e/ou baixa.

2.7.8. INDICADORES DE META E PERFORMANCE – KGI e KPI

2.7.8.1. O portal de indicadores deverá possuir relatório gráfico indicando tempo médio dos atendimentos dos incidentes por fase de análise, contenção, erradicação e recuperação, possibilitando a filtragem dos mesmos por período:

- Últimos 15 dias;
- Últimos 30 dias;
- Últimos 45 dias.

2.7.8.2. Deverá possuir gráfico comparativo entre os primeiros e últimos 15 incidentes analisados dentro do período filtrado, mostrando uma linha de tempo qual foi o incidente com o tempo de atendimento menor, maior e o tempo médio.

2.7.8.3. Deverá ser possível a consulta deste gráfico para cada uma das fases de atendimento (análise, contenção, erradicação e recuperação).

2.7.9. INDICADORES POR CATEGORIA MITRE ATT&CK

2.7.9.1. O Portal de indicadores deverá possuir gráfico que separe e classifique os incidentes de acordo com as categorias existentes na base de conhecimento do MITRE ATT&CK, sendo elas no mínimo: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement, Collection, Command and Control, Exfiltration e Impact;

2.7.10. Todos os indicadores exibidos pelo portal devem possuir a funcionalidade drill down, para que os usuários possam criar visualizações e filtros dos dados exibidos.

2.7.11. Todos os indicadores exibidos pelo portal devem ainda possuir funcionalidade de exibição dos dados gerados no gráfico de maneira tabular, a fim de que seja possível aferir os dados brutos.

2.7.12. O portal deve armazenar os dados durante o período mínimo de 1 (um) ano e deverá permitir a criação de filtros por períodos.

2.7.13. A qualquer tempo o TCE-GO poderá solicitar os dados brutos coletados das soluções que compõem o objeto contratado.

2.7.14. Os dados exibidos pelo portal devem representar o ambiente em tempo de execução e de forma automática (real time).

2.7.15. O portal deverá possibilitar customizar limiares dos serviços e eventos para gerar alarmes de acordo com o acordo de nível de serviço definido no presente termo de referência.

2.7.16. Deverá prover mecanismo para análise de risco e métricas de disponibilidade através de relatórios e dashboards de todas as soluções que compõem o objeto.

3. ESPECIFICAÇÃO DOS SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO

3.1. SERVIÇO GERENCIADO DE MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA

3.1.1. Visa o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao TCE-GO, através do fornecimento de serviços com capacidade de correlacionamento de eventos, para detecção de ameaças direcionadas ao TCE-GO para detecção de comportamento anômalo de serviços, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

3.1.2. GAP ANALYSIS

3.1.2.1. O objetivo é a realização de uma avaliação, no início do contrato, nos ambientes físico e digital para reduzir o risco iminente de comprometimento. Ela consiste em uma análise dos principais riscos atuais, do processo de detecção e de resposta a incidentes de segurança no ambiente do TCE-GO, e serão propostas melhorias rápidas que aperfeiçoarão de modo eficiente esses ambientes.

3.1.2.2. A avaliação de MITRE ATT&CK utiliza uma base de conhecimento acessível globalmente de táticas e técnicas adversárias com base em observações do mundo real. A base de conhecimento da ATT&CK é usada como base para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de segurança cibernética. Nesse processo de avaliação deverão ser checadas as 14 táticas e todas as técnicas e sub técnicas relacionadas e aplicáveis.

3.1.2.3. Os entregáveis desta análise são:

- Relatório de GAPs;
- Infográfico de Maturidade;
- Artefatos de Avaliação;
- Avaliação das Técnicas e Sub Técnicas;
- Matriz de Priorização.

3.1.3. PLANO DE RESPOSTA A INCIDENTES

3.1.3.1. O objetivo desse plano é arquitetar a concepção de atividades de resposta a incidente baseado nas características organizacionais e políticas do TCE-GO aliado ao serviço de monitoramento e resposta a incidente exposto neste termo de referência.

3.1.3.2. Instrução para estruturação de comitês e grupos de trabalho com orientações quanto a atuação e atribuições vinculadas, apoiando no processo de estabelecer prioridades, avaliação dos impactos e lições aprendidas;

3.1.3.3. Desenvolver fluxo de comunicação, conforme prioridade e tipo de incidente;

3.1.3.4. Arquitetar as etapas abaixo do tratamento de incidentes, indicando o fluxo de trabalho, elementos chave e nível de maturidade com riqueza de detalhes da atuação de cada participante e área do TCE-GO e da CONTRATADA.

- Identificação;
- Análise;
- Contenção;
- Erradicação;
- Recuperação e
- Pós-Incidente.

3.1.3.5. Criação de Matriz RACI, estabelecendo os papéis dos envolvidos no tratamento e resposta a incidentes;

3.1.3.6. Desenvolver fluxo de interligação dos serviços entregues no caderno técnico, observando desde o monitoramento até a gestão dos serviços de segurança fornecidos ou geridos pelo item “Serviço de operação e resposta a requisições”.

3.1.4. SOBRE AS FERRAMENTAS UTILIZADAS

3.1.4.1. Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento que atendam o descritivo técnico a seguir.

3.1.4.2. A plataforma utilizada deverá ter capacidade de operar com volumes massivos de dados em tempo real utilizando algoritmos de aprendizagem de máquina (Machine Learning) e deve contar com casos de uso para detectar ameaças avançadas;

3.1.4.3. A plataforma deverá ser extremamente escalável e tolerante a falhas, capaz de ingerir centenas de terabytes por dia e suportar a retenção de eventos de segurança por longo período;

3.1.4.4. Junte-se a eventos ao longo do tempo usando modelos Kill Chain para a análise de eventos de maior risco;

3.1.4.5. Deve permitir o hunting rápido de ameaças por meio da pesquisa em linguagem natural.

3.1.4.6. A solução deve ter recursos de "Multi-tenant";

3.1.4.7. Deve ser do tipo Nuvem em Software como um modo de Serviço e ter as certificações SOC 2 TYPE II e ISO 27001;

3.1.4.8. Deve garantir retenção dos logs conforme arquitetura abaixo:

- 7 dias hots retention;
- 90 dias warm retention;
- 365 dias cold retention.

3.1.4.9. Deve ter alta disponibilidade e mecanismos de recuperação de desastres;

3.1.4.10. Deve permitir a filtragem e compressão de dados seletivos em até 90% no ponto de coleta;

3.1.4.11. Deve permitir o gerenciamento da largura de banda para a transmissão de dados entre os coletores e os servidores de gerenciamento;

3.1.4.12. Deve executar o armazenamento em cache local e/ou em buffer nos coletores para garantir que nenhum dado seja perdido em trânsito no caso de um problema de rede ou um pico no volume do evento;

3.1.4.13. Deve oferecer suporte ao mascaramento de dados por meio de controles de acesso granulares baseados em funções, para ofuscar qualquer informação de usuário potencialmente sensível na camada de interface do usuário;

3.1.4.14. Deve suportar controle de acesso baseado em função granular (RBAC) com suporte a administração delegada, tanto para as funcionalidades na interface do usuário quanto acesso aos dados e configurações;

3.1.4.15. Deve incluir uma ferramenta de Security Datalake baseada em Big Data, uma arquitetura aberta e escalável e com capacidade de coletar e reter dados por períodos estabelecidos para fins de conformidade e investigação;

3.1.4.16. Deve ter uma instância de homologação para testes que permita isolar, do ambiente de produção, novas integrações, novos desenvolvimentos de conteúdos e novos analisadores;

3.1.4.17. A solução deve atender as seguintes características:

3.1.4.18. Deve oferecer suporte à integração com mais de 500 fontes de eventos usando métodos de syslog, formatos de log estruturados (CEF, LEEF, MEF, JSON, XML), arquivos, bancos de dados (conexão JDBC), conexão API (AWS, Azure, Box, Crowdstrike, Google Report, Netskope, SVN, Salesforce, Splunk, QRadar, Netwitness, Office 365, Okta, Proofpoint, Sumologic, Workday, entre outros), WMI, consultas LDAP/LDAPS, dados e fluxo (Netflow, sFlow, jFlow), Hadoop, Registros não estruturados (Regex), agentes de terceiros (snare);

3.1.4.19. Deve permitir a integração com diferentes tipos de fontes de dados, como dados de identidade, logs de atividades / transações, logs de eventos de segurança, fluxos de rede, log de aplicativos / plataformas de nuvem, permissões de acesso, fontes de inteligência de ameaças, dados não estruturados e metadados de ativos;

3.1.4.20. Deve permitir conexão a sistemas externos de gerenciamento de identidade, como Active Directory / LDAP ou soluções de IAM (gestão de identidade), como Aveksa/Sailpoint, sistemas de RH, como Peoplesoft/Workday, para realizar o enriquecimento contextual de eventos adicionando identidade do usuário;

3.1.4.21. Deve ser capaz de se conectar nativamente através de APIs ou outros meios com serviços em nuvem como Salesforce, Amazon Web Services S3 e Cloudtrail, BOX, Microsoft Azure, Office 365, Google Apps, Google Cloud, Netskop, ServiceNow, entre outros.

3.1.4.22. Deve ter uma interface de usuário que permita modificar conectores, analisadores (parsers) existentes ou construir novos analisadores (parsers) na mesma interface de usuário;

3.1.4.23. Deve ter conectores, analisadores (parsers) pré-configurados, prontos para uso, mas que possam ser modificados conforme necessário. A análise, normalização e categorização dos coletores devem ser totalmente personalizáveis na interface do usuário.

3.1.4.24. Deve ter uma API RESTful de serviços para integração bidirecional com outras tecnologias;

3.1.4.25. Deve fornecer integração com pelo menos 5 fontes de inteligência de ameaças inclusas no valor do serviço ofertado;

3.1.4.26. Deve realizar o enriquecimento dos eventos com dados contextuais no momento da captura e ingestão de dados, adicionando aos eventos:

- Identidade do usuário;
- Contexto de negócios;
- Metadados de ativos;
- Informações de rede;
- Localização Geográfica;
- Dados de inteligência de ameaças.

3.1.4.27. Deve enriquecer eventos em tempo real com contexto de usuário e entidade. Os dados ricos podem fornecer atributos de contexto que podem ser usados para perfis comportamentais, comparações de pares, pesquisas e investigações;

3.1.4.28. Deve detectar ameaças cibernéticas e internas avançadas (insider threat) usando aprendizado de máquina para criar perfis e linhas de base de comportamento de usuários e entidades;

3.1.4.29. Deve ter conteúdo pré-empacotado de casos de uso e modelos de ameaças prontos para uso na detecção avançada de ameaças, como:

- Detecção de ameaças internas (insider threat) utilizando técnicas de aprendizagem de máquina;

- Detecção de ameaças cibernéticas (cyber threat) utilizando técnicas de aprendizagem de máquina;
- Detecção de ameaças na nuvem (cloud threat) utilizando técnicas de aprendizagem de máquina.

3.1.4.30. Deve fornecer recursos abrangentes para modelar e ajustar a pontuação de risco com base no perfil do usuário e/ou entidade, gravidade da ameaça e sequência/combinação de eventos que ocorrem durante um período;

3.1.4.31. Deve permitir a modelagem de risco a partir da interface do usuário de acordo com as prioridades da organização;

3.1.4.32. Deve ter modelos de ameaças que permitam agrupar eventos realizados por um usuário ou entidade que duram dias, semanas, meses e assim por diante. Essas atividades devem ser exibidas como uma cadeia de eliminação com cada evento categorizado em estágios predefinidos.

3.1.4.33. Deve ter algoritmos preditivos para identificar usuários de risco (por exemplo, usuários prestes a deixar a organização);

3.1.4.34. Deve fornecer análises para diferentes tipos de anomalias, como relacionadas ao tempo, volume de transferência de dados, origem do evento relacionado, destino do evento relacionado, anomalias por usuário e grupo de pares, anomalias relacionadas a localização geográfica / velocidade terrestre, bem como rastrear usuários ou outras entidades nas listas de observação;

3.1.4.35. Deve ter algoritmos de aprendizagem não supervisionados para analisar eventos atuais e históricos e determinar associações, para estabelecer padrões de comportamento da atividade do usuário em cada fonte de evento por dia, semana, mês, hora do dia e dia da semana. Qualquer desvio do padrão regular deve ser marcado como uma anomalia;

3.1.4.36. Deve ter algoritmos de aprendizagem supervisionados para detectar ameaças de malware avançadas, como DGA, ataques de phishing/spam e muito mais;

3.1.4.37. Deve ter técnicas de análise baseadas em pares para detectar usuários que estão começando a se comportar de maneira diferente dos pares, traçando o perfil do comportamento de diferentes usuários no grupo de pares e, em seguida, comparando as transações do usuário com a dos pares;

3.1.4.38. Deve haver técnicas de análise de raridade de eventos pelas quais atividades suspeitas que não foram vistas antes possam ser identificadas;

3.1.4.39. Deve ter técnicas de análise de comportamento por enumeração que permita criar linhas de base de eventos do mesmo tipo e procurar qualquer desvio do normal;

3.1.4.40. Deve ter técnicas de análise de tráfego para identificar padrões de beaconing, agentes de usuários incomuns, conexões com URLs incomuns, conexões com domínios DGA, etc;

3.1.4.41. Deve fornecer a capacidade de definir políticas baseadas em regras para detectar ameaças conhecidas. Essas ameaças conhecidas devem ser usadas como intensificadores de risco e combinadas com as verificações “não assinadas” nos modelos de ameaças;

3.1.4.42. Deve haver modelagem de ameaças que permita a identificação de ameaças compostas, que se observadas isoladamente podem ser de baixo risco, porém, quando combinadas, são indicativas de um evento de alto risco;

3.1.4.43. Deve reduzir o número de falsos positivos aplicando recursos avançados de aprendizado de máquina para aprender o que é normal e o que não é normal no ambiente monitorado;

3.1.4.44. Deve ter relatórios de ameaças que forneçam visibilidade da postura de segurança cibernética. Por exemplo: usuários de alto risco, ativos de alto risco, principais ameaças, principais IPs maliciosas, etc;

3.1.4.45. Deve ter relatórios que forneçam visibilidade sobre as operações de segurança. Por exemplo, para dispositivos VPN, os relatórios devem incluir as melhores sessões de VPN por duração, os principais eventos de saída de dados, a distribuição dos eventos de login por geografia, as principais tentativas de login com falha e assim por diante;

3.1.4.46. Deve ter relatórios de conformidade alinhados com requisitos de conformidade específicos, como PCI, SOX, HIPPA, GDPR, ISO27002, etc;

3.1.4.47. Deve ter relatórios de resumo executivo de violações, incidentes e operações;

3.1.4.48. Deve ter relatórios sobre a atividade do usuário;

3.1.4.49. Deve permitir que os dados sejam exibidos com diferentes tipos de gráficos: gráfico de linhas, gráfico de barras, gráfico de pizza, mapa geográfico, tabelas, gráfico empilhados, gráfico N principais, gráficos de bolhas, gráficos de relacionamento de origem e destino;

3.1.4.50. Deve permitir a visualização de dados através de links que permitam vincular qualquer conjunto de atributos e visualização a relação entre eles;

3.1.4.51. O serviço deve possuir solução para análise de artefatos maliciosos que minimamente contemple as funcionalidades a seguir:

3.1.4.52. Analisar mais de 1000 indicadores comportamentais de um artefato;

3.1.4.53. Realizar análise estatística e dinâmica para avaliar se o artefato é malicioso ou não;

3.1.4.54. Deve suportar a análise dos artefatos BAT, CHM, DLL, ISO, HTA, HWP, JAR, JS, JSE, JTD, LNK, MSI, MHTML, documentos do Microsoft Office, EXE, PE32, PDF, VBE, URLs, WSF, XML e ZIP.

3.1.5. PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA

3.1.5.1. A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada;

3.1.5.2. A fim de balizar todo o processo de monitoramento de ataques cibernéticos da CONTRATANTE, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir.

3.1.5.3. É sabido que para o sucesso de um monitoramento de ataques cibernético, a primeira definição se deve a que tipo de ocorrência de eventos de segurança deseja-se detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.

3.1.5.4. Tal definição de linha de base de eventos de segurança monitorados, não deve ser tomada de forma unilateral pela CONTRATADA. O TCE-GO deverá participar ativamente no processo de construção de forma consultiva. Porém, é de responsabilidade da CONTRATADA a definição e a colocação em operação tal linha de base.

3.1.5.5. Espera-se que a linha de base de eventos de segurança monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e espera-se que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a linha de base, para que em um cenário onde estes novos ataques sejam direcionados ao TCE-GO, sejam detectados através dos serviços em questão.

3.1.5.6. O produto de um evento é a correlação dos logs gerados pelos itens de configurações do parque tecnológico do TCE-GO. Uma vez definida a linha de base de eventos, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento estão sendo enviados corretamente para a ferramenta.

3.1.5.7. Caso a CONTRATADA identifique a ausência dos insumos (eventos) que deveriam ser gerados por um item de configuração, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração descritos no tópico AMBIENTE TECNOLÓGICO DO TCE-GO (HARDWARE E SOFTWARE). Caso o item de configuração não pertencer ao

objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar ao TCE-GO a correção e/ou habilitação de tal insumo no item de configuração em questão.

3.1.5.8. Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

3.1.5.9. Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se as ferramentas e soluções estão funcionando dentro do esperado. Estes eventos são também úteis para gerar estatísticas como, por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.

3.1.5.10. Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento anômalo, se comparado a linha de base de operação padrão do ambiente (serviço ou solução), porém, ainda não gerou algum tipo de impacto ao ambiente (serviço ou solução) do TCE-GO. Exemplo: É esperado que existam 1.000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém, na última hora, este número passou para 10.000 (dez mil) ataques, todavia, o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, trafego e/ou solução).

3.1.5.11. Eventos de Exceção: Estes eventos são aqueles que sugerem que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Uma infecção gerada por um malware do tipo ransomware, onde a mesma não tenha sido bloqueada pela solução de antivírus do TCE-GO. Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico, do presente termo de referência.

3.1.5.12. Uma vez classificado o evento, inicia-se o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

3.1.5.13. Para eventos do tipo Informação, não é requerido qualquer tipo de ação, porém, como já mencionado no presente termo de referência, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança. Portanto, a CONTRATADA deverá utilizá-los para tal fim.

3.1.5.14. Para eventos do tipo Aviso, a CONTRATADA deverá garantir que uma interface humana, ou seja, um analista que pertence ao grupo de monitoramento de ataques, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomar as ações cabíveis para identificar a causa raiz da mudança de comportamento do ambiente.

3.1.5.15. Para eventos do tipo Exceção, a CONTRATADA deverá transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação definida no PROCESSO DE MONITORAMENTO, DETECÇÃO E RESPOSTA, descrito no presente termo de referência. Após a abertura do incidente de segurança, obedecendo os critérios estabelecidos para tal, encerra-se a participação do grupo de monitoramento de ataques.

3.1.5.16. Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas os tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento, o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

3.1.5.17. Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

3.1.6. PROCESSO DE CAÇADA CONTINUA A AMEAÇAS

3.1.6.1. Com o aumento do volume e complexidade das ameaças será exigido que a CONTRATADA execute processos manuais de caçada de ameaças (threat hunting) no ambiente do TCE-GO. A fim de balizar todo o processo de caça a ameaças, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir.

3.1.6.2. A CONTRATADA deverá, inclusive nos finais de semana e feriados, definir uma hipótese e uma declaração de uma possibilidade de ameaça, onde tal hipótese deve ser elaborada utilizando como referência novos vetores de ameaças e novas tendências baseadas em inteligência de ameaças e fontes de riscos digitais, informações relevantes coletadas por processos de aprendizagem de máquina e inteligência artificial e investigações de táticas, técnicas e

procedimentos criando desta forma uma hipótese de como ameaças podem existir dentro do ambiente e de como encontrá-las;

3.1.6.3. Uma vez que a hipótese tenha sido definida, a CONTRATADA deverá realizar um plano de coleta dos eventos dentro das plataformas relevantes de acordo com a hipótese definida;

3.1.6.4. Uma vez que os eventos relevantes estejam disponíveis, a CONTRATADA deverá avaliar a massa de eventos para buscar anomalias associadas a hipótese definida;

3.1.6.5. Caso sejam encontrados eventos maliciosos, estes entram no processo de resposta a incidentes de segurança da informação, conforme descrito neste documento;

3.1.6.6. Caso não sejam encontrados eventos maliciosos, o processo de caçada é finalizado, sendo repetido no dia seguinte com uma nova hipótese;

3.1.6.7. Todo processo deve ser documentado através da plataforma de ITMS, incluindo qual hipótese foi utilizada, quais dados foram analisados e o resultado da análise;

3.1.7. GRUPO TÉCNICO DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

3.1.7.1. Através dos seus Centros de Operações de Segurança, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.

3.1.7.2. Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem com os demais serviços descritos no objeto do presente termo de referência.

3.1.7.3. Todos os profissionais que integram GRUPO DE MONITORAMENTO DE ATAQUES, devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), sendo proibida a terceirização ou subcontratação de tal serviço.

3.1.7.4. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.

3.1.7.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos do TCE-GO, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE

MONITORAMENTO DE ATAQUES com ao menos 01 (um) perfil de cada profissional que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança I	ISFS (Information Security Foundation)	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista de Segurança II	Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD.

Tabela 5 - Certificações e qualificações do Grupo de Monitoramento de Ataques.

3.1.7.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

3.1.7.7. No momento da assinatura do contrato, será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE MONITORAMENTO DE ATAQUES, os quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme Tabela 5.

3.1.8. ENTREGAS

3.1.8.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o TCE-GO definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

Denominação	Forma de Cálculo	Filtro	Agrupador	Descrição
Quantitativo de eventos	Soma de eventos correlacionados	Eventos correlacionados	Eventos correlacionados	Número total de eventos

correlacionados				correlacionados
Quantitativo de incidentes abertos	Soma de incidentes abertos	Incidentes abertos	Incidentes	Número total de incidentes abertos
Quantitativo de solicitações por grupo de tecnologia	Soma de solicitações relacionadas aos grupos de tecnologia	Solicitações relacionadas aos grupos de tecnologia	Solicitações	Número total de solicitações relacionadas por grupo de tecnologia
Quantitativo de regras de correlacionamento	Soma do número de regras de correlacionamento	Regras de correlacionamento	Regras de correlacionamento	Número total de regras de correlacionamento
TOP 10 – Regras de correlacionamento	Soma do número de eventos correlacionados por regra de correlacionamento	Eventos correlacionados	Regra de correlacionamento	TOP 10 do número de eventos correlacionados por regra de correlacionamento
TOP 10 – IP de destino de regras de correlacionamento	Soma do número de eventos correlacionados por IP de destino	Eventos correlacionados por IP de destino	IP de destino	TOP do número de eventos correlacionados por IP de destino
TOP 10 – Regras de correlacionamento por país de origem	Soma do número de eventos correlacionados por país de origem	Eventos correlacionados por país de origem	País de origem	TOP do número de eventos correlacionados por país de origem
TOP 10 – Tipos de ataques	Soma do número de ataques correlacionados por tipo de ataque	Eventos correlacionados por ataque	Ataques	TOP 10 por tipo de ataque

Tabela 6 - Indicadores Estratégicos de Monitoramento de Ataques Cibernéticos.

3.1.8.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com a presença de profissional que conheça todos os serviços prestados, e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler).

3.1.8.3. Neste contexto, o profissional deve apresentá-los de forma presencial nas dependências do TCE-GO ou de forma virtual por meio de solução de videoconferência.

3.2. SERVIÇO DE GESTÃO VULNERABILIDADES

3.2.1. Tem por objetivo de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações do TCE-GO, identificando proativamente as vulnerabilidades de aplicações que seriam vetores de ataques, e tornando-as elegíveis de blindagem contra a exploração das vulnerabilidades

identificadas afim de evitar que ataques cibernéticos direcionados ao TCE-GO obtenham sucesso explorando tais vulnerabilidades já conhecidas.

3.2.2. A CONTRATADA nomeará os ativos a serem monitorados para gerir todo ciclo de vida das vulnerabilidades encontradas, nos servidores e ativos críticos do TCE-GO.

3.2.3. Para garantir a padronização dos resultados e correlacionamento de dados e vulnerabilidades pelo time do Centro de Operações de Segurança, todo o serviço deverá ser prestado através da utilização de ferramentas/soluções do mesmo fabricante, sem qualquer tipo de customização não autorizada pelo mesmo;

3.2.4. A solução deve ser licenciada de modo a realizar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

3.2.5. A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede;

3.2.6. O licenciamento da plataforma deverá ser por ativo, sendo este um dos abaixo:

- Ativos em rede;
- Servidores e Estações de trabalho ou Notebooks;
- Servidores em Cloud;
- Containers;
- Aplicações Web e API.

3.2.7. O licenciamento deverá ser flexível, ou seja, não limitado por módulo. Cada licença adquirida deverá possibilitar a utilização para qualquer um dos ativos do item anterior;

3.2.8. Deverá ser possível alterar o uso da licença entre os ativos acima. Caso haja algum prazo mínimo para esta mudança de uso de licenciamento, este deverá ser de no máximo 90 dias;

3.2.9. O gerenciamento da plataforma deverá ser centralizado e único para todos os módulos descritos neste documento;

3.2.10. O gerenciamento da solução deverá ser em nuvem;

3.2.11. A solução em nuvem deverá atender, no mínimo, os seguintes requerimentos de segurança:

3.2.12. A solução deve prover no mínimo 99.95% de disponibilidade no nível de serviço;

3.2.13. A solução deve criptografar todas as informações em trânsito;

3.2.14. Deve utilizar no mínimo chave AES-256 para criptografar os dados armazenados;

3.2.15. A solução deve ser capaz de gerar uma chave randômica com no mínimo 256 bits para cada scanner conectado na plataforma de gerência;

3.2.16. Todos os dados enviados para a plataforma de gerenciamento devem ser criptografados no mínimo com protocolo TLS 1.2 com tamanho de chave de 4096 bits;

3.2.17. Dados indexados devem possuir no mínimo criptografia utilizando algoritmo AES-256;

3.2.18. A plataforma deve ser capaz de gerar uma chave randômica de no mínimo 128 bits para qualquer “Job” gerado;

3.2.19. A plataforma deve utilizar no mínimo chave AES-256 para Backups e dados Replicados;

3.2.20. Todas as credenciais armazenadas na plataforma deverão ser criptografadas com algoritmo AES-256, no mínimo;

3.2.21. A solução deve possuir no mínimo as seguintes certificações de privacidade e segurança:

- EU-U.S. Privacy Shield Framework;
- Swiss-U.S. Privacy Shield Framework;
- Cloud Security Alliance (CSA) STAR.

3.2.22. A solução deve possuir ferramentas e processos automatizados para monitorar: uptime, comportamentos anômalos e performance da plataforma;

3.2.23. Deve possuir retenção na nuvem de no mínimo 12 meses dos resultados dos scans realizados no ambiente;

3.2.24. Os dados de clientes deverão ser totalmente separados um dos outros, não possuindo compartilhamento de dados;

3.2.25. O fabricante da solução deverá implementar controles de segurança, como Análise de Vulnerabilidade no mínimo semanal, Firewalls, segmentação de rede, e monitoramento de segurança 24/7/365, para garantir a segurança da aplicação;

3.2.26. O desenvolvimento da solução deverá seguir metodologias de Desenvolvimento Seguro;

3.2.27. A fabricante da solução deverá possuir ISO 27001.

3.2.28. CONTROLE DE USUÁRIOS

3.2.28.1. A solução deve suportar RBAC (Role Based Access Control) com no mínimo 5 tipos de usuários pré-definidos;

3.2.28.2. Deve possuir no mínimo um perfil administrador e um perfil somente leitura;

3.2.28.3. Deve permitir autenticação com Single Sign On suportando os padrões SAML 2.0 ou Shibboleth 1.3;

3.2.28.4. A solução deve possibilitar a criação de Grupos de Usuários;

3.2.28.5. Deve permitir configurar quais usuários, ou grupos de usuários, tem permissão de visualizar determinados ativos da organização e suas vulnerabilidades, e quais tem permissão de executar análises de vulnerabilidades nesses ativos;

3.2.28.6. Possuir duplo fato de autenticação nativo na própria solução;

3.2.28.7. Deve possibilitar configurar permissões, por usuário e grupo de usuário, específicas para cada política de análise de vulnerabilidades. No mínimo deverá ser possível configurar permissões de “Nenhum Acesso”, “Somente Ver Resultados”, “Configuração” ou “Execução das políticas”;

3.2.29. RELATÓRIOS E DASHBOARDS

3.2.29.1. Deve ser capaz de exportar dashboards em modelo de relatórios, de forma periódica de acordo com a frequência estabelecida pelo administrador;

3.2.29.2. Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

3.2.29.3. A solução deve suportar o envio automático de relatórios para destinatários específicos;

3.2.29.4. Deve ser possível definir a frequência na geração dos relatórios para no mínimo: Diário, Mensal, Semanal e Anual;

3.2.29.5. A solução deve possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;

3.2.29.6. Deve possuir ao menos 10 modelos de dashboards já criados, podendo ser customizados;

3.2.29.7. A solução deve permitir exportar dados do que está sendo apresentado na tela, no mínimo para:

- Ativos gerenciados pela solução;
- Todas as vulnerabilidades existentes nos ambientes e em quais ativos ela existe;
- Vulnerabilidades por ativo gerenciado pela solução;
- Vulnerabilidades de um único ativo;
- Uma única vulnerabilidade e todos os ativos que possuem.

3.2.29.8. Deve ser possível exportar os dados em HTML, PDF ou CSV;

3.2.29.9. Em caso de exportação por CSV deve ser possível selecionar, via console de gerenciamento, quais campos deseja exportar;

3.2.29.10. Deve ser possível exportar somente os gráficos dos dashboards, através da console de gerenciamento, em PDF, PNG e JPG;

3.2.29.11. Deve ser possível criar um Dashboard e definir este como padrão de visualização do usuário, ou seja, o primeiro Dashboard a aparecer na console;

3.2.29.12. Deve ser possível configurar um filtro permanente no Dashboard para apresentar informações de todos os ativos, ou somente ativos específicos do ambiente;

3.2.29.13. A solução deve permitir compartilhar Dashboards com um ou mais usuários, bem como com grupo de usuários da aplicação;

3.2.29.14. Deve ser possível configurar SLAs em dias, representando a idade das vulnerabilidades no ambiente, sendo o período em que a mesma foi encontrada até a resolução. Está informação deverá ser apresentada no Dashboard da solução.

3.2.30. ANÁLISE DE CONFORMIDADE

3.2.30.1. A solução deve ser totalmente licenciada para realizar scans de auditoria e compliance;

3.2.30.2. A solução deve ser capaz de realizar auditoria de conformidade sem a necessidade de agente instalado no dispositivo de destino;

3.2.30.3. A solução deve ser licenciada para realizar scans de conformidade e compliance de forma ilimitada;

3.2.30.4. Toda a solução deve ser licenciada de modo a realizar scans de conformidade para os seguintes padrões: CIS, SCAP e OVAL;

3.2.30.5. A solução deverá possuir modelos prontos de padrões de configuração, no mínimo para: CIS, DISA e MSCT (Microsoft Security Compliance Toolkit)

3.2.30.6. Deve suportar a verificação de compliance para no mínimo:

- Bluecoat ProxySG;
- Brocade Fabric OS;
- Checkpoint;
- Cisco IOS;
- Citrix Xenserver;
- Fireeye;
- Fortinet FortiOS;
- IBM iSeries;
- Netapp Data ONTAP;
- Palo Alto Firewall;
- Red Hat Enterprise Virtualization;
- Unix;
- Windows;
- VMware.

3.2.30.7. A solução deve mostrar se o critério de compliance foi atendido ou não fornecendo no mínimo os seguintes status:

- Passou;
- Falhou;
- Atenção.

3.2.31. ANÁLISE DE RISCO DO AMBIENTE

3.2.31.1. A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

3.2.31.2. O score deve ser gerado automaticamente por meio de algoritmos de inteligência artificial (Machine Learning) e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade;

3.2.31.3. Deve ser capaz de calcular a criticidade dos ativos da organização;

3.2.31.4. A solução deve ser capaz de realizar um benchmark no ambiente do TCE-GO comparando sua maturidade com outras organizações do mesmo setor;

3.2.31.5. A solução deve permitir modificar a qualquer momento o tipo de indústria para comparação. Ex: Mudar de Setor Público para Mercado Financeiro;

3.2.31.6. Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

3.2.31.7. A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo);

3.2.31.8. A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;

3.2.31.9. A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

3.2.31.10. Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;

3.2.31.11. A solução deverá apresentar indicadores específicos referentes a remediação, possuindo no mínimo informações referentes ao tempo entre remediação e o tempo o qual a vulnerabilidade foi descoberta no ambiente, tempo entre a remediação e a data de publicação da vulnerabilidade, quantidade média de vulnerabilidades críticas por ativo e a comparação da quantidade de vulnerabilidades corrigidas por criticidade;

3.2.31.12. A solução deve possuir um gráfico indicativo do percentual de ativos com soluções de proteção de endpoint instaladas, bem como o nome e a versão da solução;

3.2.31.13. A solução deve permitir a segregação lógica entre áreas distintas da organização afim de obter a pontuação referente a exposição cibernética por área;

3.2.31.14. A solução deve permitir a segregação lógica entre aplicações distintas da organização afim de obter a pontuação referente a exposição cibernética por aplicação.

3.2.32. PLATAFORMA DE GESTÃO DE VULNERABILIDADES EM ATIVOS DE REDE

3.2.32.1. Deve possibilitar, por meio da console, no mínimo 3 (três) métodos de escaneamento:

- Scan ativo;
- Scan com uso de agentes;
- Scan passivo.

3.2.32.2. Deve ser capaz de identificar no mínimo 50.000 CVE´S;

3.2.32.3. A solução deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades diferente do padrão CVSS;

3.2.32.4. Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial (machine learning);

3.2.32.5. O Algoritmo de priorização deve considerar no mínimo 100.000 vulnerabilidades distintas para realizar o cálculo do score da vulnerabilidade;

3.2.32.6. Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades;

3.2.32.7. A solução deve ser capaz de aplicar algoritmos de inteligência artificial (machine learning) para analisar mais de 130 fontes de dados relacionadas a vulnerabilidades;

3.2.32.8. O sistema de pontuação e priorização de vulnerabilidades deve avaliar no mínimo as seguintes características:

3.2.32.9. CVSSv3 Impact Score;

3.2.32.10. Idade da Vulnerabilidade;

3.2.32.11. Se existe ameaça ou Exploit que explore a vulnerabilidade;

3.2.32.12. Número de produtos afetados pela vulnerabilidade;

3.2.32.13. Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;

3.2.32.14. Lista de todas as fontes (canais de mídia social, Dark Web etc.) em que ocorreram eventos de ameaças relacionados a vulnerabilidade;

3.2.32.15. A solução de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação);

3.2.32.16. Deve possuir uma API abrangente para automação de processos e integração com aplicações terceiras;

3.2.32.17. Deve ser capaz de fazer a correlação diária de ameaças ativas contra as vulnerabilidades existentes na infraestrutura, incluindo feeds de inteligência de ameaças, tanto de fontes públicas como também de fontes não gratuitas;

3.2.32.18. A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

3.2.32.19. A solução deve possuir conectores para a seguintes plataformas:

- Amazon Web Service (AWS);
- Microsoft Azure;
- Google Cloud Platform.

3.2.32.20. A solução deve ser capaz de analisar vulnerabilidades em servidores na AWS utilizando somente o conector, sem a necessidade de instalação de agente ou uso de qualquer outro tipo de sensor de rede da solução.

3.2.32.21. A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;

3.2.32.22. A solução deve ser PCI ASV (Approved Scanning Vendor);

3.2.32.23. A solução deve ser capaz de identificar novos hosts no ambiente sem a necessidade de um scan;

3.2.32.24. A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

3.2.32.25. A solução deve ser licenciada para no mínimo 50 scanners ativos;

3.2.32.26. A solução deve ser licenciada para o uso de no mínimo 20 sensores passivos de rede para realizar o monitoramento em tempo real do ambiente;

3.2.32.27. Deve ser possível determinar quais portas estão abertas em determinado ativo;

3.2.32.28. Deve ser capaz de guardar no mínimo os seguintes atributos de um ativo:

- Endereço IPv4 e IPv6;
- Sistema Operacional;
- Nome NetBIOS:
- FQDN.

3.2.32.29. A solução deve ser capaz de realizar em tempo real a descoberta de novos ativos para no mínimo:

- Bancos de dados;
- Hypervisors;
- Dispositivos móveis;
- Dispositivos de rede;
- Endpoints;
- Aplicações.

3.2.32.30. Deve realizar em tempo real a identificação de informações sensíveis no tráfego de rede do ambiente;

3.2.32.31. A solução deve ser capaz de identificar a comunicação de malwares na rede de forma passiva;

3.2.32.32. Deve ter a capacidade de guardar em tempo real informações de GET, POST e Download que trafeguem na rede;

3.2.32.33. A solução deve ser capaz de, em tempo real, detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;

3.2.32.34. Permitir identificar vulnerabilidades associadas a servidores SQL no tráfego de rede em tempo real sem a necessidade de um agente;

3.2.32.35. A solução deve ser capaz de realizar varreduras (scans) de vulnerabilidades para o número de ativos contratados;

3.2.32.36. A solução deve ser licenciada pra uso de agentes instalados em estações de trabalho e servidores, para varredura diretamente no sistema operacional, para o número total de ativos contratados.

3.2.32.37. A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo no mínimo Windows, Linux e Mac OS, bem como Hypervisors e Dispositivos de Rede;

3.2.32.38. A solução deverá estar licenciada para varreduras em dispositivos móveis (Ex.: Smartphones, Tablets), sendo realizada através de integração com solução de MDM de mercado ou uso de agente próprio;

3.2.32.39. A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões e gerenciar todos por uma console central;

3.2.32.40. A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento de configurações e vulnerabilidades;

3.2.32.41. A solução deve incluir a capacidade de programar períodos onde varreduras não podem ser executadas em determinados ativos, podendo selecionar no mínimo a frequência da agenda (diário, semanal, etc), hora de início e fim da janela, quais ativos serão excluídos e o fuso horário do agendamento;

3.2.32.42. A solução deve ser configurável para permitir a otimização das configurações de varredura, permitindo no mínimo definir o período de timeout, o número de conexões TCP concorrentes e reduzir a análise em execução caso detecte congestionamento de rede;

3.2.32.43. A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

3.2.32.44. A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até acesso de sistema ou administrativo;

3.2.32.45. A solução deve ser capaz de realizar pesquisas de dados confidenciais;

3.2.32.46. Deve permitir executar uma análise de remediação, para verificar que uma solução foi aplicada corretamente. Essa análise de remediação será executada somente nos ativos impactados, analisando somente a vulnerabilidade remediada, sendo sua política criada especificamente para esta finalidade;

3.2.32.47. Deverá ser possível agrupar sensores em grupos. A solução deverá automaticamente distribuir uma atividade de análise entre os sensores pertencentes ao grupo, para aumentar a performance de um scan;

3.2.32.48. A solução deverá apresentar o status da vulnerabilidade, demonstrando na interface de gerenciamento se a mesma é Nova, Persistente, Corrigida ou Reapareceu no ativo

3.2.32.49. Deverá ser possível aceitar uma vulnerabilidade, onde a mesma não irá mais aparecer na console. Este processo poderá ser feito para um único ativo ou múltiplos ativos. Ainda, deverá ser possível definir uma data de expiração para a Aceitação.

3.2.32.50. Deverá ser possível modificar a severidade das vulnerabilidades, de um único ativo ou múltiplos ativos, podendo ainda definir uma data de expiração para esta modificação

3.2.32.51. A solução deve suportar o uso de Tags nos ativos, sendo estes aplicados de forma manual ou automaticamente;

3.2.32.52. No caso de Tags automáticas, deverá ser possível configurar regras para atender, no mínimo:

3.2.32.53. Ativo analisado ou não em relação a vulnerabilidades;

3.2.32.54. Informações de nuvem pública, como por exemplo Região na AWS, Azure Resource ID ou GCP Cloud Project ID;

3.2.32.55. Deverá ser possível configurar quais usuários, ou grupos de usuários, podem editar as Tags;

3.2.32.56. A solução deverá usar as Tags como filtros, podendo ser utilizadas na lista de vulnerabilidades, onde o objetivo é ver todas as vulnerabilidades existentes nos ativos que possuem determinada Tag;

3.2.32.57. Ser possível fazer análise dos ativos através de Tags, como exemplo todos os Ativos que possuem a Tag Linux;

3.2.33. PLATAFORMA DE GESTÃO DE VULNERABILIDADES EM APLICAÇÕES WEB

3.2.33.1. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web como parte dos ativos a serem inspecionados;

3.2.33.2. A solução deverá ser capaz de executar varreduras em sistemas web através de seus endereços FQDN (DNS);

3.2.33.3. A plataforma deverá avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);

3.2.33.4. A solução deverá ser homologada como PCI ASV;

3.2.33.5. Deve suportar as diretivas PCI ASV 6.1 para definição de balanceadores de carga das aplicações bem como suas configurações para inclusão no relatório de resultados;

3.2.33.6. Deve possuir modelos (templates) prontos de varreduras e também ser possível a criação de modelos customizados;

3.2.33.7. Para varreduras extensas e detalhadas, deve varrer e auditar no mínimo os seguintes elementos:

- Cookies, Headers, Formulários e Links;
- Nomes e valores de parâmetros da aplicação;
- Elementos JSON e XML;
- Elementos DOM.

3.2.33.8. Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

3.2.33.9. Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;

3.2.33.10. Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;

3.2.33.11. Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

3.2.33.12. Deve ser capaz de instituir no mínimo os seguintes limites:

- Número máximo de URLs para crawl e navegação;
- Número máximo de diretórios para varreduras;
- Número máximo de profundidade dos elementos DOM;
- Tamanho máximo de respostas;
- Limite de requisições de redirecionamentos;
- Tempo máximo para a varredura;
- Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
- Número máximo de requisições HTTP por segundo;

3.2.33.13. A solução deve ser capaz de detectar congestionamento de rede e limitar os seguintes aspectos da varredura:

- Limite em segundos para timeout de requisições de rede;
- Número máximo de timeouts antes que a varredura seja abortada;

3.2.33.14. Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;

3.2.33.15. Deve ser capaz de enviar notificações através de no mínimo E-mail;

3.2.33.16. Deve possuir a flexibilidade de selecionar quais testes serão realizados de forma granular, através da seleção de testes, plug-ins ou ataques;

3.2.33.17. Deverá avaliar sistemas web utilizando frameworks modernos, como AJAX, HTML5 e SPA;

3.2.33.18. Deverá possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;

3.2.33.19. Deverá ser compatível com avaliação de RESTful APIs, utilizando o padrão OpenAPI (Swagger);

3.2.33.20. Deverá suportar no mínimo os seguintes esquemas de autenticação:

- Autenticação básica (digest);
- NTLM;
- Form de login;
- Autenticação de Cookies;
- Autenticação através de Selenium;

3.2.33.21. Deve ser capaz de importar scripts de autenticação selenium previamente configurados pelo usuário;

3.2.33.22. Deve ser capaz de customizar parâmetros Selenium como delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

3.2.33.23. Deve ser capaz de exibir os resultados das varreduras em dashboard dedicados para este tipo de análise;

3.2.33.24. Deve ser capaz de exibir os resultados agregados de acordo com as categorias do OWASP Top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project);

3.2.33.25. Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

3.2.33.26. Para cada vulnerabilidade encontrada, deve ser exibido evidências da mesma em seus detalhes;

3.2.33.27. Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc), deve evidenciar nos detalhes do evento encontrado:

- Payload injetado;
- Evidência em forma de resposta da aplicação;
- Detalhes da requisição HTTP;
- Detalhes da resposta HTTP;

3.2.33.28. Os detalhes das vulnerabilidades devem conter descrição da falha e referências didáticas para a revisão dos analistas;

3.2.33.29. Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação das mesmas;

3.2.33.30. A solução deve possuir suporte a varreduras de componentes para no mínimo: Wordpress, Blog Designer Plugin for Wordpress, Event Calendar Plugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Spark e Apache Struts, Atlassian Confluence, Atlassian Crowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;

3.2.33.31. A solução deverá possuir controle de permissão de usuários, com no mínimo 3 níveis, sendo: Administrador, Operador de Scan e Somente Leitura;

3.2.33.32. Deverá possuir a capacidade de manter privado os resultados de um scan, ou seja, não aparecendo o resultado no dashboard da solução;

3.2.33.33. A solução deverá possuir um Add-on para o browser que permite gravar uma macro de autenticação para criação do Selenium;

3.2.33.34. Deverá ser possível excluir a interação com elementos DOM durante o Scan. Está exclusão poderá ser configurada para cada elemento, sendo possível escolher o Conteúdo do texto ou do Atributo CSS.

3.2.33.35. Deverá ser possível exportar os gráficos do dashboard em PDF, PNG ou JPEG, nativamente pela console de gerência.

3.2.33.36. Deve ser possível alterar o user agent utilizado pela solução;

3.2.33.37. A solução deve suportar listas de exclusão globais;

3.2.33.38. Deve possuir um dicionário já criado com as principais páginas comuns e páginas de backup existentes.

3.2.33.39. Deve apresentar a nota do CVSSv3 nas vulnerabilidades encontradas.

3.2.33.40. Deve ser possível gerar relatório das vulnerabilidades, no mínimo em PDF, HTML e CSV.

3.2.34. PLATAFORMA DE GESTÃO DE VULNERABILIDADES EM CONTAINERS

3.2.34.1. A solução deverá ser licenciada contabilizando o número de imagens únicas, não sendo contabilizadas novas versões de uma mesma imagem;

3.2.34.2. A solução de gestão de vulnerabilidades deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações em Containers Docker como parte dos ativos a serem inspecionados;

3.2.34.3. A solução deve ser capaz de analisar imagens preparadas pelos desenvolvedores na esteira DevOps em busca de imagens com vulnerabilidades identificadas e malware residente no sistema de arquivos;

3.2.34.4. A solução deve ser capaz de se integrar a esteira DevOps através de API, invocando o envio da imagem para análise em repositório próprio da solução ou utilizando scanner implementado em infraestrutura proprietária do órgão com a finalidade de evitar o envio de imagens e propriedade intelectual do CONTRATANTE;

3.2.34.5. A documentação de API da solução deverá ter acesso público através de website ou documentação do próprio fabricante;

3.2.34.6. A console de administração deverá possuir controle de acesso no mínimo permitindo usuários com capacidade de somente visualizar as informações, e usuários com capacidade para efetuar análise das imagens;

3.2.34.7. A solução deve inventariar o sistema operacional de cada imagem analisada e suas vulnerabilidades encontradas;

3.2.34.8. A solução deve ser capaz de identificar containers que não foram analisados antes de sua implementação em produção;

3.2.34.9. A solução deve analisar as camadas (layers) de um container;

3.2.34.10. A solução deve ser capaz de identificar containers que tiveram mudanças de arquivos entre a análise e a sua implementação em produção;

3.2.34.11. A solução deve ser capaz de identificar as devidas tags das imagens avaliadas;

3.2.34.12. A solução deve informar os CVEs para cada vulnerabilidade encontrada nos pacotes e bibliotecas residentes na imagem;

3.2.34.13. A solução deve ter a capacidade de testar automaticamente todas as imagens armazenadas, ou previamente testadas, sempre que uma nova vulnerabilidade for publicada e atualizada no banco de dados de vulnerabilidade da solução, sem qualquer tipo intervenção manual;

3.2.34.14. Deve ser capaz de inventariar os pacotes e bibliotecas e suas respectivas versões e listar as mesmas dentro do relatório de resultados de análise de cada imagem;

3.2.34.15. A solução deve possuir conectores e permitir importação de imagens dos seguintes repositórios:

- Docker;
- Docker EE;
- AWS ECR;
- JFrog Artifactory;

3.2.34.16. A solução deve possuir integração com Microsoft Azure Container, Vmware Harbor e Sonatype Nexus para importar e analisar imagens;

3.2.34.17. A solução deve fornecer scanner em formato Docker para implementação local e análise de imagens sem a necessidade de envio destas para repositório remoto, fora do ambiente da CONTRATANTE;

3.2.34.18. A solução deve ser capaz de configurar políticas usando como condições: CVSS Score, CVEs específicos e Malware identificado;

3.2.34.19. Caso a condição da política seja verdadeira, a solução deve ser capaz de prevenir o pull destas para implementação ou identificar a falha de compliance das imagens para ação do time de segurança;

3.2.34.20. A solução deve permitir a criação de políticas especificas por repositório;

3.2.34.21. A solução deve prover integração com as seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernets;

3.2.34.22. A solução deverá ser capaz de analisar vulnerabilidades também na infraestrutura onde as imagens de container são executadas, tanto do sistema operacional quanto das aplicações que nele estão instaladas. Esta capacidade poderá ser nativa da solução, desde que exista uma extensa compatibilidade de sistemas operacionais e aplicações relacionadas a container, algumas já explicitadas em itens anteriores, e já licenciada para uso.

3.2.35. ANÁLISE DE VULNERABILIDADES – ATIVOS NÃO CRÍTICOS

3.2.35.1. Para a análise e varredura dos ativos de infraestrutura não críticos, IoTs e estações de trabalho a serem eleitos pelo CONTRATANTE, a solução deverá atender os requisitos abaixo:

3.2.35.2. Deve possuir personalização de relatórios classificados por vulnerabilidade ou host;

3.2.35.3. Os relatórios devem ser exportados pelo menos em HTML, CSV ou PDF;

3.2.35.4. Deve ser capaz de enviar notificações de resultados de varredura por e-mail;

3.2.35.5. A solução deve prover a descoberta e varredura de ativos:

3.2.35.6. Varreduras incluindo redes IPv4 / IPv6 / FQDN;

3.2.35.7. Varreduras em busca de vulnerabilidades sem utilização de credenciais;

3.2.35.8. Varreduras utilizando credenciais e verificação de patches;

3.2.35.9. Varreduras de sistemas operacionais, dispositivos de rede, hpervisors, base dados, servidores web;

3.2.35.10. Deve possuir trilha de auditoria;

3.2.35.11. Suportar hypervisors pelo menos, Red Hat Enterprise Virtualization (RHEV), VMware, além de outros;

3.2.35.12. Deve ser compatível com os sistemas Operacionais: Windows 7 SP1, 8.1 e 10, Linux Debian 9 e 10 Red Hat ES 6,7 e 8, no mínimo;

3.2.35.13. A verredura por credenciais deve ser suportada nas seguintes bases de dados: Oracle, SQL Server, MySQL, DB2, PostgreSQL, MongoDB;

3.2.35.14. Deve possuir varredura de conformidade personalizada para Windows e Unix,

3.2.35.15. Possuir suporte a detecção de vírus, malwares botnets, processos conhecidos e desconhecidos;

3.2.35.16. A solução deve auditar os agentes do antivírus instalado, informando se estão mal configurados e se estão com regras desatualizadas;

3.2.35.17. Auditoria de configuração baseada no mínimo em critérios do CIS, mas não limitada a outros entes como: CERT, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA, PCI;

3.2.35.18. Possui suporte a configuração de políticas e templates;

3.2.35.19. A solução deve conter pontuação de risco: ranking de vulnerabilidade baseado em CVSS, cinco níveis (crítico, alto, médio, baixo, informações), níveis de gravidade personalizáveis para reformulação de riscos;

3.2.35.20. Possuir escaneamento de quantidade de IPs de destino/dispositivos alvo ilimitados;

3.2.35.21. O Gerenciamento deverá ser realizado por interface web;

3.2.35.22. A solução deve possuir agendamento de escaneamento possibilitando definir subnets ou IP's alvo específicos;

3.2.35.23. A solução deve apresentar formas de resolução ou mitigação das vulnerabilidades, detalhando atualizações e configurações necessárias para eliminar ou, não sendo possível, para reduzir a exposição ao risco;

3.2.35.24. Deve fornecer o acesso a templates (modelos de configuração pré-determinados) de escaneamento para identificação de vulnerabilidades específicas (por exemplo, o ransoware WannaCry e suas variantes);

3.2.35.25. Identificadores CVE (Common Vulnerabilities and Exposures) associados as vulnerabilidades identificadas para geração de relatórios, gerenciamento de riscos e mitigação de ameaças;

3.2.35.26. Identificação de vulnerabilidades de aplicação, tais como: Cross-SiteScripting, SQL Injection e outros;

3.2.35.27. Manutenção do histórico de escaneamentos anteriores.

3.2.36. PROCESSO DE EXECUÇÃO DO SERVIÇO PARA GESTÃO DE VULNERABILIDADES

3.2.36.1. A fim de balizar todo o processo de gestão de vulnerabilidade do TCE-GO, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir.

3.2.36.2. O TCE-GO deverá apresentar uma lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade. Tal lista poderá ser revisitada e atualizada durante todo o período de vigência de contrato, e deverá conter as seguintes informações mínimas, a saber:

- Nome do ativo e/ou serviço;
- Grupo de serviço;
- IP;
- Janela de análise (Horário permitido para análise);
- Prioridade.

3.2.36.3. A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional do TCE-GO, a fim de consultivamente sugerir e complementar a lista de ativos e recursos disponibilizados ao TCE-GO.

3.2.36.4. De acordo com as variáveis e critérios estabelecidos no catálogo de serviço, e na lista de ativos e recursos do TCE-GO, a CONTRATADA deverá realizar checagens (scans) e varreduras, buscando encontrar vulnerabilidades de segurança no ambiente do TCE-GO, utilizando as ferramentas e soluções definidas no presente termo de referência.

3.2.36.5. Após o término das rotinas de checagens (scans) e varreduras no ambiente, deverá a CONTRATADA realizar uma análise de falso positivo das vulnerabilidades descobertas, isso quer dizer, que devem ser informadas ao TCE-GO apenas vulnerabilidades que existam de fato em seu ambiente.

3.2.36.6. Após análise de falso positivo, a CONTRATADA deverá informar ao TCE-GO as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no presente termo de referência.

3.2.36.7. Uma vez autorizada a mudança para correção de uma determinada vulnerabilidade, caberá a CONTRATADA sugerir as correções de vulnerabilidades encontradas no ambiente listado no tópico AMBIENTE TECNOLÓGICO DO TCE-GO (Hardware e Software), obrigatoriamente obedecendo as definições proposta pelo comitê de mudança do TCE-GO.

3.2.36.8. Para as vulnerabilidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá a CONTRATADA apresentar medidas de contorno, que para aplicá-las ao ambiente, deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.

3.2.36.9. Como último passo a CONTRATADA deverá atualizar todos os controles e indicadores, estabelecidos no presente termo de referência.

3.2.36.10. O processo descrito é o mínimo esperado a ser seguido e executado pela CONTRATADA, todavia como o objeto do presente termo de referência se trata

de um serviço continuado, logo espera-se da CONTRATADA a apresentação da melhoria contínua deste, o qual pode ser alterado desde que aprovado pelo TCE-GO.

3.2.36.11. O ciclo de vida do processo de gestão de vulnerabilidade, deve ser executado de forma recorrente. Recorrência está descrita no catálogo de serviço definido e detalhado no anexo II do presente termo de referência. O início do processo não se limita apenas em rotinas de tempo pré-definidas no catálogo de serviço, mas poderá o TCE-GO também solicitar análises sobre demanda a qualquer tempo.

3.2.37. GRUPO TÉCNICO PARA EXECUÇÃO DO SERVIÇO

3.2.37.1. Através dos seus 2 (dois) Centros de Operações de Segurança especificados neste certame, a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), com objetivo e foco de trabalhar no processo de gestão de vulnerabilidades.

3.2.37.2. Todos os profissionais que integram o grupo de ataque cibernético controlado, devem obrigatoriamente compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), não havendo possibilidade a terceirização ou subcontratação de tal serviço.

3.2.37.3. Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no item Gestão de Vulnerabilidade do presente termo de referência.

3.2.37.4. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de gestão de vulnerabilidades do TCE-GO, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), com ao menos 1 (um) perfil de cada que segue descrito abaixo:

Certificações	Descrição
• Linux LPIC 1, Linux LPIC 2 ou Linux LPIC 3; • CompTIA Security+ ou Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC). Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em

segurança da informação.

3.2.37.5. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team).

3.2.37.6. No momento da assinatura do contrato será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA e as devidas certificações técnicas para comprovação do conhecimento.

3.2.38. ENTREGAS

3.2.38.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o TCE-GO definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução, através do portal de indicadores descrito no tópico de condições gerais para prestação do serviço deste termo de referência, a saber:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de vulnerabilidades	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	Número total de vulnerabilidades
Quantitativo de vulnerabilidades de severidade 5 por área responsável	Soma de vulnerabilidades de severidade 5 por área responsável	Vulnerabilidades de severidade 5	Vulnerabilidades	Número total de vulnerabilidades de severidade 5 por área responsável
Quantitativo de vulnerabilidades de severidade 4 por área responsável	Soma de vulnerabilidades de severidade 4 por área responsável	Vulnerabilidades de severidade 4	Vulnerabilidades	Número total de vulnerabilidades de severidade 4 por área responsável
Quantitativo de novas vulnerabilidades de severidades 4 e 5 por área responsável	Soma de novas vulnerabilidades de severidades 4 e 5 por área responsável	Vulnerabilidades de severidades 4 e 5	Vulnerabilidades	Número total de novas vulnerabilidades de severidades 4 e 5 por área responsável
Quantitativo de	Soma de	Vulnerabilidades	Vulnerabilidades	Número total de

vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	vulnerabilidades corrigidas de severidades 4 e 5 por área responsável	corrigidas de severidades 4 e 5		vulnerabilidades corrigidas de severidades 4 e 5 por área responsável
Quantitativo de vulnerabilidades em Aplicações WEB	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 5	Soma de vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades em Aplicações WEB de severidade 5	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 5
Quantitativo de vulnerabilidades em Aplicações WEB de severidade 4	Soma de vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades em Aplicações WEB de severidade 4	Vulnerabilidades	Número total de vulnerabilidades em Aplicações WEB de severidade 4
Quantitativo de novas vulnerabilidades em Aplicações WEB de severidades 4 e 5	Soma de novas vulnerabilidades em Aplicações WEB de severidades 4 e 5	Vulnerabilidades em Aplicações WEB de severidades 4 e 5	Vulnerabilidades	Número total de novas vulnerabilidades em aplicações WEB de severidades 4 e 5
Quantitativo de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Soma de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5	Vulnerabilidades	Número total de vulnerabilidades corrigidas em Aplicações WEB de severidades 4 e 5
Quantitativo de certificados digitais expirados	Soma de certificados digitais expirados	Certificados digitais expirados	Certificados digitais	Número total de certificados digitais expirados
Quantitativo de certificados digitais a expirar em 3 meses	Soma de certificados digitais a expirar em 3 meses	Certificados digitais a expirar em 3 meses	Certificados digitais	Número total de certificados digitais a expirar em 3 meses
TOP 10 – Ativos mais vulneráveis	Soma de vulnerabilidades por ativo	Vulnerabilidades por ativo	Vulnerabilidades	TOP 10 do número de vulnerabilidades por ativo
TOP 10 – Vulnerabilidades mais comuns em ativos	Soma de vulnerabilidades	Vulnerabilidades	Vulnerabilidades	TOP 10 do número de vulnerabilidades
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades	Soma de vulnerabilidades por área responsável	Vulnerabilidades por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades por área

				responsável
TOP 10 – Áreas responsáveis com maior número de vulnerabilidades de severidade 4 e 5	Soma de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do número de vulnerabilidades de severidade 4 e 5 por área responsável
TOP 10 – Áreas responsáveis com percentual de vulnerabilidades de severidade 4 e 5	Percentual de vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades de severidade 4 e 5 por área responsável	Vulnerabilidades	TOP 10 do percentual de vulnerabilidades de severidade 4 e 5 por área responsável
TOP 10 – Aplicações WEB mais vulneráveis	Soma de vulnerabilidades em Aplicações WEB	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB
TOP 10 – Aplicações WEB mais vulneráveis em comparação com OWASP	Soma de vulnerabilidades em Aplicações WEB em comparação com OWASP	Vulnerabilidades em Aplicações WEB	Vulnerabilidades	TOP 10 do número total de vulnerabilidades em Aplicações WEB em comparação com OWASP

Tabela 7 - Indicadores Estratégicos Gestão de Vulnerabilidades

3.2.38.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços prestados e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring). Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências do TCE-GO ou de forma virtual, por meio de solução de videoconferência.

3.3. SERVIÇOS DE OPERAÇÃO E RESPOSTA A REQUISIÇÕES – MSS

3.3.1. Tem por objetivo sustentar e operar as soluções de Firewall e Endpoint Protection através de um catálogo de serviço pré-estabelecido pelo TCE-GO no anexo II do presente termo, porém, não se limitando apenas a este, a CONTRATADA também deverá definir e realizar de forma periódica, ações proativas de acompanhando de todo o parque, a fim de mantê-lo sempre estável, disponível e confiável.

3.3.2. A CONTRATADA deverá realizar um Health Check e estudo de baseline, da situação das ferramentas gerenciadas, criando e apresentando documentação deste estudo

com as possíveis recomendações e melhorias baseadas nas melhores práticas de mercado.

3.3.3. Este serviço ainda tem por finalidade e responsabilidade, gerenciar todo o ciclo de vida de todas as requisições de serviços, referente ao parque de segurança da informação do TCE-GO, visando:

3.3.4. Oferecer canais de comunicação integrados para funcionários autorizados do corpo técnico do TCE-GO requisitarem e receberem devolutivas de serviços pré-definidos, presentes no catálogo de serviço deste instrumento.

3.3.5. Realizar mudanças padrões, pré-definidas e presentes no catálogo de serviço deste instrumento.

3.3.6. Receber reclamações e sugestões a respeito dos serviços prestados.

3.3.7. SOBRE O SISTEMA DE ITSM A SER UTILIZADO

3.3.7.1. Todas as requisições devem ser registradas, controladas, coordenadas, promovidas e gerenciadas por todo o seu ciclo de vida por meio de um único sistema. Isto garante uma abordagem consistente e reproduzível para o tratamento das requisições, e reduz o potencial conflito, e a quantidade de requisições perdidas que possam surgir durante o tratamento.

3.3.7.2. Tal sistema de gestão e controle de requisições de serviço, deve ser do tipo ITSM, do inglês Information Technology Service Management (Gerenciamento de Serviços de TI). E caso o sistema não atenda a contratada deverá substituir por outro sistema que obrigatoriamente deve possuir certificação reconhecida.

3.3.7.3. O sistema de ITSM deve ser obrigatoriamente de propriedade da CONTRATADA, ter suporte e garantia ativos com o fabricante, ser instalado em infraestrutura de propriedade da CONTRATADA, não sendo permitida a utilização de sistemas de ITSM do tipo open source.

3.3.7.4. Para que em qualquer tempo, independentemente do local, funcionários autorizados do corpo técnico do TCE-GO, tenham a possibilidade de abrir requisições para os SOCs (Security Operations Center) da CONTRATADA, o sistema de ITSM utilizado pela CONTRATADA, deverá ser acessível via internet, utilizando protocolo SSL (Secure Socket Layer), com certificado digital emitido em nome da CONTRATADA.

3.3.8. SOLICITANTES AUTORIZADOS E QUALIDADE DOS ATENDIMENTOS

3.3.8.1. Uma das origens de requisição de serviço, poderá ser via interface humana, e a fim de evitar possíveis alterações anômalas e indesejadas no ambiente de segurança da informação, apenas funcionários autorizados do corpo técnico do TCE-GO poderão realizar abertura de requisições de serviços.

3.3.8.2. Sempre que uma nova requisição de serviço for solicitada pelo corpo técnico do TCE-GO, a CONTRATADA deverá previamente observar se tal contato está autorizado a solicitar tais serviços, antes de iniciar o atendimento. Caso tal contato não seja autorizado, o atendimento não deverá ser iniciado, e um comunicado de tentativa de abertura de atendimento não autorizado deve ser enviado ao gestor de contrato do TCE-GO.

3.3.8.3. A CONTRATADA deverá manter uma plataforma para gerir tais contatos autorizados, constando ao menos as seguintes informações dos contatos: nome, telefone, e-mail, cargo. O gerenciamento (criar, atualizar, desativar e remover) desta plataforma, deve estar disponível via internet para o TCE-GO, seguindo os critérios de segurança estabelecido para o sistema de ITSM, ou seja, acessível via internet utilizando protocolo SSL (Secure Socket Layer), com certificado digital emitido em nome da CONTRATADA.

3.3.8.4. Em tal plataforma de gestão de contatos autorizados, deve ter a capacidade de relacionar os contatos autorizados com os itens de configuração de sua responsabilidade, do ambiente de segurança da informação do TCE-GO.

3.3.8.5. Nos primeiros 30 (trinta) dias iniciais do contrato, o TCE-GO informará através de ofício destinado a CONTRATADA, sobre quem e quantos são os contatos autorizados, bem como uma matriz de responsabilidade relacionando aos itens de configuração que compõem a arquitetura de segurança da informação da CONTRATANTE.

3.3.8.6. Após o recebimento do ofício, a CONTRATADA deverá, em até 15 (quinze) dias corridos, disponibilizar os acessos aos canais de comunicação a todos os contatos autorizados. A CONTRATADA ainda deve enviar o comunicado de boas-vindas para cada contato, com manual de acesso a cada canal de comunicação, bem como também suas devidas credenciais.

3.3.8.7. O acesso aos canais de comunicação relacionados no presente termo, de qualquer tipo (telefonia, sistemas, e-mails) devem estar disponíveis para todos os contatos autorizados, a serem relacionados pelo TCE-GO, independentemente da quantidade.

3.3.8.8. No fechamento de toda e qualquer requisição de serviço, independente da severidade e/ou tempo de atendimento, a CONTRATADA deverá enviar uma pesquisa de satisfação para o solicitante. Tal pesquisa deve se basear no método NPS, do inglês Net Promoter Score.

3.3.8.9. Caso a satisfação do atendimento avaliado for menor do que 70% (setenta por cento), um analista de qualidade da CONTRATADA deverá entrar em contato

com o requisitante do serviço, a fim de avaliar com mais detalhes e propriedade as razões pelas quais o atendimento não alcançou a satisfação desejada.

3.3.8.10. Posteriormente, um processo de não conformidade deve ser aberto, e em até 07 (sete) dias úteis deve ser apresentado ao TCE-GO, um plano de ação de melhorias para que eventual insatisfação não volte a acontecer.

3.3.9. CENTRAL DE SERVIÇOS

3.3.9.1. Para atender ao determinado processo apresentado no tópico PROCESSO DE ATENDIMENTO PARA CUMPRIMENTO DE REQUISIÇÃO DE SERVIÇOS do presente termo, a CONTRATADA deverá possuir uma central de serviço, com o objetivo de proporcionar um único ponto de contato para todos os funcionários do TCE-GO, autorizados a realizar uma requisição de serviço.

3.3.9.2. Tal central de serviço deve ser do tipo virtual, ou seja, deve ser instalada fisicamente em ao menos 02 (dois) locais distintos, com distância geográfica de, no mínimo, 300km (trezentos quilômetros) e em estados distintos, e funcionar como uma única central de atendimento, ou seja, ambas devem utilizar e estarem acessíveis através dos mesmos canais de comunicação, obedecendo os requisitos estabelecidos no tópico CANAIS DE COMUNICAÇÃO deste termo, bem como também utilizar do mesmo sistema de ITSM (Information Technology Service Management), obedecendo os requisitos estabelecidos no tópico SOBRE O SISTEMA DE ITSM A SER UTILIZADO.

3.3.9.3. A indisponibilidade física e/ou virtual de uma das centrais de serviços, não pode afetar o funcionamento da oferta de serviço oferecida pela mesma.

3.3.9.4. Tal central terá acesso a dados e informações referente a arquitetura de segurança da informação do TCE-GO, e com o objetivo de manter tais acessos aos dados e informações sobre a governança e legislação brasileira, ambas as centrais de serviço devem, obrigatoriamente, serem instaladas fisicamente no Brasil.

3.3.9.5. Os SOCs (Security Operations Center), devem obrigatoriamente ser de propriedade da CONTRATADA, e ao menos 01 (um) dos SOCs deve possuir certificação ABNT NBR ISO/IEC 20001 em nome da CONTRATADA, sendo proibida a terceirização ou subcontratação de tal ambiente físico e/ou serviço.

3.3.9.6. A qualquer tempo, a CONTRATADA pode ser auditada pelo TCE-GO, e/ou instituição independente CONTRATADA pelo TCE-GO, referente aos itens de controle e normas estabelecidos na ABNT NBR ISO/IEC 20001. Portanto, espera-se que a CONTRATADA tenha evidências e experiência de execução da norma, mesmo antes de ter o contrato assinado com o TCE-GO, referente a tal objeto do presente termo.

3.3.10. PROCESSO DE ATENDIMENTO PARA CUMPRIMENTO DE REQUISIÇÃO DE SERVIÇOS

3.3.10.1. A fim de balizar todo o processo de cumprimento de requisição de serviço do TCE-GO, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual, obrigatoriamente, a CONTRATADA deverá seguir.

3.3.10.2. Ao receber uma solicitação de requisição de serviço via e-mail ou telefone, de funcionários autorizados do TCE-GO, o analista da central de serviços deve registrar ou complementar as informações da requisição.

3.3.10.3. Para requisições de serviços abertas via web, o sistema de ITSM (Information Technology Service Management) deve, automaticamente, realizar o registro da requisição de serviço.

3.3.10.4. Quando o requisitante realiza a requisição através de e-mail ou telefone, o analista da central de serviços deve, após registrar ou complementar a requisição, fazer a categorização e priorização da requisição de serviços.

3.3.10.5. A categorização deve ser realizada pelo analista da central de serviços, relacionando o item de configuração com o seu grupo definido no catálogo de serviço anexo II deste termo. As demais informações levantadas, devem ser documentadas na requisição de serviço.

3.3.10.6. Quando o meio de solicitação for via web, o sistema de ITSM deve realizar a categorização e priorização da requisição de serviço, automaticamente, obedecendo as mesmas regras seguidas pelo processo de registro via e-mail ou telefone.

3.3.10.7. A priorização deve ser realizada de acordo com as regras de negócio estabelecidas no tópico ACORDO DE NÍVEIS DE SERVIÇO deste termo.

3.3.10.8. Caso o analista da central de serviços não identifique o serviço solicitado como um item do catálogo de serviço, deverá informar ao solicitante sobre sua inexistência. Na sequência, o analista deve registrar uma solicitação de novo serviço, ou modificação em serviço existente, que deve ser tratada pelo processo gerenciamento de portfólio do CONTRATANTE.

3.3.10.9. Uma vez identificado, que o serviço requisitado consta no catálogo de serviços, e está disponível, o analista da central de serviços deve verificar se o serviço precisa ou não de aprovação para ser executado. Caso seja necessário, o analista deve submeter a requisição a um grupo aprovador.

3.3.10.10. O sistema de ITSM deve identificar, automaticamente, se o serviço é ou não elegível em primeiro nível, conforme configurado no catálogo de serviços.

3.3.10.11. Caso o serviço seja elegível para primeiro nível, o analista da central de serviço deverá atuar, desde que exista procedimento pré-estabelecido e aprovado pelo CONTRATANTE.

3.3.10.12. É de responsabilidade da CONTRATADA manter uma base de conhecimento, como todos os procedimentos pré-estabelecidos e aprovados pelo TCE-GO. Tal base de conhecimento deve fazer parte do sistema de ITSM, e a qualquer tempo, estar acessível ao TCE-GO para consultas e aprovações de novos procedimentos.

3.3.10.13. Também é de responsabilidade da CONTRATADA a criação, revisão, manutenção, de tais procedimentos operacionais, sendo de responsabilidade do TCE-GO apenas participar como aprovador, sempre que um procedimento for criado, e/ou sofrer algum tipo de alteração.

3.3.10.14. Caso a solução da requisição de serviço dependa da atuação de um terceiro fornecedor do TCE-GO, o analista deve comunicar ao requisitante o status da requisição de serviço (pendente fornecedor), e o prazo previsto para o seu cumprimento. Neste caso, a contagem do acordo de nível de serviço (SLA) é interrompida.

3.3.10.15. O analista da central de serviços que atuou no cumprimento da requisição, deve fazer o registro da sua atuação, descrevendo informações relevantes para o cumprimento daquele serviço em particular.

3.3.10.16. Em caso de solução, o analista da central de serviços que atuou no cumprimento da requisição, deve registrar no sistema de ITSM que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.

3.3.10.17. O analista da central de serviços, ao identificar que a requisição não é elegível em primeiro nível, deve encaminhá-la para o grupo solucionador indicado. Este encaminhamento poderá ser automático, quando o grupo solucionador e a elegibilidade do serviço estiverem determinados no catálogo de serviços.

3.3.10.18. Ao receber uma requisição de serviço, o grupo solucionador deve analisá-la para verificar se compete ao grupo, ou se deve ser encaminhada a outro grupo solucionador e, se para atendê-la, será necessária uma mudança.

3.3.10.19. Ao identificar que uma requisição de serviços encaminhada para a fila do grupo não faz parte do seu escopo, o analista do grupo solucionador deverá redirecioná-la ao grupo mais indicado para atender a requisição. Se compete ao grupo solucionador, este atuará no cumprimento da requisição.

3.3.10.20. Caso seja necessária uma mudança para executar o serviço requisitado, o fluxo segue para o processo gerenciar mudanças. A governança sobre processo de

gestão de mudança não pertence ao objeto deste termo, a CONTRATADA apenas participará, quando convocada sobre o processo de gestão de mudança já estabelecido pelo CONTRATANTE.

3.3.10.21. Se ao buscar atender à requisição de serviço o grupo solucionador identificar que para seu atendimento é necessário direcionar a solicitação a um fornecedor externo (de serviços ou de infraestrutura), deve acionar o fornecedor conforme as regras que serão estabelecidas pelo TCE-GO.

3.3.10.22. Neste ponto, o status do chamado no sistema de ITSM deve ser atualizado para "encaminhado para fornecedor" e ficará aguardando seu retorno.

3.3.10.23. O registro da requisição de serviço na ferramenta do fornecedor, quando for o caso, deve ser documentado no registro da requisição no sistema de ITSM da CONTRATADA. Caberá ao grupo solucionador, acompanhar e monitorar o fornecedor no atendimento da solicitação.

3.3.10.24. Cabe ao grupo solucionador avaliar e validar a entrega efetuada pelo fornecedor. São elementos de controle de qualidade e desempenho desta atividade, os níveis mínimos de serviço, ou as regras definidas no instrumento contratual, edital de licitação e termo de referência.

3.3.10.25. O grupo que atuou no cumprimento da requisição de serviço deve fazer o registro da sua atuação no sistema de ITSM, descrevendo as informações relevantes para o cumprimento daquele serviço em particular.

3.3.10.26. Em caso de solução, o grupo que atuou no cumprimento da requisição deve registrar no sistema de ITSM, que a requisição de serviço foi resolvida, devendo: Informar o(s) item(ns) de configuração envolvido(s) com a requisição; e corrigir a categorização da requisição de serviços, se necessário.

3.3.10.27. Após ser resolvida, a requisição de serviço deve ficar por 03 (três) dias corridos com status igual a resolvido, podendo ser reaberta pelo CONTRATANTE no determinado período, caso este entenda que tal requisição não foi resolvida de fato. Ao final de 03 (três) dias corridos, caso não haja nenhuma intervenção da CONTRATANTE, a requisição deverá ser alterada para o status fechada.

3.3.11. GRUPO TÉCNICO DE OPERAÇÕES

3.3.11.1. Através do seus 02 (dois) SOCs (Security Operations Center), a CONTRATADA deverá manter uma torre de operação denominada GRUPO SOLUCIONADOR, com objetivo e foco de trabalhar no processo de gestão de vulnerabilidades.

3.3.11.2. Este grupo deverá ser exclusivo para trabalhar no GRUPO TÉCNICO DE OPERAÇÕES, não podendo os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos neste termo de referência.

3.3.11.3. Todos os profissionais que integram o GRUPO SOLUCIONADOR, devem, obrigatoriamente, compor o quadro de colaboradores da CONTRATADA em regime de trabalho CLT (Consolidação das Leis do Trabalho), sendo proibida a terceirização ou subcontratação de tal serviço.

3.3.11.4. Deverá ser de responsabilidade da CONTRATADA, dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO deste termo de referência.

3.3.11.5. A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para resolver as requisições de serviço, baseados nas tecnologias e fabricantes que compõem o parque de segurança do TCE-GO, atualmente, a CONTRATADA obrigatoriamente deverá compor o GRUPO SOLUCIONADOR, com ao menos 01 (um) perfil de cada profissional que segue descrito abaixo:

Perfis	Certificações	Descrição
Analista de Segurança Perímetro	ISFS (Information Security Foundation)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC). Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista de Segurança DLP	• CompTIA Security+ • Certificação sobre a plataforma/solução utilizada	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC). Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado.

Analista de Segurança Endpoint	Certificação sobre a plataforma/solução utilizada na CONTRATANTE	Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação. Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC). Conhecimento avançado em segurança da informação, com experiência em operação, sustentação e suporte a ambientes similares ao supracitado. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

Tabela 8 - Certificações e Qualificações do Grupo Solicionador

3.3.11.6. Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO SOLUCIONADOR. Porém, conforme já foi mencionado neste termo de referência, este(s) deve(m) compor única e exclusivamente o time denominado GRUPO SOLUCIONADOR.

3.3.11.7. No momento da assinatura do contrato, será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO SOLUCIONADOR, os quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme a tabela de Certificações e Qualificações do Grupo Solucionador.

3.3.12. ENTREGAS

3.3.12.1. Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, o TCE-GO definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma online e em tempo de execução:

DENOMINAÇÃO	FORMA DE CÁLCULO	FILTRO	AGRUPADOR	DESCRIÇÃO
Quantitativo de requisições abertas	Soma de requisições abertas	Requisições abertas	Requisições	Número total de requisições abertas
Quantitativo de requisições por	Soma de requisições	Requisições por função	Requisições por função	Número total de requisições por

função	abertas por função			função
Quantitativo de requisições concluídas	Soma de requisições concluídas	Requisições concluídas	Requisições concluídas	Número total de requisições concluídas
Quantitativo de requisições em backlog	Soma de requisições em backlog	Requisições em backlog	Requisições em backlog	Número total de requisições em backlog
TOP 10 – Ativos configurados	Soma do número de configurações por ativo	Requisições por ativo	Ativo	TOP do número de requisições por ativo
TOP 10 – Requisições por origem	Soma do número de requisições por origem	Requisições por origem	Origem	TOP do número de requisições por origem
TOP 10 – Aplicações configuradas	Soma do número de aplicações configuradas	Requisições por Aplicações	Aplicações	TOP 10 requisições por aplicações

Tabela 9 - Indicadores Estratégicos de Requisições de Serviço

3.3.12.2. Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com a presença de profissional que conheça todos os serviços prestados, e com uma das seguintes certificações: CISSP (Certified Information Systems Security Professional), CISM (Certified Information Security Manager, CIA (Certified Intrusion Analyst), GSEC (GIAC Security Essentials), GCIH (GIAC Incident Handler) ou GMON (GIAC Continuous Monitoring), conforme condições expostas no tópico

3.3.12.3. Neste contexto, o profissional deve apresentá-lo de forma presencial nas dependências do TCE-GO, ou de forma virtual, por meio de solução de videoconferência.

4. MENSURAÇÃO

4.1. O pagamento será feito mensalmente, levando-se em consideração o Nível Mínimo de Serviço (NMS) acordado em contrato, para o período de faturamento avaliado. O valor a ser pago será o valor unitário do item correspondente, alinhado com o NMS previsto em contrato.

4.2. Conforme ACORDO DE NÍVEIS DE SERVIÇO, os SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO serão medidos, nos seguintes termos:

4.3. DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS: Acompanha a execução do SERVIÇO DE GESTÃO DE DISPONIBILIDADE sobre os ativos de segurança, sob responsabilidade da CONTRATADA.

4.4. As qualificações técnicas exigidas para o perfil de analista(s) que participará do GRUPO DE DISPONIBILIDADE, da CONTRATADA:

Perfis	Certificações	Descrição
Analista de Segurança I	ITIL foundation V3 ou ISFS (Information Security Foundation)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC). Conhecimento pleno em segurança da informação, realizando monitoramento de disponibilidade de ambiente de segurança da informação, similares ao ambiente supracitado. Experiência comprovada de no mínimo 12 (doze) meses em tecnologia da informação.

Tabela 10 - Qualificações do Grupo de Disponibilidade

4.5. No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais que participarão do GRUPO DE DISPONIBILIDADE, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme tabela de exigências de qualificações.

4.6. ENTREGA MENSAL DOS SERVIÇOS: Acompanha a execução de todos os demais serviços que compõem o objeto SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, sobre os ativos de segurança sob responsabilidade da CONTRATADA.

TIPO DE PRIORIDADE	QUANTIDADE DE ATENDIMENTOS REALIZADOS NO PERIODO	QUANTIDADE DE ATENDIMENTOS EM DESACORDO COM O NMS	FATOR DE ABATIMENTO POR DESEMPENHO DE SERVIÇO
P1			
P2			
P3			
P4			
P5			
P6			
P7			
P8			
VTAD (Valor R$ total apurado)			

Tabela 11 - Dashboard de Entrega de Serviços

DENOMINAÇÃO	FORMA DE FILTRO	AGRUPADOR

	CÁLCULO		
Tipo de prioridade	N/A	N/A	N/A
Quantidade de atendimentos realizados no período	Soma de todos os atendimentos realizados no período	Período de apuração	Prioridade
Quantidade de atendimentos em desacordo com o NMS	Soma de todos os atendimentos realizados no período que não estão em conformidade com o NMS	Período de apuração	Prioridade
Fator de abatimento por desempenho de serviço (FADS)	Conforme item ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO	Fator de abatimento por desempenho de serviço (FADS)	Conforme item ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO
VTAD (Valor R$ total apurado)	Soma do total de FADS, e subtrai do valor total previsto para o período	Período de apuração	N/A

Tabela 12 - Legenda de Entrega de Serviços

4.7. A reunião mensal deverá ocorrer até o 5° (quinto) dia útil após o término do período de faturamento, que coincidirá com o mês legal, e a disponibilidade dos relatórios será condição necessária ao recebimento dos serviços pelo TCE-GO. O primeiro mês de faturamento será parcial e proporcional, contado da data da emissão do termo de recebimento definitivo até o último dia do mês. Neste contexto, o profissional deve apresentá-lo de forma presencial nas dependências do TCE-GO, ou de forma virtual, por meio de solução de videoconferência.

4.8. A respectiva nota fiscal/fatura, já deduzidos os fatores de abatimento calculados, deverá ser emitida somente após o recebimento definitivo dos serviços, e após a homologação das informações apresentadas pela CONTRATADA ao TCE-GO.

4.9. A qualquer tempo e a critério do TCE-GO, a bases dos sistemas utilizados para cálculo das entregas e indicadores listados neste tópico, poderão ser solicitadas para auditorias e aferições.

5. EXECUÇÃO DOS SERVIÇOS

5.1. A CONTRATADA deverá atender às seguintes condições gerais para início da prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente e ativação de serviços, sem ônus adicionais ao TCE-GO:

5.2. Reunião de início do projeto (kick-off), a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pelo TCE-GO com 02 (dois) dias úteis de antecedência.

5.3. A reunião poderá ser online (remota), ou presencial na sede do Tribunal de Contas do Estado de Goiás, localizado na Av. Ubirajara Berocan Leite, Nº 640. Setor Jaó, na cidade de Goiânia – GO.

5.4. Serão de responsabilidade da CONTRATADA as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, excluindo-se a Solução de Segurança do TCE-GO já ativa, em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para prévia aprovação pelo TCE-GO;

5.5. A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se necessário, efetuar visita técnica para verificar eventuais requisitos físicos para a correta instalação e prestação dos serviços;

5.6. A conclusão da fase de implantação dos serviços é de até 60 (sessenta) dias corridos, contados a partir da data de início da vigência do contrato, iniciando-se, a partir de então, a fase de prestação mensal dos serviços, apenas após a emissão do termo de recebimento definitivo.

5.7. A elaboração do Projeto Executivo é de responsabilidade da CONTRATADA e deverá atender as seguintes condições:

5.7.1. Conter as fases do projeto, os cronogramas de execução e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase.

5.7.2. Conter a descrição de topologia lógica e física da rede atual e topologia pretendida em cada etapa;

5.7.3. Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade do TCE-GO;

5.7.4. Para a implantação dos serviços, indicar de forma detalhada as condições de rollback de cada mudança no ambiente do TCE-GO;

5.7.5. Estimar o consumo de unidades de rack em U's e de energia de cada ativo a ser instalado nas dependências do TCE-GO;

5.8. Os softwares e demais componentes necessários à correta prestação dos serviços deverão:

5.8.1. Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional do TCE-GO, e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;

5.8.2. Conter a última versão de software e firmware homologado pelo fabricante;

5.8.3. Ter configuradas senhas de acesso para que a equipe de funcionários designados pelo TCE-GO efetue o acesso para a visualização das configurações e logs (acesso seguro e remoto);

5.8.4. Ter configurada senha com direitos totais de administração e configuração a ser utilizada pelo TCE-GO em caso de emergência;

5.9. Para aprovação da instalação e configuração de qualquer item que ensejar a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;

5.10. Quando realizadas no ambiente de produção, as atividades poderão ser agendadas para serem executadas após o horário de expediente, a saber, em horários noturnos – após às 20h00 (vinte horas) – além de finais de semana e feriados, conforme disponibilidade do TCE-GO;

5.11. Se necessário, após a implantação das soluções, será realizada operação assistida em produção com duração de até 30 (trinta) dias corridos. Caso o TCE-GO encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;

5.12. Caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade no TCE-GO, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação, sem quaisquer custos adicionais ao TCE-GO;

5.13. Para todos os componentes da solução, a CONTRATADA deverá implementar e documentar as respectivas configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (hardening), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de kernel, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.

5.14. Para o planejamento e o acompanhamento da instalação dos softwares necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do as-built, e para as demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a CONTRATADA deverá alocar GERENTES DE PROJETOS.

5.15. As qualificações técnicas mínimas exigidas para o perfil de GERENTE DE PROJETO da CONTRATADA são:

Certificações	Descrição

5.16. Ao menos uma das certificações de gerenciamento de projetos: • Project Management Professional (PMP); • Prince2 Practitioner Certificate in Projetct Management; • Professional Scrum Master I.	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC). Conhecimento avançado em gerencia de projetos, com experiência mínima de 12 (doze) meses.

Tabela 13 - Qualificações Gerente de Projeto

5.17. No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais com perfil de GERENTE DE PROJETO, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme a tabela de exigências de qualificações.

6. ACORDO DE NÍVEIS DE SERVIÇO

6.1. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade da prestação dos serviços.

6.2. Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para realização dos pagamentos previstos.

6.3. De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) dos Serviços Gerenciados de Segurança da Informação, são apresentadas, a seguir, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela CONTRATADA na execução do contrato, a saber:

6.4. DISPONIBILIDADE MENSAL DOS GRUPOS DE TECNOLOGIAS

6.4.1. Para os itens 1 a 3 dos Serviços Gerenciados de Segurança da Informação, a Meta de Disponibilidade Mensal (MDM) por grupo de tecnologia deve ser de, no mínimo:

Item	Grupo de Tecnologia	MDM (%)	FPI
1	Gestão de Vulnerabilidades	99	1,5
2	Monitoramento, triagem, tratamento e resposta a	99	1,5

	incidentes de segurança		
3	MSS – Firewall e Antivírus	98	1,5

Tabela 14 - Meta de Disponibilidade Mensal

6.4.2. O SERVIÇO DE GESTÃO DE DISPONIBILIDADE foi arquitetado para garantir e medir a disponibilidade do parque de segurança da informação descrito neste termo de referência. Logo, o mesmo deverá ser utilizado para apurar a meta de disponibilidade mensal (MDM).

6.4.3. Em cada período avaliado, o cálculo do Percentual de Disponibilidade Mensal (PDM) por item de serviço deve ser calculado com a seguinte fórmula:

$$PDM_k = \frac{[TM - TI_k]}{TM} * 100$$

PDM_k = Percentual de Disponibilidade Mensal do k-ésimo item de serviço;

k = k-ésimo item de serviço;

TM = Tempo total mensal de operação, em minutos, no mês de faturamento;

TI_k = Tempo total mensal de indisponibilidade do k-ésimo item de serviço, em minutos, no mês de faturamento.

6.4.4. Devem ser incluídos como Tempo de Indisponibilidade (TI_k):

6.4.4.1. Tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;

6.4.4.2. Tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação.

6.4.5. Não devem ser incluídos como Tempo de Indisponibilidade (TI_k):

6.4.5.1. Falta de energia no local de prestação dos serviços;

6.4.5.2. Indisponibilidade da rede lógica do TCE-GO;

6.4.5.3. Problemas derivados de ocorrências no ambiente do TCE-GO, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;

6.4.5.4. Ações necessárias para resolução de problemas que tenham sido autorizadas pelo TCE-GO;

6.4.5.5. Indisponibilidade gerada pela operadora de telecomunicação responsável pelos links e equipamentos do ambiente do TCE-GO;

6.4.5.6. Fatores externos à prestação dos serviços, desde que justificados e acordados com o TCE-GO;

6.4.5.7. Indisponibilidade do ambiente virtualizado do TCE-GO, infraestrutura computacional em que parte dos softwares que compõem a solução deve ser instalada;

6.4.5.8. Manutenções programadas pelo TCE-GO;

6.4.5.9. Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pelo TCE-GO.

6.4.6. Tickets abertos, cujo prazo de resolução encerre somente no próximo período de faturamento, somente terão calculados os fatores de abatimento, a partir do período seguinte;

6.4.7. Os Fatores de Abatimento por Indisponibilidade de Serviços (FAIS) relativos ao Percentual de Disponibilidade Mensal deverão, ainda, ser multiplicados por um Fator de Peso do Item (FPI), segundo a Tabela 14 - META DE DISPONIBILIDADE MENSAL, por grupo de tecnologia.

6.4.8. O Percentual de Disponibilidade Mensal (PDM) é subsidiário para o cálculo do Fator de Abatimento por Indisponibilidade de Serviço (FAIS), desconto a ser aplicado no valor de prestação mensal de cada conjunto ou item de serviço;

6.4.9. Assim sendo, o Fator de Abatimento por Indisponibilidade de Serviço (FAIS) deve ser calculado de acordo com a seguinte fórmula:

$$FAIS = \sum_{k=1}^{3} VMIk \;\; X \;\; FPIk \;\; X \;\; \left\{ \frac{MDMk - MIN(MDMk, PDk)}{100} \;\; X \;\; MTI \right\}$$

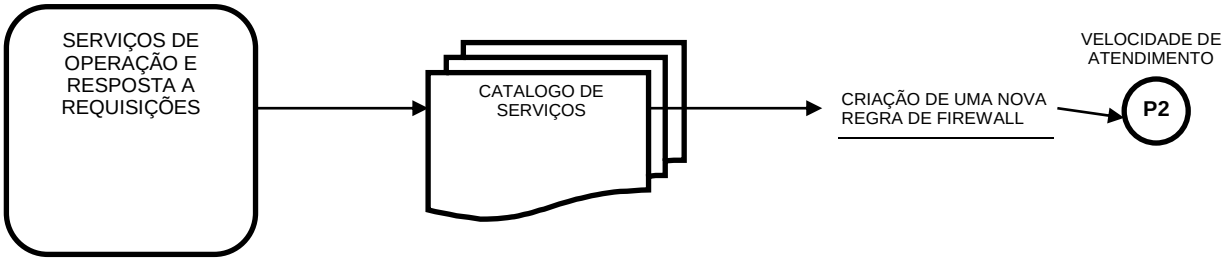
Variável	Descrição
k	Número do grupo de tecnologia
FAIS	Fator de abatimento por indisponibilidade de serviço
VMI	Valor mensal do item de serviço de Gestão de Disponibilidade
FPI	Fator de Peso do Item
MDM	Meta de disponibilidade mensal do item
PD	Percentual de disponibilidade mensal, calculada segundo fórmula supracitada.
MTI	Multiplicador por tempo de indisponibilidade, conforme definido a seguir: Valor = 1, se (MDM - PD) menor ou igual 1; Valor = 2, se (MDM - PD) maior que 1 e menor ou igual a 5; Valor = 3, se (MDM - PD) for maior que 5;
Min	Função que retorna o valor mínimo.

Tabela 15 - Variáveis de Cálculo de Fator de Abatimento por Indisponibilidade de Serviço

6.5. ENTREGA MENSAL DOS SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO

6.5.1. Além da meta de disponibilidade mensal do parque de segurança da informação do TCE-GO, a qual avalia especificamente o SERVIÇO DE GESTÃO DE DISPONIBILIDADE, também deverão ser apurados os níveis de serviço para os demais serviços que, somados, compõem o objeto Serviços Gerenciados de Segurança da Informação.

6.5.2. Todos os serviços que compõem o objeto contratado, possuem catálogo de serviço descrito no anexo II deste termo de referência. Cada item (serviço) que compõe o catálogo de serviço, deve estar relacionado com os tipos de velocidade de atendimento descritos na Tabela 16 deste termo de referência, conforme exemplo ilustrado na figura abaixo:



Tipos	Nível mínimo de serviço (NMS)	IndMeta	Fator de peso da Atividade (FAT)
P1	2 Horas	2 Horas	1
P2	4 Horas	4 Horas	1
P3	8 Horas	8 Horas	0,5
P4	16 Horas	16 Horas	0,5
P5	32 Horas	32 Horas	0,5
P6	64 Horas	64 Horas	0,25
P7	128 Horas	128 Horas	0,25
P8	256 Horas	256 Horas	0,25

Tabela 16 - Níveis de Prioridade de Atendimento

6.5.3. Em um atendimento onde seja necessária uma janela para execução dos serviços solicitados, o tempo transcorrido entre a necessidade do atendimento e a janela de execução, deverão ser excluídos.

6.5.4. Os Fatores de Abatimento por Desempenho de Serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviços definidos na tabela NIVEIS DE PRIORIDADES DE ATENDIMENTO.

6.5.5. O FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir:

$$FADS = \sum_{i=1}^{8}\sum_{j=1}^{n} VMC \times \left[\frac{Max\,(INDATINGi.j, INDMETAi) - INDMETAi}{10 \times INDMETAi}\right] \times FPAi$$

Variável	Descrição
i	Tipo de prioridade.
j	Contador de ocorrências do tipo de prioridade que não atenderam o NMS definido.
n	Quantidade de ocorrências do tipo de prioridade que não atenderam o NMS definido.
FADS	Fator de abatimento por desempenho de Serviço
VMC	Valor mensal do contrato.
INDMETA	Índice de meta (NMS), em minutos/horas/dias, definido para a atividade.
INDATING	Índice atingido, em minutos/horas/dias, pela atividade que ultrapassou o (NMS).
FPA	Fator de peso da atividade.
Max	Função que retorna o valor máximo.

Tabela 17 - Variáveis de Cálculo de Fatores de Abatimento por Desempenho de Serviço (FADS)

7. PAPÉIS E RESPONSABILIDADES

7.1. Durante a vigência contratual, e toda a prestação do serviço objeto desta contratação, deverão ser observados e cumpridos os seguintes papéis e responsabilidades dos profissionais:

7.2. Patrocinador do Projeto: é o Diretor de Tecnologia da Informação, responsável por representar os interesses do TCE-GO no contexto da presente contratação, pela aprovação da necessidade, dos objetivos e, por fim, pela negociação das ações necessárias para a melhoria da Governança de TI;

7.3. Gestor do Contrato: é o servidor formalmente designado pelo TCE-GO, responsável pelo monitoramento da prestação do serviço ao longo do período de vigência do contrato, pelo controle da evolução dos gastos com o contrato, pela proposição de aditamentos ao contrato, pela participação no planejamento da contratação, pela verificação dos resultados pretendidos, e por garantir que a metodologia adequada seja empregada;

7.4. Fiscal do Contrato: é o servidor da unidade de Tecnologia da Informação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução e, também, acompanhar, inspecionar, examinar e verificar a conformidade da execução contratual, subsidiando a atuação do gestor do contrato;

7.5. Preposto (CONTRATADA): é o profissional indicado pelo Fornecedor de Serviço para representá-la administrativa e tecnicamente. É o responsável pela coordenação operacional das atividades previstas nos projetos, de forma a solucionar qualquer dúvida, conflito ou desvio técnico que possa comprometer a execução das OS. Deverá ter bons conhecimentos em gestão de projetos para garantir o controle sobre os sinais vitais de cada projeto. Também é responsável pela interlocução com o Gestor do Contrato do TCE-GO.

7.6. As qualificações técnicas exigidas para o perfil de PREPOSTO da CONTRATADA:

Certificações	Descrição
Ao menos uma das certificações de segurança da informação: • CISSP (Certified Information Systems Security Professional); • CISM (Certified Information Security Manager; • CIA (Certified Intrusion Analyst); • GSEC (GIAC Security Essentials); • GCIH (GIAC Incident Handler); • GMON (GIAC Continuous Monitoring).	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC). Conhecimento avançado em segurança da informação, com experiência mínima de 12 (doze) meses em coordenação e gestão de contratos de serviços continuados.

Tabela 18 - Certificações e Qualificações do Preposto

7.7. No momento da assinatura do contrato, será exigido da CONTRATADA, a apresentação das documentações do(s) profissionais com perfil de PREPOSTO, as quais devem comprovar as exigências e obrigações descritas neste termo de referência: carteira de trabalho devidamente assinada pela CONTRATADA, para comprovação de habilidades, e as devidas certificações técnicas para comprovação do conhecimento conforme Tabela 18.

TERMO DE VISTORIA OPCIONAL

1) Declaro, para fins de convalidação do domínio de informações relevantes para a participação no Pregão Eletrônico nº ____/2022, que vistoriei o ambiente e parque tecnológico do TCE-GO onde serão prestados os serviços e integrados os dispositivos a serem protegidos pela solução.

2) Declaro que estiveram a minha disposição todas as informações necessárias, inclusive as que requisitei para a identificação dos serviços, das condições e dos requisitos licitatórios, tendo sido sanada pela equipe técnica dos órgãos, todas as dúvidas que foram por mim apresentadas e questionadas.

3) Declaro, sob as responsabilidades impostas pela legislação vigente, que a empresa que represento participará da fase de lances exclusivamente na convicção de que cumpre as exigências expressas no Edital.

4) Declaro ainda, que será mantido por mim o sigilo de todas as informações e documentos conhecidos nesta Vistoria, cuidando para que no repasse destas informações a outrem, admitido exclusivamente para formulação de preço e condições de execução, o mesmo compromisso seja firmado formalmente.

Goiânia (GO), ____de_____de 2022

_____

Empresa Licitante
Data, nome, assinatura do responsável pela Visita Técnica e CNPJ da Empresa

_____

TCE GO
Data, nome e assinatura autorizada

ANEXO II

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO Nº 202200047003608

MINUTA DO CONTRATO Nº ____/2022

Constitui objeto do presente instrumento, contratação de empresa especializada para fornecimento de serviços gerenciados de segurança da informação ao Tribunal de Contas Estado de Goiás (TCE-GO).

CONTRATANTE: TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS, inscrito no CNPJ (MF) sob o n.º 02.291.730/0001-14, com sede na Avenida Ubirajara Berocan Leite, nº 640, Setor Jaó, Goiânia–GO – CEP: 74.674-015, neste ato representado por seu **Presidente, Conselheiro Edson José Ferrari.**

CONTRATADA: [Nome da empresa contratada], inscrita no CNPJ (MF) sob o n.º _____, localizada no (a) _____, neste ato representada por _____**,** portador(a) da Cédula de Identidade n.º _____ e inscrito no CPF (MF) sob o n.º _____.

Os **CONTRATANTES** acima qualificados celebram o presente contrato, conforme ato homologatório exarado no Despacho nº ___, de __ de _____ de 2021, da Presidência do TCE-GO, nos autos do **Processo TCE-GO nº 202200047003608**, que fica fazendo parte integrante deste instrumento, realizado nos termos da Lei Federal nº 10.520/02, e subsidiariamente, no que couber, da Lei Federal nº 8.666/93, da Lei Estadual nº 17.928/2012 do Decreto Estadual nº 9.666/2020, com suas alterações e legislação correlata, sujeitando-se às normas dos supramencionados diplomas legais, mediante as cláusulas e condições a seguir estabelecidas.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. A presente licitação tem por objeto a contratação de empresa especializada para fornecimento de serviços gerenciados de segurança da informação ao Tribunal de Contas Estado de Goiás (TCE-GO), compreendendo: Serviço de gestão de vulnerabilidades, Serviço de monitoramento, triagem, tratamento e resposta a incidentes de segurança e Serviço de operação e resposta a requisições, por 12 (doze) meses, de acordo com as especificações constantes do Termo de Referência, dos seguintes itens:

DESCRIÇÃO	QTD	AFERIÇÃO	MÉTRICA	PERÍODO
SERVIÇO DE GESTÃO DE VULNERABILIDADES	1.000	Mensal	Por Ativo	12 meses
SERVIÇO GERENCIADO DE MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA	3.500	Mensal	EPS	12 meses
SERVIÇO DE OPERAÇÕES E RESPOSTAS AS REQUISIÇÕES	2	Mensal	Por solução de SI	12 meses

1.2. Fazem parte integrante deste CONTRATO, para todos os fins de direito, independentemente da transcrição, e obrigando as partes em todos os seus termos, os seguintes documentos:

a) Edital PREGÃO ELETRÔNICO Nº 036/2022 e seus anexos;

b) Proposta da CONTRATADA.

CLÁUSULA SEGUNDA – DA EXECUÇÃO

2.1. Em conformidade com os artigos 73 a 76 da Lei nº 8.666/1993, os itens objeto da prestação dos serviços serão recebidos da seguinte forma:

2.2. Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para a perfeita execução efetiva da prestação dos serviços.

2.2. O dimensionamento da equipe para a execução adequada do serviço contratado é de responsabilidade exclusiva do Fornecedor de Serviço, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência e seus anexos.
Dependendo da complexidade, criticidade e do prazo do projeto, os serviços poderão ser realizados nas instalações da CONTRATADA ou do TCE-GO.
Todos os custos com licenças de simuladores e softwares devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extras, seja a que título for.

2.3. O período de prestação dos serviços, a partir da emissão do termo de recebimento definitivo, será o estabelecido na tabela abaixo, observadas as etapas previstas no item EXECUÇÃO DOS SERVIÇOS do Anexo IV do presente Termo de Referência. As quantidades da tabela abaixo foram baseadas no ambiente especificado no Anexo III deste Termo de Referência e em estimativa de fluxo de dados no switch principal do TCE-GO.

DESCRIÇÃO	QTD	AFERIÇÃO	MÉTRICA	PERÍODO
SERVIÇO DE GESTÃO DE VULNERABILIDADES	1.000	Mensal	Por Ativo	12 meses
SERVIÇO GERENCIADO DE MONITORAMENTO, TRIAGEM, TRATAMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA	3.500	Mensal	EPS	12 meses
SERVIÇO DE OPERAÇÕES E RESPOSTAS AS REQUISIÇÕES	2	Mensal	Por solução de SI	12 meses

2.4. A partir da assinatura do contrato, correrão os seguintes prazos:

2.5. Reunião de início do projeto (kick-off): a ser realizada em até 10 (dez) dias corridos após a assinatura do contrato, a ser previamente agendada pelo TCE-GO com 02 (dois) dias úteis de antecedência.

2.6. Entrega do Projeto Executivo: até 30 (trinta) dias corridos, contados a partir da reunião de início do projeto (kick-off);

2.7. O TCE-GO se manifestará no prazo de até 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;

2.8. Havendo necessidade de ajustes, a CONTRATADA terá até 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo TCE-GO, a respeito da manifestação sobre o Projeto Executivo;

2.9. A conclusão da fase de implantação dos serviços é de até 60 (sessenta) dias corridos, contados a partir da data de início da vigência do contrato, mediante a emissão do termo de recebimento definitivo pelo TCE-GO.

2.10. O termo de recebimento definitivo obedecerá os seguintes critérios:

2.11. O TCE-GO terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo, depois de finalizado o planejamento, customização e a instalação do ambiente;

2.12. A prestação dos serviços mensais iniciará somente a partir da emissão do termo de recebimento definitivo pelo TCE-GO;

2.13. Para todos os bens importados, caso necessários por parte da CONTRATADA, que sejam instalados nas dependências do TCE-GO, será necessária a apresentação dos respectivos comprovantes de origem.

2.14. Os Centros de Operações de Segurança da CONTRATADA deverão estar em pleno funcionamento, operando em regime 24x7x365, em até – no máximo – 90 (noventa) dias corridos, contados da data de início da vigência contratual.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

3.1. São obrigações do TCE-GO:

3.1.2 Efetuar o pagamento à CONTRATADA de acordo com as condições de preços e prazos do Termo de Referência.

3.1.3 Prestar todas as informações e os esclarecimentos solicitados pela CONTRATADA.

3.1.4 Comunicar a CONTRATADA toda e quaisquer ocorrências relacionadas com o fornecimento dos produtos.

3.1.5. Acompanhar e fiscalizar os serviços, quanto aos aspectos qualitativos e quantitativos, anotando em registro próprio as falhas e solicitando as medidas corretivas, podendo sustar, recusar, solicitar fazer ou desfazer qualquer entrega ou serviços, no todo ou em parte, que não estejam de acordo com as condições e exigências estabelecidas no Termo de Referência.

3.1.6. Emitir relatórios sobre os atos relativos à execução do contrato que vier a ser firmado, em especial, quanto ao acompanhamento e fiscalização da execução dos serviços, à exigência de condições estabelecidas e proposta de aplicação de sanções.

3.1.7 O CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, bem como por quaisquer ônus, direitos ou obrigações vinculadas à legislação tributária, trabalhista, previdenciária ou securitária, e decorrentes da execução do estabelecido no termo de referência, cujo cumprimento e responsabilidades caberão, exclusivamente, à CONTRATADA.

3.1.8 Aplicar a CONTRATADA, as penalidades previstas nas leis que regem a matéria e, especificamente este Contrato, pelo descumprimento de suas cláusulas.

3.1.9 Transmitir as suas orientações e instruções por escrito, salvo em situações de urgência ou emergência, sendo-lhe reservado o direito de solicitar da CONTRATADA, por escrito, a posterior confirmação de ordens ou instruções verbais;

3.1.10 Respeitar a titularidade do direito autoral, patrimonial e comercial da CONTRATADA sobre os produtos fornecidos, seus componentes de software, suas adaptações, derivações e customizações resultantes da execução dos serviços objeto deste Termo de Referência, comprometendo-se a não doar, ceder, disponibilizar e permitir o manuseio e utilização dos códigos-fonte e componentes de software por terceiros ou praticar qualquer outra forma de transferência dos aplicativos sem anuência da CONTRATADA, conforme legislação específica;

3.1.11. Tomar providências necessárias para que sejam seguidas as recomendações da CONTRATADA, concernentes às condições de uso correto da solução;

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATADA

4.1. A empresa CONTRATADA deve ser comprometer a:

4.1.2. Comprovar a origem dos bens importados oferecidos e a quitação dos tributos de importação a eles referentes, se houver, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa;

4.1.3. Dar plena e fiel execução ao contrato, respeitadas todas as cláusulas e condições estabelecidas;

4.1.4. Substituir, arcando com as despesas decorrentes, o produto que não se conformar com as especificações deste termo, no prazo de 10 (dez) dias, contados a partir da data do termo de recusa;

4.1.5. Assumir integral responsabilidade pela boa execução e eficiência dos serviços que realizar, assim como pelos danos causados, direta ou indiretamente ao Contratante ou a terceiros, em virtude de culpa ou dolo na execução do contrato, independente de ocorrerem ou não em áreas afetas à execução de suas atividades;

4.1.6. Exigir que seus técnicos ou empregados se apresentem nas dependências do Tribunal de Contas do Estado de Goiás devidamente identificados;

4.1.7. Executar todos os serviços obedecendo a melhor técnica vigente, enquadrando-os, rigorosamente, dentro dos preceitos normativos da ABNT – Associação Brasileira de Normas Técnicas;

4.1.8. Emitir Nota Fiscal/Fatura correspondente à sede ou filial da empresa que apresentou a documentação na fase de habilitação;

4.1.9. Considerar que a ação de fiscalização da Administração do Tribunal de Contas de Estado de Goiás não exonera a empresa a ser contratada de suas responsabilidades contratuais;

4.1.10. Dar plena e fiel execução ao contrato, respeitadas todas as cláusulas e condições estabelecidas;

Usar mão de obra capacitada, que assegure a execução integral dos serviços nos prazos convencionados com segurança e qualidade;

4.1.11. Fornecer telefone e e-mail para comunicação entre as partes; e

4.1.12. Tratar com urbanidade e respeito qualquer servidor ou pessoa dentro das dependências desta Corte;

4.1.13. Sendo necessário algum tipo de serviço, estes deverão ser prestados no horário de 7:00h às 19:00h, nos dias úteis, e sempre que possível nas dependências do CONTRATANTE;

4.1.14. Fornecer os produtos e prestar os serviços requeridos nas condições e prazos estipulados neste Termo de Referência e seus anexos;

4.1.15. Observar os processos de trabalho, políticas e normas internas do TCE-GO;

4.1.16. Assumir a responsabilidade, sem qualquer espécie de solidariedade por parte do TCE-GO, pelos encargos previdenciários e obrigações sociais previstas na legislação em vigor, obrigando-se a saldá-los na época própria, bem como pelos encargos fiscais e comerciais resultantes da contratação e pelos decorrentes de eventual demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência;

4.1.17. Manter-se, durante o período de vigência do contrato, em compatibilidade com as condições de habilitação e qualificação exigidas na licitação;

4.1.18. Planejar, desenvolver, implantar, executar e manter os serviços de acordo com os níveis de serviço estabelecidos neste Termo de Referência e seus anexos;

4.1.19. Reparar, corrigir, remover, reconstruir ou substituir às suas expensas, no todo ou em parte, serviços efetuados nos quais se verificar vícios, defeitos ou incorreções;

4.1.20. Não transferir a outrem, no todo ou em parte, o objeto do Contrato, exceto quando autorizado formalmente pelo TCE-GO, respeitando-se os limites e preceitos legais.

CLÁUSULA QUINTA – DIREITOS DO TCE-GO

5.1. Rejeitar, no todo ou em parte, os produtos/serviços entregues/executados em desacordo com as exigências das especificações técnicas estampadas no Termo de Referência.

CLÁUSULA SEXTA - DOS PREÇOS E DOS CRÉDITOS ORÇAMENTÁRIOS

6.1. O valor do presente Contrato é de R$ ____ (_____) de acordo com os valores especificados na Proposta de preços.

6.2. As despesas decorrentes dos serviços relativas ao presente exercício correrão à conta do crédito orçamentário _____, Grupo _____, Fonte _____, Tipo de Recurso _____, na Natureza de Despesa _____ – _____.

6.3. Para fazer face à despesa, foi emitida pela CONTRATANTE a Nota de Empenho nº ____.

CLÁUSULA SÉTIMA - DO PAGAMENTO, FISCALIZAÇÃO E GERENCIAMENTO

7.1. A gestão e a fiscalização do contrato competirão respectivamente aos servidores Licardino Siqueira Pires (Gerente de Tecnologia da Informação) e Bruno Henrique de Oliveira Peixoto (Chefe do Serviço de Sistemas da Informação), conforme designado no inciso I do art. 1º da Portaria nº 128/2021 do Tribunal de Contas do Estado de Goiás.

7.2. À fiscalização caberá ainda:

7.2.1 assegurar-se da boa qualidade dos materiais recebidos, verificando sempre a conformidade dos mesmos com as especificações das marcas e modelos de referência;

7.2.2 documentar as ocorrências havidas e fiscalizar o cumprimento das obrigações contratuais assumidas pela CONTRATADA, inclusive quanto à não interrupção dos serviços prestados;

7.2.3. emitir pareceres em todos os atos relativos à execução do Contrato, em especial quando da necessidade de aplicação de sanções, alterações e repactuações do Contrato.

7.2.4 A fiscalização nos moldes do Termo de Referência não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados ao Tribunal de Contas do Estado de Goiás ou a terceiros, resultantes de imperfeições técnicas, vícios ou defeitos

ocultos de serviços que os desqualificam para o uso normal e rotineiro e, na ocorrência destes, não implica corresponsabilidade do TCE-GO ou de seus agentes e prepostos.

7.3. Ao Tribunal de Contas do Estado de Goiás caberá:

7.3.3. Apresentar à CONTRATADA as observações, reclamações e exigências que se impuserem em decorrência da Fiscalização;

7.3.4. Notificar à CONTRATADA, por escrito, sobre a ocorrência de eventuais imperfeições na nos produtos, fixando prazo para sua correção, conforme sua conveniência.

7.4. À CONTRATANTE não caberá qualquer ônus pela rejeição de serviços ou materiais considerados inadequados pelo Fiscal.

7.5. Será emitida nota de empenho em favor da empresa adjudicatária, após a homologação da licitação, caso se efetive a contratação.

7.6. O pagamento será efetuado de acordo com os valores estipulados no Contrato Administrativo firmado com a CONTRATADA, sendo realizado de acordo com as Ordens de Serviço ou de Fornecimento de Bens;

7.7. Os serviços entregues serão homologados pelos Fiscais e Gestor do Contrato;

7.8. A Aceitação dar-se-á após a assinatura do TERMO DE RECEBIMENTO DEFINITIVO;

7.9. O Tribunal de Contas do Estado de Goiás - efetuará o pagamento até o 30º (trigésimo) dia do mês subsequente à entrega definitiva devidamente atestada pela Gerência de Tecnologia da Informação.

7.10. O pagamento será creditado em favor da adjudicatária, por meio de Ordem Pagamento, em qualquer instituição bancária indicada na Nota Fiscal, devendo, para isto, ficar especificado o nome do banco, agência com a qual opera, localidade e número da conta corrente em que deverá ser efetivado o crédito.

7.11. O TCE-GO não efetuará pagamento por meio de títulos de cobrança bancária.

7.12. Qualquer erro ou omissão ocorrido na documentação fiscal será motivo de correção por parte da adjudicatária e haverá, em decorrência, suspensão do prazo de pagamento até que o problema seja definitivamente sanado.

7.13. Quando do pagamento a ser efetuado pelo Tribunal de Contas do Estado de Goiás, a adjudicatária deverá comprovar sua regularidade no tocante à Documentação Obrigatória (Receita Federal, Dívida Ativa da União, Estado e Município, FGTS, INSS e Justiça do Trabalho). Tal comprovação será objeto de confirmação “ON LINE”, sendo suspenso o pagamento, caso esteja irregular.

7.14. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação das obrigações, em virtude de penalidades impostas à CONTRATADA ou inadimplência total ou parcial referente à contratação.

7.15. Não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação das obrigações, em virtude de penalidades impostas à CONTRATADA ou inadimplência total ou parcial referente à contratação.

7.16. O TCE/GO reserva-se o direito de suspender o pagamento se o produto entregue estiver em desacordo com as especificações constantes no Edital e em seus Anexos.

7.17. O TCE/GO reserva-se o direito de suspender o pagamento se o produto entregue estiver em desacordo com as especificações constantes no Edital e em seus Anexos.

7.18. No caso de atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, serão devidos pela CONTRATANTE encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples;

7.18.1. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

7.19. No ato do pagamento será comprovada a manutenção das condições iniciais de habilitação quanto à situação de regularidade da CONTRATADA.

CLÁUSULA OITAVA - DA VIGÊNCIA

8.1. A vigência da contratação será de 12 (DOZE) meses à partir da assinatura do contrato, podendo ser prorrogado até o limite de 60 (sessenta) meses.

8.2. Para efeitos de continuidade da vigência contratual, a cada 12 (doze) meses, todos os itens são considerados como serviços de natureza continuada, e poderão ser renovados anualmente até o limite de 60 (sessenta) meses.

8.3. A CONTRATADA deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei nº 8.666/93.

8.5. A CONTRATADA deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei nº 8.666/93.

CLÁUSULA NONA – DOS CRITÉRIOS DE REAJUSTE

9.1. A periodicidade para eventual reajuste de preços do contrato será anual, contando-se a partir da data limite para apresentação da proposta comercial pela CONTRATADA e aceita pela CONTRATANTE, ou do último reajuste, adotando-se como parâmetro o Índice de Custo da

Tecnologia da Informação (ICTI), ocorrido nos últimos 12 (doze) meses, e ainda, os preços praticados no mercado e a negociação entre as partes.

CLÁUSULA DÉCIMA - DAS SANÇÕES ADMINISTRATIVAS

10.1 Ficará impedido de licitar e de contratar com o Estado e será descredenciado no CADFOR, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato, além das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

a) não assinar o contrato ou a ata de registro de preços;

b) não entregar a documentação exigida no edital;

c) apresentar documentação falsa;

d) causar o atraso na execução do objeto;

e) não mantiver a proposta;

f) falhar na execução do contrato;

g) fraudar a execução do contrato;

h) comportar-se de modo inidôneo;

i) declarar informações falsas; e

j) cometer fraude fiscal.

10.2 As sanções serão registradas e publicadas no CADFOR.

10.3 As sanções descritas no item 11.1, também se aplicam aos integrantes do cadastro de reserva em pregão para registro de preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.

10.4 A multa poderá ser descontada dos pagamentos eventualmente devidos ou ainda, quando for o caso, cobrada judicialmente.

10.5. Pela inexecução parcial ou total das condições pactuadas, garantida a prévia defesa, ficará a CONTRATADA sujeita às seguintes sanções:

a) Advertência;

b) Multa sobre o valor total do contrato, observados os seguintes limites:

I - 10% (dez por cento) sobre o valor do contrato ou instrumento equivalente, em caso de descumprimento total da obrigação, inclusive no caso de recusa do

adjudicatário em assinar o Contrato ou retirar o instrumento equivalente, dentro de 10 (dez) dias contados da data de sua convocação;

II - 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do serviço não realizado;

III - 0,7% (sete décimos por cento) sobre o valor da parte do serviço não realizado, por cada dia subsequente ao trigésimo.

c) Impedimento de licitar e contratar com a Administração Pública Estadual e descredenciamento do CADFOR pelo prazo de até 5 (cinco) anos.

10.5.1. A inexecução contratual, também poderá dar causa a rescisão contratual sem prejuízos das demais penalidades previstas na Lei nº 8.666/93;

10.6. A multa, aplicada após regular processo administrativo, será recolhida em favor do CONTRATANTE, no prazo máximo de 10 (dez) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente, ou será descontada dos pagamentos devidos à CONTRATADA ou, ainda, quando estas não ocorrerem ou não forem suficientes, o saldo será inscrito na Dívida Ativa do Estado e cobrado judicialmente.

10.7. A critério da Administração poderão ser suspensas as penalidades, no todo ou em parte, quando o atraso no fornecimento dos itens ou da prestação dos serviços for devidamente justificado pela CONTRATADA e aceito pela Administração da CONTRATANTE, que fixará novo prazo, improrrogável, para a completa execução das obrigações assumidas.

10.8. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isolada ou cumulativamente, sem prejuízo de outras medidas cabíveis e previstas na Lei nº 8.666/93 e na Lei Estadual nº 17.928/2012.

10.9. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, com oportunidade de defesa prévia da interessada, no respectivo processo, no prazo de 5 (cinco) dias úteis, observando-se o procedimento previsto na Lei nº 8.666, de 1993 e, subsidiariamente, na Lei Estadual nº 13.800, de 2001.

10.10. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

CLÁUSULA DÉCIMA PRIMEIRA - DA RESCISÃO

11.1. O descumprimento de qualquer cláusula ou de simples condição deste contrato, assim como a execução do seu objeto em desacordo com o estabelecido em suas cláusulas e condições, dará direito ao CONTRATANTE de rescindi-lo mediante notificação expressa, sem que caiba à CONTRATADA qualquer direito, exceto o de receber o estrito valor correspondente ao fornecimento realizado, desde que estejam de acordo com as prescrições ora pactuadas, assegurada a defesa prévia.

11.2. Este Contrato poderá, ainda, ser rescindido nos seguintes casos:

a) decretação de falência, pedido de concordata ou dissolução da CONTRATADA;

b) alteração do Contrato Social ou a modificação da finalidade ou da estrutura da CONTRATADA, que, a juízo do CONTRATANTE, prejudique a execução deste pacto;

c) transferência dos direitos e/ou obrigações pertinentes a este Contrato, sem prévia e expressa autorização do CONTRATANTE;

d) cometimento reiterado de faltas, devidamente anotadas;

e) no interesse do CONTRATANTE, mediante comunicação com antecedência de 05 (cinco) dias corridos;

f) no caso de descumprimento da legislação sobre trabalho de menores, nos termos do disposto no inciso XXXIII do art.7º da Constituição Federal.

CLÁUSULA DÉCIMA SEGUNDA – DA ALTERAÇÃO CONTRATUAL

12.1. Este contrato pode ser alterado nos casos previstos no art. 65 da Lei Federal nº 8.666/93, desde que haja interesse da CONTRATANTE, com a apresentação das devidas justificativas.

CLÁUSULA DÉCIMA TERCEIRA - DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO DO CONTRATO

13.1. O presente Contrato fundamenta-se nas Leis Federais nºs 10.520/2002 e 8.666/1993, na Lei Estadual nº 17.928/2012 e Decreto Estadual nº 9.666/2020, e vincula-se ao Edital e seus Anexos do Pregão Eletrônico nº 036/2022, constante do Processo nº 202200047003608, bem como à proposta da CONTRATADA.

CLÁUSULA DÉCIMA QUARTA - DA PUBLICAÇÃO

14.1. A publicação do presente contrato no Diário Oficial do Estado, por extrato, será providenciada até o 5º (quinto) dia útil do mês seguinte ao de sua assinatura, para ocorrer no prazo de 20 (vinte) dias corridos, daquela data, correndo as despesas às expensas da CONTRATANTE.

CLÁUSULA DÉCIMA QUINTA - DO FORO

15.1. As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas pela Justiça Estadual, no foro da Comarca de Goiânia, Estado de Goiás.

CLÁUSULA DÉCIMA SEXTA - DA FRAUDE E DA CORRUPÇÃO

16.1. A CONTRATADA deverá observar os mais altos padrões éticos durante o fornecimento dos gêneros/produtos objetos deste contrato, estando sujeitas às sanções previstas na legislação brasileira.

16.2. Pela inexecução total ou parcial, ou ainda pelo descumprimento de qualquer das suas obrigações, estará sujeita às sanções administrativas previstas neste contrato e na legislação aplicável, cuja individualização será definida pela gravidade do ato praticado, podendo haver cumulação de sanções ou cumulação de sanções com penalidades.

16.3. Se ficar comprovado que um funcionário da CONTRATADA ou quem atue em seu lugar incorreu em práticas corruptas, a CONTRATANTE poderá declarar inelegível a CONTRATADA e/ou seus funcionários diretamente envolvidos em práticas corruptas, temporária ou permanentemente, para participar em futuras licitações ou contratos.

CLÁUSULA DÉCIMA SÉTIMA - SIGILO E PROPRIEDADE

17.1. Manter a mais absoluta confidencialidade a respeito de quaisquer informações, dados, processos, modelos ou outros materiais de propriedade do TCE-GO ou de terceiros, aos quais tiver acesso em decorrência da prestação de serviços objeto do contrato, ficando terminantemente proibida de fazer uso ou revelar estes, sob qualquer justificativa.

17.2. A CONTRATADA deverá observar na condução de suas atividades as diretrizes estabelecidas pela Política de Segurança da Informação do TCE-GO.

CLÁUSULA DÉCIMA OITAVA - DAS DISPOSIÇÕES FINAIS

18.1. Declaram as partes que este Contrato corresponde à manifestação final, completa e exclusiva do acordo entre elas celebrado.

18.2. E, por assim estarem justos e contratados, assinam este instrumento contratual em 02 (duas) vias de igual teor e forma, na presença das testemunhas abaixo, para todos os efeitos legais.

Gabinete da Presidência do **TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS,** em Goiânia, aos _____ dias do mês de _____ de 2022.

_____
Conselheiro Edson José Ferrari
TRIBUNAL DE CONTAS DO ESTADO DE GOIÁS
CONTRANTE

_____
Nome do Representante
NOME DA EMPRESA
CONTRATADA

ANEXO III

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO ELETRÔNICO Nº 202200047003608

MODELO DE PROPOSTA

NOME DA EMPRESA:
ENDEREÇO:
CNPJ/MF:
INSCRIÇÃO ESTADUAL/MUNICIPAL:
PRAZO DE VALIDADE DA PROPOSTA:

PLANILHA MODELO ANEXO II DO TERMO DE REFERÊNCIA

NOTA: As licitantes devem apresentar planilha orçamentária com data base referente à data de abertura das propostas.

O prazo de validade da proposta de preços não será inferior a 60 (sessenta) dias corridos, contados da data do envio da proposta atualizada em conformidade com o último lance ofertado no Sistema Eletrônico.

Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus Anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas no Termo de Referência.

Declaramos que nos preços cotados estão incluídas todas as despesas que, direta ou indiretamente, fazem parte do presente objeto, tais como gastos da empresa com suporte técnico e administrativo, impostos, seguros, taxas, ou quaisquer outros que possam incidir sobre gastos da empresa, sem quaisquer acréscimos em virtude de expectativa inflacionária e deduzidos os descontos eventualmente concedidos.

Caso nos seja adjudicado o objeto da Licitação, comprometemos a assinar o Contrato/entregar o objeto, no prazo determinado no documento de convocação, e para esse fim fornecemos os seguintes dados:

Razão Social: _____
CNPJ/MF: _____
Endereço: _____
Tel./Fax: _____
CEP: _____
Cidade: _____ UF: _____
Banco: _____ Agência: _____ c/c: _____

Dados do Representante Legal da Empresa para assinatura do Contrato:

Nome:_____
Endereço:_____
CEP:_____Cidade:_____UF:_____
CPF/MF:_____Cargo/Função:_____
RG nº:_____Expedido por: _____
Naturalidade: _____Nacionalidade: _____

Goiânia, ___ de _____ de 2022.

_____
Representante Legal
(com carimbo da empresa)

ANEXO IV

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO Nº 202200047003608

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO À HABILITAÇÃO

(NOME DA EMPRESA) _____, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº _____, sediada (endereço completo)_____, por meio de seu representante legal (nome)_____, inscrito no CPF/MF sob o nº_____, portador do RG nº _____, DECLARA sob as penas da lei, que até a presente data, **inexiste** fato superveniente impeditivo para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

_____
Local e Data

_____
Representante Legal
(com carimbo da empresa)

ANEXO V

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO nº 202200047003608

DECLARAÇÃO DE NÃO EMPREGAR MENOR

(NOME DA EMPRESA) _____, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº _____, sediada (endereço completo)_____, por meio de seu representante legal (nome)_____, inscrita no CPF/MF sob o nº_____, portador do RG nº _____, **DECLARA** para fins do disposto no inciso V do art. 27 da Lei Federal nº 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, em conformidade com o previsto no inciso XXXIII, do art. 7º, da Constituição Federal/88, que **não possui** em seu quadro de pessoal empregado(s) menor(es) de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos.

_____
Local e Data

_____
Representante Legal
(com carimbo da empresa)

ANEXO VI

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO nº 202200047003608

DECLARAÇÃO PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE

(Nome da empresa)....., inscrita no CNPJ nº....., por intermédio de seu representante legal o(a) Sr.(a)....., portador(a) da Carteira de Identidade nº..... e do CPF nº....., **DECLARA**, para fins legais, ser microempresa/empresa de pequeno porte nos termos do artigo 3º da Lei Complementar nº 123/2006, não estando incurso nas exclusões do § 4º do citado artigo.

_____
Local e Data

_____
Representante Legal
(com carimbo da empresa)

ANEXO VII

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO nº 202200047003608

DECLARAÇÃO QUE NÃO POSSUI PARENTESCO

(Nome da empresa)_____, pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº _____, portadora da inscrição estadual/municipal nº _____, através de seu representante legal, _____(nome), _____(qualificar)_____, inscrito no CPF/MF sob o nº _____, portador do RG nº _____, **DECLARA**, para todos os fins de direito e sob as penas da lei, que **não possui** em seus quadros de empregados e em seu corpo acionário cônjuge, companheiros ou parentes em linha reta ou colateral, até o terceiro grau, ou por afinidade, até o segundo grau, de Conselheiros, Auditores e Procuradores de Contas do Tribunal de Contas do Estado de Goiás, e ainda, com os servidores detentores de cargo em comissão ou função de confiança que atuem diretamente na realização do certame e/ou na posterior formalização contratual.

_____
Local e Data

_____
Representante Legal
(com carimbo da empresa)

ANEXO VIII

EDITAL DO PREGÃO ELETRÔNICO Nº 036/2022

PROCESSO nº 202200047003608

MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

Declaro, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico nº 036/2022, instaurado pelo Processo nº 202200047003608, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas do meio ambiente.

Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para contratação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da Instrução Normativa nº 01, de 19 de janeiro de 2010, do Ministério do Planejamento, Orçamento e Gestão (MPOG).

Estou ciente da obrigatoriedade da apresentação do registro no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais, caso minha empresa exerça uma das atividades constantes no Anexo II da Instrução Normativa nº31, de 03 de dezembro de 2009, IBAMA.

Por ser a expressão da verdade, firmamos o presente.

Goiânia,____ de _____de 2022.
Nome:
RG/CPF:
Cargo: