



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

EDITAL

(x) Contratação delegada

COMPONENTES DO EDITAL

- I. PREÂMBULO**
- II. PARTE FIXA**
- III. TR/HABILITAÇÃO**
- IV. MINUTA DE CONTRATO**
- V. ANEXOS DO EDITAL**

I. PREÂMBULO

1. Regência legal:

Em conformidade com as regras estipuladas no Contrato de Empréstimo n.º 4970/OC-BR, celebrado no dia 19 de abril de 2022, entre o Banco Interamericano de Desenvolvimento (BID) e o Estado da Bahia, da República Federativa do Brasil, para financiamento do Programa de Modernização e Fortalecimento da Gestão Fiscal do Estado da Bahia – PROFISCO II - BA, esta licitação obedecerá as disposições da Lei nº 14.634, de 28 de novembro de 2023, da Lei Complementar nº 123, de 14 de dezembro de 2006, das normas gerais da Lei nº 14.133, de 1º de abril de 2021, e respectivas alterações.

2. Requisito de participação:

2.1 Inscrição no Cadastro de Fornecedores do Estado da Bahia /SAEB

Serão admitidos a participar desta licitação os interessados, **inscritos ou não** no Cadastro de Fornecedores do Estado da Bahia, que atenderem a todas as exigências contidas no instrumento convocatório, e que pertençam ao ramo de atividade pertinente ao objeto licitado, e que tenham realizado seu credenciamento como usuário junto ao Banco do Brasil, para a obtenção de chave de identificação ou senha individual.

Poderão participar deste pregão interessados oriundos de países elegíveis do Banco Interamericano de Desenvolvimento (BID).

2.2 Tratamento diferenciado e simplificado (ME e EPP)

(x) Serviços – Sem reserva de cota

2.2.1 Na concessão do tratamento diferenciado e simplificado, deverá ser observado o disposto no art. 4º da Lei Federal nº 14.133/2021.

2.3 Consórcio

2.3.1 A definição quanto à participação de pessoas jurídicas reunidas em consórcio observará o disposto no Termo de Referência/Habilitação.

3. Processo administrativo - Órgão/entidade e setor:

013.1412.2025.0012189-58 Secretaria da Fazenda do Estado da Bahia/SEFAZ/SGF/DTI/GSINF

4. Modalidade/número de ordem:

(x) Pregão eletrônico nº 003/2025

4.1 Modo de disputa



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Aberto

4.2 Intervalo mínimo de diferença entre lances (degrau de valor ou percentual):

Sim (conforme orçamento estimado em planilha constante do TR/Habilitação)

5. Critério de julgamento:

Menor Preço

Global

6. Objeto da licitação/Codificação no Certificado de Registro – SAEB:

Família: 02.81

Código:02.81.13.00002129-6, 02.81.13.00002130-0,02.81.13.00002131-8, 02.81.13.00002132-6

7. Ordem de fases da licitação:

(X) Na presente licitação, a fase de habilitação **sucedera** as fases de apresentação de propostas e lances e de julgamento.

8. Agendamento da vistoria, quando exigível no TR:

Responsável pelo agendamento de vistoria:

A vistoria prévia deverá ser previamente agendada com a Diretoria de Tecnologia da Informação (DTI) da SEFAZ - BA pelo telefone (071) 3115-2429 e através do e-mail seginfo@sefaz.ba.gov.br.

9. Meio de acesso à íntegra do edital e anexos:

9.1 Portal Nacional de Contratações Públicas (PNCP), portal *Comprasnet.BA* e <https://licitacoes-e2.bb.com.br/aop-inter-estatico/>.

10. Local, dia e hora para recebimento das propostas e documentos e início da sessão pública da licitação:

Site: <https://licitacoes-e2.bb.com.br/aop-inter-estatico/>

Recebimento das propostas: das 08:00 horas do dia 06/05/2025, às 13:45 horas do dia 08/05/2025

Início da sessão pública: às 14:00 horas do dia 08/05/2025

11. Impugnação e pedido de esclarecimento:

11.1 A impugnação e o pedido de esclarecimento serão realizados por petição junto ao Sistema Eletrônico de Informação – SEI, ou por mensagem no correio eletrônico (e-mail:) copel@sefaz.ba.gov.br.

12. Disponibilização de vista dos autos:

12.1 O licitante deverá solicitar o acesso aos autos, o qual será concedido por meio de envio de *link* para o correio eletrônico (e-mail).

13. Controle prévio de legalidade ou dispensa de análise jurídica individualizada

Declaro que a análise jurídica individualizada do processo licitatório está dispensada, nos termos do art. 19, §1º, da Lei nº 14.634/2023, conforme autorização constante do ato abaixo, tendo sido



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

integralmente obedecida a **orientação jurídica referencial formalmente qualificada**, a seguir indicada:

Portaria PGE nº: 36/2024 Art.:1º,§1º

Despacho de Qualificação nº PA-076-2024 : () efeito sistêmico (x) efeito uniforme

14. Responsável pela consolidação das informações, componentes e anexos na minuta de edital, e meio de contato:

Servidor responsável e portaria de designação:

Endereço: Av. Luiz Viana Filho, 2ª Avenida nº 260, Plataforma II, 3º Andar, Paralela. Cep- 41.745-003, Salvador Bahia – Brasil. Centro Administrativo da Bahia - SEFAZ

Horário: 0900 às 12 14:00 às 17:00 Tel.: 3115.2621 – 3115-2450 - *E-mail:* copel@sefaz.ba.gov.br

Salvador- Ba. 16 de Abril de 2025

Alda dos Santos Costa



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

II. PARTE FIXA

(x) GERAL

1. RITO PROCEDIMENTAL

1.1 O rito procedimental da presente licitação seguirá o disposto nesta Parte Fixa, relativamente à operacionalização das fases do procedimento da licitação pelo critério de julgamento por menor preço ou maior desconto, na forma eletrônica.

1.1.1 Para fins deste Edital, considera-se responsável pela licitação o agente de contratação ou comissão de contratação a quem compete a condução do procedimento licitatório.

1.1.2 No caso de pregão, o agente de contratação será designado pregoeiro.

1.2 Na presente licitação será observado o que se segue:

- a) os documentos serão produzidos por escrito, com data e local de sua realização e assinatura dos responsáveis;
- b) os valores, os preços e os custos utilizados terão como expressão monetária a moeda corrente nacional; e
- c) o desatendimento de exigências meramente formais que não comprometam a aferição da qualificação do licitante ou a compreensão do conteúdo de sua proposta não importará seu afastamento da licitação ou a invalidação do processo;
- d) será disponibilizado o acesso aos documentos que compõem a proposta e os documentos de habilitação apresentados no processo licitatório.

2. ORDEM DAS FASES DA LICITAÇÃO

2.1 A realização da licitação pelo critério do menor preço ou maior desconto observará as seguintes fases sucessivas:

- a) preparatória;
- b) divulgação do edital de licitação;
- c) apresentação de propostas e lances;
- d) julgamento;
- e) habilitação;
- f) recursal; e
- g) homologação.

2.2 Na hipótese de inversão de fases, desde que observados os requisitos do art. 17, §1º, da Lei Federal nº 14.133/2021, e que seja disponibilizada a funcionalidade no sistema eletrônico, a fase de habilitação antecederá as fases de apresentação de propostas e lances e de julgamento.

3. PARTICIPAÇÃO NA LICITAÇÃO

3.1 O site, dia e hora para recebimento das propostas e início da sessão pública estão indicados no Preâmbulo deste Edital.

3.1.1 Reputa-se credenciada a pessoa natural regularmente designada para representar a licitante no processo licitatório.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

3.1.2 Cada licitante poderá credenciar apenas um representante e cada representante somente poderá representar uma única licitante.

3.2 O licitante deverá credenciar-se previamente no sistema eletrônico utilizado no certame.

3.2.1 O credenciamento do usuário implica em sua responsabilidade legal e na presunção de capacidade técnica para realização das transações inerentes à licitação.

3.2.2 O credenciamento do usuário será pessoal e intransferível para acesso ao sistema, sendo o licitante responsável por todos os atos praticados.

3.3 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.4 Não poderão disputar esta licitação:

- a) aquele que não atenda às condições deste Edital e seu(s) anexo(s);
- b) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;
- c) empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre obra, serviços ou fornecimento de bens a ela necessários;
- d) pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;
- e) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;
- f) empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;
- g) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação deste edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;
- h) agente público do órgão ou entidade licitante;
- i) Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

3.4.1 Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme §1º do art. 9º da Lei Federal nº 14.133/2021.

3.5 O impedimento relativo a pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta, será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.6 A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem as alíneas "b" e "c" do subitem 3.4 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

3.7 Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.8 O disposto nas alíneas "b" e "c" do subitem 3.4 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

3.9 Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei Federal nº 14.133/2021.

3.10 As vedações de que tratam a alínea h do subitem 3.4 e o subitem 3.4.1 se estendem a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica, conforme o §2º do art. 9º da Lei Federal nº 14.133/2021.

4. DO CADASTRAMENTO DA PROPOSTA INICIAL

4.1. Os licitantes cadastrarão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado, até a data e o horário estabelecidos para abertura da sessão pública no Preâmbulo do Edital.

4.2 Na hipótese de inversão de fases, os licitantes encaminharão os documentos de habilitação simultaneamente com o cadastramento da proposta, na forma e no prazo estabelecidos no subitem 4.1.

4.3 No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema eletrônico:

- a) a inexistência de fato impeditivo para licitar ou contratar com a Administração Pública;
- b) o pleno conhecimento e aceitação das regras e das condições gerais da contratação, constantes deste Edital;
- c) a responsabilidade pelas transações que forem efetuadas no sistema eletrônico, assumindo-as como firmes e verdadeiras;
- d) o cumprimento do disposto no inc. VI do art. 68 da Lei Federal nº 14.133/2021;
- e) o cumprimento dos requisitos para habilitação e a conformidade de sua proposta com as exigências de deste Edital.

4.3.1 Ao cumprir o disposto nas alíneas "b" e "e" do subitem 4.3, o licitante automaticamente declara:

- a) a aceitação de todas as condições dos anexos deste Edital;
- b) que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo, nos termos do §1º do art. 63 da Lei Federal nº 14.133/2021;
- c) não possuir empregados executando trabalho degradante ou forçado, observando o disposto nos incs. III e IV do art. 1º e no inc. III do art. 5º da Constituição Federal;
- d) que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, nos termos do inc. IV do art. 63 da Lei Federal nº 14.133/2021.

4.3.2 Para os fins da alínea "b" do subitem 4.3, além das disposições constantes no Termo de Referência e na minuta do contrato, será também considerada condição geral da contratação, não possuir, a contratada, empregados executando trabalho degradante ou forçado, nos termos dos incs. III e IV do art. 1º e no inc. III do art. 5º da Constituição Federal.

4.4 O licitante enquadrado como microempresa ou empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 3º da Lei Complementar nº 123/2006, estando apto a usufruir do tratamento estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º da Lei Federal nº 14.133/2021.

4.5 A falsidade de qualquer declaração de que trata o item 4 sujeitará o licitante às sanções previstas neste Edital, na Lei Federal nº 14.133/2021 e as referidas na Lei nº 14.634/2023.

4.6 Os licitantes poderão retirar ou substituir a proposta e, quando for o caso, os documentos de habilitação, anteriormente inseridos no sistema, até a abertura da sessão pública.

4.7. Na hipótese de inversão de fases, os licitantes poderão retirar ou substituir os documentos de habilitação anteriormente inseridos no sistema eletrônico, até a abertura da sessão pública.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

4.8 Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante.

4.9 Desde que disponibilizada a funcionalidade no sistema eletrônico, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá as seguintes regras:

a) a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

b) os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata a alínea "a" deste subitem.

4.10 Desde que disponibilizada a funcionalidade no sistema eletrônico, o valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo licitante durante a fase de disputa, sendo vedado:

a) valor superior a lance já registrado pelo licitante no sistema, quando adotado o critério de julgamento por menor preço; e

b) percentual de desconto inferior a lance já registrado pelo licitante no sistema, quando adotado o critério de julgamento por maior desconto.

4.11 O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do subitem 4.9 possuirá caráter sigiloso para os demais licitantes e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4.12 Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

5. DO CONTEÚDO DA PROPOSTA

5.1 O licitante deverá elaborar a sua proposta em conformidade com o que dispõe o Termo de Referência.

5.2 Todas as especificações do objeto contidas na proposta vinculam o licitante.

5.3 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

5.4 Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

5.5 Com a apresentação da proposta, o proponente assume o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

5.5.1 Os licitantes devem respeitar os preços máximos fixados pela Administração ou por órgão oficial competente ou constantes de tabela de preços referenciais.

5.5.2 Caso o critério de julgamento seja o de maior desconto, o preço resultante da aplicação do desconto ofertado deverá respeitar os preços máximos fixados pela Administração ou por órgão oficial competente ou constantes da tabela de preços referenciais.

5.6 Somente será admitida a indicação da tributação relativa ao Simples Nacional pelos licitantes que explorem as atividades de serviço de vigilância, limpeza ou conservação, de forma exclusiva ou em conjunto com outras atividades que não tenham sido objeto de vedação à inclusão no Simples, conforme previsto no art. 17, §1º, c/c art. 18, §5º-C, inc. VI, da Lei Complementar nº 123/2006, devendo observar, ainda, no que respeita ao serviço de vigilância, o disposto na Lei Federal nº 14.967, de 9 de setembro de 2024.

5.7 Nas licitações destinadas à contratação de serviços com fornecimento de mão de obra em regime de dedicação exclusiva que não sejam de serviço de vigilância, limpeza ou conservação, o licitante incluído no Simples Nacional deverá formular proposta considerando a tributação comum aplicável aos serviços, sob pena de desclassificação.

5.7.1 Na hipótese do subitem 5.7, o licitante que venha a ser contratado estará sujeito à exclusão obrigatória do Simples Nacional a contar do mês seguinte ao da contratação, em face do disposto no art. 31, inc. II, da Lei Complementar nº 123/2006.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

5.7.2 O pedido da exclusão do Simples Nacional deverá ser feito no prazo previsto no art. 30, §1º, inc. II, da Lei Complementar nº 123/2006, devendo a contratada apresentar cópia do ofício encaminhado à Receita Federal do Brasil, com comprovante de recebimento, como condição para recebimento da primeira fatura da prestação dos serviços.

6. ABERTURA DA SESSÃO PÚBLICA E FORMULAÇÃO DE LANCES

Sessão pública

6.1 A abertura da licitação se dará automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados no Preâmbulo deste Edital.

Lances

6.2 Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico.

6.3 Poderá ser fixado intervalo mínimo de tempo a ser observado entre as ofertas de lances.

6.4 Ressalvada a hipótese de parametrização referida no subitem 4.9, é vedado ao licitante apresentar seus lances de forma sucessiva, padronizada, intermitente, simultânea ou em intervalos de poucos segundos entre eles, ou de outros mecanismos indicativos da utilização de software lançador "robô".

6.4.1 Se inobservada a vedação estabelecida neste subitem, o responsável pela licitação desclassificará a proposta e determinará a consequente abertura de processo administrativo para apuração do ilícito.

6.5 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas neste Edital.

6.6 O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior, conforme o caso, ao último por ele ofertado e registrado pelo sistema.

6.7 Quando for constatado o oferecimento de lances com variação insignificante, poderá ser aplicado intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta (degrau).

6.7.1. O degrau deverá ser aquele indicado no Termo de Referência.

6.8 Caso o sistema eletrônico disponibilize essa funcionalidade, o licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de 15 (quinze) segundos após o registro no sistema eletrônico, na hipótese de lance inconsistente ou inexequível.

6.9 Não serão aceitos 2 (dois) ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

6.10 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

6.11 Na hipótese de o sistema eletrônico se desconectar no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

6.12 Caso, durante a desconexão do sistema eletrônico para o responsável pela licitação, ocorra o encerramento da disputa, o responsável pela licitação dará prosseguimento aos atos do certame somente após decorridas 24 (vinte e quatro) horas da comunicação do fato aos participantes, no sítio eletrônico utilizado para divulgação deste Edital.

6.13 Caso não sejam apresentados lances, o julgamento será feito com a proposta inicial.

6.14 O procedimento seguirá de acordo com o modo de disputa adotado.

Modo de disputa "aberto"

6.15 No modo de disputa "aberto", os licitantes apresentarão lances públicos e sucessivos, com prorrogações.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

6.15.1 A etapa de lances da sessão pública terá duração de 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.

6.15.2 A prorrogação automática da etapa de lances de que trata o subitem 6.15.1 será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

6.15.3 Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública será encerrada automaticamente e o sistema ordenará e divulgará os lances, segundo a ordem crescente de valores ou decrescente de percentual de desconto, conforme o critério de julgamento adotado.

6.15.4 Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o responsável pela licitação poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.15.5 Após o reinício previsto no subitem 6.15.4, os licitantes serão convocados para apresentar lances intermediários.

Modo de disputa "aberto e fechado"

6.16 No modo de disputa "aberto e fechado" os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

6.16.1 A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até 10 (dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

6.16.2 Encerrado o prazo previsto no subitem 6.16.1, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo ou de maior percentual de desconto, conforme o critério de julgamento adotado, e os das ofertas com preços até 10% (dez por cento) superiores ou inferiores àquela possam ofertar um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

6.16.3 No procedimento de que trata o subitem 6.16.2, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

6.16.4 Não havendo pelo menos 3 (três) ofertas nas condições definidas neste subitem, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de 3 (três), oferecer um lance final e fechado em até 5 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

6.16.5 Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores ou decrescente de percentual de desconto, conforme o critério de julgamento adotado.

Modo de disputa "fechado e aberto"

6.17 No modo de disputa "fechado e aberto" somente serão classificados para a etapa da disputa aberta, com a apresentação de lances públicos e sucessivos, o licitante que apresentou a proposta de menor preço ou de maior percentual de desconto e os das propostas até 10% (dez por cento) superiores ou inferiores àquela, conforme o critério de julgamento adotado.

6.17.1 Não havendo pelo menos 3 (três) propostas nas condições definidas no subitem 6.17.0, poderão os licitantes que apresentaram as 3 (três) melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

6.17.2 A etapa de lances da sessão pública terá duração de 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.

6.17.3 A prorrogação automática da etapa de lances de que trata o subitem 6.17.2 será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

6.17.4 Não havendo novos lances na forma estabelecida nos subitens anteriores, a sessão pública será encerrada automaticamente, e o sistema ordenará e divulgará os lances, segundo a ordem crescente de valores ou decrescente de percentual de desconto, conforme o critério de julgamento adotado.

6.17.5 Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o responsável pela licitação poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.17.6 Após o reinício previsto no subitem 6.17.5, os licitantes serão convocados para apresentar lances intermediários, podendo optar por manter o seu último lance.

Empate ficto

6.18 Em relação aos itens de ampla participação, será observado o que se segue:

6.18.1 O sistema eletrônico identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de se aplicar o disposto nos arts. 44 e 45 da Lei Complementar nº 123/2006.

6.18.2 Nas condições do subitem 6.18.1, as propostas de microempresas e empresas de pequeno porte que se encontrarem no intervalo percentual de até 5% (cinco por cento), tratando-se de pregão eletrônico, ou de até 10% (dez por cento), tratando-se de concorrência eletrônica, relativamente à proposta mais bem classificada, serão consideradas empatadas com a primeira colocada (empate ficto).

6.18.3 A microempresa ou empresa de pequeno porte mais bem classificada, nos termos do subitem 6.18.2, terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ou em percentual de desconto superior ao da primeira colocada, conforme o critério de julgamento adotado, no prazo de 5 (cinco) minutos controlados pelo sistema eletrônico, contados da comunicação automática.

6.18.4 Caso a microempresa ou a empresa de pequeno porte mais bem classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais microempresas ou empresas de pequeno porte, em situação de empate ficto, na ordem de classificação, para o exercício do mesmo direito, no mesmo prazo.

6.18.5 No caso de equivalência dos valores ou dos percentuais de descontos apresentados pelas microempresas e empresas de pequeno porte, conforme o critério de julgamento adotado, que se encontrem nos intervalos percentuais estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

6.18.6 Se não ocorrer o desempate, prevalecerá a melhor oferta inicial.

Empate real

6.19 Ocorrendo empate real, será observado o procedimento a seguir definido.

6.19.1 Só poderá haver empate entre propostas iguais (não seguidas de lances) ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

6.19.2 Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei Federal nº 14.133/2021, nesta ordem:

- a) disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;
- b) avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei Federal nº 14.133/2021;
- c) desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme o art. 4º, §§1º a 3º do Decreto nº 22.665/2024;
- d) desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

6.19.2.1 A comprovação do desenvolvimento de ações de equidade e de programa de integridade a que se referem a alínea "c" e "d" deste subitem será feita de forma documental, mediante diligência do responsável pela licitação.

6.19.3 Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

- a) empresas estabelecidas no Estado da Bahia;
- b) empresas brasileiras;
- c) empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;
- d) empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187/2009.

6.19.4 Se, após observados os subitens 6.19.2 e 6.19.3, não houver desempate, será realizado sorteio entre os licitantes, vedando-se qualquer outro critério.

Sorteio em ato público

6.20 A realização de sorteio, nas hipóteses previstas neste Edital, será realizada em ato público, para o qual os licitantes serão convocados, e do qual será lavrada ata específica.

6.20.1 Não sendo possível, por razões de ordem operacional, a realização do sorteio por meio do sistema eletrônico, deverá ser designada a realização de ato público presencial, assegurado o acompanhamento e a manifestação por videoconferência ou outro meio idôneo.

6.20.1.1 Na hipótese do subitem 6.20.1, o responsável pela licitação deverá juntar aos autos do processo licitatório no Sistema Eletrônico de Informações – SEI a gravação da sessão pública em áudio e vídeo, nos termos dos §§2º e 5º do art. 17 da Lei Federal nº 14.133/2021.

6.20.1.2 O link da gravação, para fins de disponibilização aos interessados, constará de despacho do responsável pela licitação.

Chat para troca de mensagens

6.21 Ao final da disputa de lances, o sistema disponibilizará campo próprio para troca de mensagens entre o responsável pela licitação e os licitantes.

6.22 O responsável pela licitação concederá o prazo de 3 (três) horas para envio da proposta readequada ao último lance ofertado.

6.22.1 No caso de licitação em que o procedimento exija apresentação de planilhas com indicação dos quantitativos e dos custos unitários, estas deverão ser encaminhadas pelo sistema com os respectivos valores readequados à proposta provisoriamente classificada em primeiro lugar, sob pena de não aceitação da proposta.

6.22.2 Em se tratando de serviços de engenharia, o licitante mais bem classificado deverá apresentar, por meio eletrônico, conforme o critério de julgamento adotado, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo que integra o Termo de Referência, bem como com o detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores readequados ao valor final da proposta provisoriamente classificada em primeiro lugar, na forma disciplinada no Termo de Referência.

6.22.3 O prazo definido no subitem 6.22 poderá ser prorrogado por solicitação fundamentada feita no "chat" pelo licitante, antes de sua conclusão.

6.22.4 Em casos justificados, constada a complexidade da proposta, o responsável pela licitação poderá fixar prazo diverso do definido no subitem 6.22, desde que não superior a 01 (um) dia útil.

6.23 Quando o licitante mais bem classificado se tratar de microempresa ou empresa de pequeno porte, deverá, para fins de obtenção de benefícios da Lei Complementar nº 123/2006, encaminhar, em conjunto com a proposta readequada, declaração de não ter celebrado contratos com a Administração Pública cujos valores somados excedam a receita bruta máxima admitida para fins de enquadramento como microempresa e empresa de



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

pequeno porte, nos termos do §2º do art. 4º da Lei Federal nº 14.133/2021, preferencialmente conforme modelo anexo a este Edital.

7. DA VERIFICAÇÃO DE VEDAÇÕES À PARTICIPAÇÃO

7.1 O responsável pela licitação verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei Federal nº 14.133/2021, legislação correlata e no item 3 da Parte Fixa deste Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

- a) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>);
- b) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>); e
- c) Cadastro de Fornecedores do Estado da Bahia - CAF, mantido pelo Órgão Central do Sistema de Registro Cadastral do Poder Executivo do Estado da Bahia.

7.2 A consulta aos cadastros poderá ser estendida aos administradores e sócios com poderes de administração da licitante, na hipótese de desconsideração da personalidade jurídica a que alude o art. 57 da Lei nº 14.634/2023.

7.3 Constatada a existência de sanção condenatória restritiva de direito transitada em julgado, nos termos dos arts. 43 e 44 do Decreto nº 23.113/2024, o licitante será excluído da licitação, hipótese em que o responsável pela licitação avaliará a proposta subsequente, procedendo na forma do item 6 e seus subitens.

7.3.1. A sanção de impedimento de licitar e contratar impedirá o infrator de licitar ou contratar no âmbito da Administração Pública direta e indireta do Estado da Bahia.

7.3.2 A sanção de declaração de inidoneidade para licitar e contratar impedirá o infrator de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos.

7.4 Se o licitante mais bem classificado for excluído do certame, o responsável pela licitação avaliará a proposta subsequente, de acordo com a disciplina estabelecida no item 6 e neste item 7, e assim sucessivamente, até a obtenção de proposta válida.

8. FASE DE JULGAMENTO

8.1 O responsável pela licitação examinará a proposta do licitante mais bem classificado quanto à compatibilidade do preço ou do desconto e quanto ao atendimento das especificações do objeto.

Compatibilidade do preço

8.2 O responsável pela licitação aferirá a compatibilidade da proposta em relação ao máximo estipulado para contratação e quanto à sua exequibilidade.

8.2.1 Na hipótese de o preço do licitante mais bem classificado superar o limite máximo definido pela Administração, o responsável pela licitação poderá negociar a adequação da proposta, a fim de evitar a desclassificação.

8.2.1.1 Quando a proposta do primeiro colocado, mesmo após a negociação, for desclassificada em razão de permanecer acima do preço máximo definido pela Administração, deverá ser oportunizada aos demais licitantes a possibilidade de negociação, segundo a ordem de classificação inicialmente estabelecida.

8.2.1.2 O procedimento de negociação observará o disposto no item 9.

8.2.2 No caso de bens e serviços em geral, além das disposições eventualmente constantes do Termo de Referência, será considerada como indício de inexecuibilidade a apresentação de proposta com valor inferior a 50% (cinquenta por cento) daquele orçado pela Administração, constante da estimativa do valor da contratação.

8.2.3 No caso de obras e serviços de engenharia e arquitetura, além das disposições eventualmente constantes do Termo de Referência, a análise de exequibilidade e sobrepreço considerará o que segue:



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

a) para efeito de avaliação da exequibilidade e de sobrepreço, serão considerados o preço global, os quantitativos e os preços unitários tidos como relevantes, observado o critério de aceitabilidade de preços unitário e global definidos no Termo de Referência, conforme as especificidades do mercado correspondente (art. 59, §3º, da Lei Federal nº 14.133/2021).

b) serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução (art. 59, §4º, da Lei Federal nº 14.133/2021).

c) será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei Federal nº 14.133/2021 (art. 59, §5º).

8.2.4 Se houver indício de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos, caberá a realização de diligência, a fim de oportunizar ao licitante a comprovação da exequibilidade da proposta.

8.2.4.1. Não poderá ser considerada exequível a proposta quando os custos do licitante ultrapassem o valor da proposta ou não forem demonstrados custos de oportunidade capazes de justificar a oferta.

Aferição do atendimento às especificações do objeto

8.3 O responsável pela licitação procederá à análise da proposta do licitante mais bem classificado quanto ao atendimento das especificações do objeto, sendo-lhe facultado colher manifestação escrita do setor requisitante do objeto licitado ou da área especializada.

8.4 Caso previsto no Termo de Referência, a análise a que se refere o subitem 8.3 será realizada em procedimento de exame de adequação do objeto, relativamente ao licitante mais bem classificado, compreendendo a apresentação de amostras, avaliação de conformidade, prova de conceito, ou outros testes destinados à aferição da aceitabilidade da proposta, nos seguintes termos:

8.4.1 Será divulgado o local e horário de realização do procedimento de exame de adequação do objeto, cuja participação será franqueada a todos os interessados.

8.4.2 A divulgação será feita por mensagem no sistema eletrônico, no sítio eletrônico oficial ou por outro meio idôneo, com a antecedência necessária para a sua realização.

8.4.3 Não sendo possível, por razões de ordem operacional, a permissão à participação presencial dos interessados na realização do exame de adequação do objeto, deverá ser assegurado o acompanhamento e a manifestação no ato, por videoconferência ou outro meio idôneo.

8.4.4 A recusa do licitante à realização do exame de adequação do objeto ou atraso, sem justificativa aceita pelo responsável pela licitação, de entrega da amostra, realização do exame de conformidade, de prova de conceito ou de outros testes exigidos será considerada desistência do certame, ensejando a aplicação das penalidades pertinentes.

8.4.5 O objeto será considerado inadequado, quando verificado o não atendimento das especificações previstas neste Edital.

8.4.6 Os resultados das avaliações serão divulgados pelos meios previstos no subitem 8.4.2.

Documentos complementares à proposta

8.5 Caso seja necessário, o responsável pela licitação poderá, em sede de diligência, solicitar documentos complementares à proposta, a fim de esclarecer ou confirmar situação fática ou jurídica pré-existente (art. 36 do Decreto nº 22.888/2024).

8.5.1 Na realização de diligência, o responsável pela licitação deverá atentar para o caráter de complementaridade das informações e documentos a serem juntados (art. 36, parágrafo único, do Decreto nº 22.888/2024).

8.5.2 Não serão aceitos documentos ou informações que devessem constar originariamente da proposta.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

8.5.3 O não envio dos documentos complementares no prazo indicado pelo responsável pela licitação será considerada desistência, implicando na desclassificação do licitante e à sujeição às sanções administrativas pertinentes.

Sanatória da proposta

8.6 O responsável pela licitação poderá sanar erros ou falhas que não alterem a substância da proposta, mediante despacho fundamentado registrado e acessível a todos, atribuindo-lhes eficácia para fins de classificação (art. 37 do Decreto nº 22.888/2024).

Desclassificação da proposta

8.7 Será desclassificada a proposta que:

- a) contiver vícios insanáveis;
- b) não obedecer às especificações técnicas contidas no Termo de Referência;
- c) apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;
- d) não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;
- e) apresentar desconformidade com quaisquer outras exigências deste Edital e/ou seus anexos, desde que insanável.

8.8 No caso de desclassificação, o responsável pela licitação avaliará a proposta subsequente, de acordo com a disciplina estabelecida nos itens 6 a 8, procedendo a nova verificação da ocorrência do empate ficto, se for o caso, de acordo com a disciplina estabelecida, e assim sucessivamente, até a obtenção de proposta válida

Do Encerramento da Fase de Julgamento

8.9 Não sendo possível o julgamento da proposta na mesma sessão, o responsável pela licitação deverá designar nova sessão, para a qual serão convocados os licitantes.

8.10 A fase de julgamento será encerrada com a identificação do licitante classificado detentor da melhor proposta.

9. DA NEGOCIAÇÃO

9.1. Definido o resultado do julgamento, o responsável pela licitação poderá negociar condições mais vantajosas com o licitante classificado detentor da melhor proposta.

9.1 A negociação será conduzida pelo responsável pela licitação por meio do sistema eletrônico, podendo ser acompanhada pelos demais licitantes.

9.2 O resultado da negociação será registrado na ata da sessão pública, divulgado a todos os licitantes e anexado aos autos do processo licitatório.

9.3 Concluída a negociação, o responsável pela licitação solicitará o envio da proposta readequada, observado o disposto no subitem 6.22.

10. FASE DE HABILITAÇÃO

Documentos de habilitação

10.1 Para habilitação dos licitantes, serão exigidos os documentos necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, nos termos dos arts. 62 a 70 da Lei Federal nº 14.133/2021, conforme definido no Termo de Referência, dividindo-se em: jurídica; técnica; fiscal, social e trabalhista; e econômico-financeira.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

10.1.1 A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira poderá ser substituída pelo Certificado de Registro Cadastral do Cadastro de Fornecedores do Estado da Bahia (CAF) quanto aos documentos por ele abrangidos, observado o disposto neste Edital.

10.1.2 Os documentos exigidos para fins de habilitação observarão os termos da Lei Federal nº 13.726, de 8 de outubro de 2018.

10.1.3 Na forma do art. 63, inc. I, da Lei Federal nº 14.133/2021, o licitante responderá pela veracidade das declarações a que se refere o subitem 4.3.

10.1.4 Somente haverá a necessidade de apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

Microempresas e empresas de pequeno porte

10.2 A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte observará o disposto no art. 43 da Lei Complementar nº 123/2006.

10.2.1 O responsável pela licitação procederá à verificação se a microempresa ou empresa de pequeno porte faz jus aos benefícios da Lei Complementar nº 123/2006, em conformidade com os termos definidos neste Edital.

Empresas estrangeiras

10.3 Quando permitida a participação de empresas estrangeiras que não funcionem no País, será observado o que segue:

10.3.1 As exigências de habilitação serão atendidas mediante documentos equivalentes inicialmente apresentados com tradução livre;

10.3.2 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 demais documentos de habilitação;

10.3.3 Para fins de assinatura do contrato ou da ata de registro de preços, os documentos de que trata este artigo serão traduzidos por tradutor juramentado no país e apostilados ou consularizados pelos respectivos consulados ou embaixadas.

Consórcio de empresas

10.4 Salvo vedação devidamente justificada no Termo de Referência, pessoa jurídica poderá participar de licitação em consórcio, observado o disposto no art. 15 e nos §§ 10 e 11 do art. 67, todos da Lei Federal nº 14.133/2021.

10.4.1 Quando houver a participação de consórcio de empresas, a habilitação técnica, se exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.

Processamento da habilitação

10.5 Serão exigidos os documentos de habilitação apenas do licitante classificado detentor da melhor proposta, exceto na inversão de fases (art. 63, inc. II, da Lei Federal nº 14.133/2021).

10.5.1 Quando houver inversão de fases, a exigência dos documentos de habilitação ocorrerá em relação a todos os licitantes.

10.5.2 Excetuam-se da previsão deste subitem os documentos relativos à regularidade fiscal, os quais serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas e somente do licitante classificado detentor da melhor proposta (art. 63, inc. III, da Lei Federal nº 14.133/2021).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

10.6 Os documentos de habilitação serão enviados por meio do sistema eletrônico, em formato digital, no prazo 3 (três) horas, prorrogável por igual período, contado da solicitação do responsável pela licitação (art. 63, inc. II, da Lei Federal nº 14.133, de 2021).

10.6.1 Na hipótese de inversão de fases, os licitantes encaminharão simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto.

10.6.2 Em caso de falhas técnicas ou operacionais que inviabilizem o envio de documentação de que trata este subitem 10.6, será admitido o envio correspondente para o correio eletrônico (e-mail) indicado no Preâmbulo deste Edital, devendo o responsável pela licitação informar no "chat" do sistema eletrônico a data e o horário do seu recebimento, disponibilizando o seu conteúdo, em seguida, para os demais licitantes.

10.7 A habilitação poderá ser verificada por meio do CAF, quanto aos documentos por ele abrangidos, exceto quanto aos documentos de qualificação técnica.

10.7.1 Os documentos exigidos para habilitação que não estejam contemplados no CAF, ou que dele constem como vencidos, ou que não possam ser substituídos pelo certificado, deverão ser apresentados pelo licitante, na forma prevista neste Edital.

10.7.2 Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora.

10.8 Nas licitações restritas a fornecedores cadastrados, a habilitação será verificada por meio do CAF, observado o disposto no subitem 10.6 (art. 87, §§3º e 4º da Lei Federal nº 14.133/2021).

10.9 É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no CAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo solicitar a modificação dos registros em caso de incorreção.

10.10 A verificação, pelo responsável pela licitação, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões, constitui meio legal de prova, para fins de habilitação.

Documentos complementares à habilitação

10.11 Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (art. 64 da Lei Federal nº 14.133/2021):

a) complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

b) atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

10.11.1 Os documentos serão enviados por meio do sistema eletrônico, em formato digital, no prazo 3 (três) horas, prorrogável por igual período, contado da solicitação do responsável pela licitação, observado o disposto no subitem 10.5.

10.11.2 O não envio dos documentos complementares no prazo indicado será considerada desistência, implicando na inabilitação do licitante e à sujeição às sanções administrativas pertinentes.

Sanatória

10.12 Na análise dos documentos de habilitação, o responsável pela licitação poderá sanar erros ou falhas que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação (art. 64, §1º da Lei Federal 14.133/2021).

10.12.1 Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

Da comprovação dos requisitos de habilitação diferidos



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

10.13 O responsável pela licitação definirá o prazo para a apresentação dos requisitos de habilitação cuja exigência tenha sido diferida.

10.13.1 A não apresentação da documentação no prazo definido, implicará inabilitação do licitante e sujeição às sanções administrativas pertinentes.

10.14 Tratando-se de microempresa ou empresa de pequeno porte, beneficiária do regime diferenciado da Lei Complementar nº 123/06, cuja participação tenha sido realizada com a ressalva de existência de restrição fiscal e/ou trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada a vencedora do certame, prorrogável por igual período, a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa

10.14.1 A não-regularização da documentação no prazo previsto neste item implicará decadência do direito à contratação e inabilitação do licitante, além da sujeição às sanções administrativas pertinentes, na forma do disposto no §2º do art. 53 da Lei Complementar nº 123/06.

Inabilitação

10.15 Na hipótese de o licitante não atender às exigências de habilitação, o responsável pela licitação examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda aos requisitos e especificações, procedendo, inclusive, a nova verificação da ocorrência do empate ficto, na forma prevista neste Edital.

Do encerramento da fase de Habilitação

10.16 Não sendo possível o julgamento da habilitação na mesma sessão, o responsável pela licitação deverá designar nova sessão, observado o prazo mínimo de 24h (vinte e quatro horas), para a declaração do licitante provisoriamente vencedor, para a qual ficarão convocados os licitantes.

10.17 Exceto na inversão de fases, encerrada a fase de habilitação, será declarado o licitante provisoriamente vencedor, ato do qual ficarão automaticamente intimados os licitantes.

11. IMPUGNAÇÃO AO EDITAL E PEDIDO DE ESCLARECIMENTO

11.1 Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade ou para solicitar esclarecimentos sobre os seus termos, devendo encaminhar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

11.1.1 A impugnação e o pedido de esclarecimento serão realizados na forma eletrônica.

11.2 O responsável pela licitação responderá aos pedidos de esclarecimentos e impugnação no prazo de até 03 (três) dias úteis contado da data de recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame, e poderá requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos seus anexos.

11.2.1 O responsável pela licitação poderá solicitar a manifestação dos setores técnicos do órgão ou entidade contratante, a fim de subsidiar as decisões de caráter técnico, conforme o §3º do art. 8º do Decreto nº 22.885/2024 e a oitiva, quando necessário, dos órgãos de assessoramento jurídico e de controle interno, nos termos do art. 32 do Decreto nº 22.885/2024.

11.3 A impugnação não possui efeito suspensivo, sendo a sua concessão medida excepcional que deverá ser motivada pelo responsável pela licitação nos autos do processo de licitação.

11.4 Acolhida a impugnação contra o edital de licitação, será definida e publicada nova data para realização do certame, devendo ser observado o disposto no subitem 17.12

11.5 A resposta à impugnação ou ao pedido de esclarecimento será divulgada no endereço eletrônico www.comprasnet.ba.gov.br e no <https://licitacoes-e2.bb.com.br/aop-inter-estatico/>, no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame, e vincularão os participantes e a Administração.

12. FASE RECURSAL



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

12.1 A fase recursal obedecerá à disciplina estabelecida neste Edital, observado o disposto no art. 165 da Lei Federal nº 14.133/2021.

12.2 Dos atos decorrentes do procedimento licitatório, cabem:

12.2.1 Recurso:

- a) em fase única, em face do julgamento das propostas e do ato de habilitação ou inabilitação;
- b) em face do ato de anulação ou revogação da licitação.

12.2.2 Pedido de reconsideração, relativamente a ato do qual não caiba recurso hierárquico.

12.3 O recurso em face do julgamento das propostas e do ato de habilitação ou inabilitação observará as seguintes disposições:

12.3.1 A intenção de recorrer deverá ser manifestada imediatamente, no prazo de 15 (quinze) minutos, sob pena de preclusão, após a declaração do licitante provisoriamente vencedor pelo responsável pela licitação.

12.3.1.1 A manifestação da intenção de recorrer será única, abrangendo as matérias concernentes ao julgamento das propostas e ao ato de habilitação ou inabilitação.

12.3.2 Manifestada a intenção de recorrer, as razões de recurso deverão ser apresentadas no prazo de 3 (três) dias úteis, contado da data de intimação da declaração do licitante provisoriamente vencedor.

12.3.3 O prazo para apresentação de contrarrazões será de 3 (três) dias úteis, contado da data de divulgação da interposição do recurso, a qual será feita por comunicação no chat.

12.3.4 O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, para juízo de retratação.

12.3.4.1 Se a autoridade não reconsiderar o ato ou a decisão no prazo de 3 (três) dias úteis, encaminhará o recurso com a sua motivação à autoridade superior.

12.3.5 A autoridade superior deverá proferir sua decisão no prazo máximo de 10 (dez) dias úteis, contado do recebimento dos autos.

12.3.6 O acolhimento do recurso implicará invalidação apenas de ato insuscetível de aproveitamento.

12.3.7 Os recursos interpostos fora do prazo não serão conhecidos.

12.3.8 O resultado dos recursos será divulgado no endereço eletrônico www.comprasnet.ba.gov.br.

12.4 Aplica-se o disposto no subitem 12.3, no que couber, ao recurso em face do ato de anulação ou revogação da licitação.

12.5 O pedido de reconsideração será apresentado no prazo de 3 (três) dias úteis, contado da data de intimação, observado o inc. II do art. 165 da Lei Federal nº 14.133/2021.

12.6 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

12.6.1 Na elaboração de suas decisões, a autoridade competente será auxiliada pelo órgão de assessoramento jurídico, que deverá dirimir dúvidas e subsidiá-la com as informações necessárias.

12.7 Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

13. ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1 Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior, que poderá:

- a) determinar o retorno dos autos para saneamento de irregularidades;
- b) revogar a licitação por motivo de conveniência e oportunidade;
- c) proceder à anulação da licitação, de ofício ou mediante provocação de terceiros, sempre que presente ilegalidade insanável;
- d) adjudicar o objeto e homologar a licitação.

13.1.1 Ao pronunciar a nulidade, a autoridade indicará expressamente os atos com vícios insanáveis, tornando sem efeito todos os subsequentes que deles dependam, e dará ensejo à apuração de responsabilidade de quem lhes tenha dado causa.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

13.1.2 O motivo determinante para a revogação do processo licitatório deverá ser resultante de fato superveniente devidamente comprovado.

13.1.3 Nos casos de anulação e revogação, deverá ser assegurada a prévia manifestação dos interessados.

13.1.5 Havendo justo receio de prejuízo de difícil ou incerta reparação decorrente do ato de anulação e revogação, poderá ser diferida a manifestação dos interessados, com fundamento no art. 183 da Lei nº 12.209, de 20 de abril de 2011, justificadamente.

13.2 A homologação da licitação não implicará direito à contratação.

14. CONVOCAÇÃO PARA ASSINATURA DO CONTRATO

14.1 Após a homologação, o licitante vencedor será convocado para assinar o termo de contrato, ou aceitar ou retirar o instrumento equivalente, no prazo estabelecido neste Edital, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas na Lei Federal nº 14.133/2021, e em outras legislações aplicáveis.

14.1 O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do adjudicatário durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

14.2. Será facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou não retirar o instrumento equivalente no prazo e nas condições estabelecidas, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.

14.3 Decorrido o prazo de validade da proposta indicado neste Edital sem convocação para a contratação, ficarão os licitantes liberados dos compromissos assumidos.

14.4 Na hipótese de nenhum dos licitantes aceitar a contratação nos termos do subitem 14.2 a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

- a) convocar os licitantes remanescentes para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário;
- b) adjudicar e celebrar o contrato nas condições ofertadas pelos licitantes remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

14.5. A negociação a que se refere a alínea "a" do subitem 14.4 deste artigo deverá ser oportunizada aos licitantes remanescentes, assegurada a preferência, em caso de empate, ao licitante mais bem classificado.

14.6 A recusa injustificada do adjudicatário em assinar o contrato ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão ou entidade promotor da licitação.

14.7 Equipara-se à recusa prevista no subitem 14.6 a circunstância de o adjudicatário deixar de manter as condições de habilitação exigidas na licitação, ou, por qualquer meio, dar causa à impossibilidade de celebrar o contrato.

14.8 A regra do subitem 14.6 não se aplicará aos licitantes remanescentes convocados na forma da alínea "a" do subitem 14.4, desde que não tenham passado à condição de licitante adjudicatário (art. 48, §8º do Decreto nº 22.888/2024).

14.9 Na hipótese de substituição do termo de contrato por instrumento equivalente, neste serão consideradas literalmente transcritas todas as cláusulas e condições previstas na minuta de contrato constante deste Edital.

15. INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

15.1 Constituem infrações administrativas para os fins deste Edital as condutas constantes do art. 155 da Lei Federal nº 14.133/2021 (art. 47 da Lei nº 14.634/2023).

15.2 Os licitantes estarão sujeitos às sanções administrativas referidas na Lei nº 14.634/2023, e às demais cominações legais, resguardado o direito à ampla defesa e ao contraditório.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

16. DISPOSIÇÕES ESPECÍFICAS DO SISTEMA DE REGISTRO DE PREÇOS

16.1 Tratando-se de licitação destinada ao Sistema de Registro de Preços, aplica-se o disposto nesta Parte Fixa (Geral) com os acréscimos da **Seção Específica do Sistema do Registro de Preços (SESRP)**.

17. DISPOSIÇÕES FINAIS

17.1 A ata da sessão pública será divulgada no sistema eletrônico.

17.2 Os horários estabelecidos neste Edital, no aviso da licitação e durante a sessão pública observarão o horário de Brasília, Distrito Federal, inclusive para contagem de tempo e prática de atos processuais.

17.3 As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, os princípios elencados no art. 5º da Lei Federal nº 14.133/2021, a finalidade e a segurança da contratação.

17.4 Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será responsável por quaisquer custos, independentemente da condução ou do resultado do processo licitatório.

17.5 Na contagem dos prazos estabelecidos neste Edital observar-se-á o art. 183 da Lei Federal nº 14.133/2021.

17.6 Os atos de comunicação processual da Administração com os licitantes serão realizados por meio eletrônico, na forma do disposto na Lei nº 12.209, de 20 de abril de 2011, e do Decreto nº 15.805, de 30 de dezembro de 2014.

17.6.1. A Contratada deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais, conforme Decreto nº 17.983, de 24 de outubro de 2017, devendo atender às convocações da Administração para a prática de atos nos prazos indicados.

17.7 A autoridade competente poderá, até a assinatura do contrato, excluir licitante, em despacho motivado, se tiver ciência de fato ou circunstância, anterior ou posterior ao julgamento da licitação, que revele inidoneidade ou falta de capacidade técnica ou financeira para a execução do contrato, assegurada a manifestação do interessado (art. 66 da Lei nº 14.634/2023).

17.8 Eventuais modificações neste Edital implicarão nova divulgação na mesma forma de sua divulgação inicial, além do cumprimento dos mesmos prazos dos atos e procedimentos originais, exceto se, inquestionavelmente, a alteração não comprometer a formulação das propostas, resguardado o tratamento isonômico aos licitantes.

17.9 Os casos omissos serão dirimidos pelo Órgão/Entidade indicados no Preâmbulo deste Edital, segundo as disposições contidas na Lei Federal nº 14.133/2021, na Lei nº 14.634/2023, e demais normas aplicáveis.

18. FORO

18.1 As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para solucionar quaisquer dúvidas oriundas deste instrumento que não puderem ser dirimidas por quaisquer dos meios alternativos de resolução de controvérsias de que trata a Lei Federal nº 14.133/2021.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

III. TERMO DE REFERÊNCIA /HABILITAÇÃO
SERVIÇOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA

(X) LICITAÇÃO

(Processo Administrativo nº 013.1412.2025.0012189-58)

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1 Objeto: O objeto desta contratação é um Centro de Operações de Segurança (SOC), serviços gerenciados de segurança e soluções de TI associados.

1.1.1 As especificações do objeto obedecerão as condições e exigências estabelecidas neste Termo de Referência, observado o disposto na tabela abaixo.

Participação [ampla/exclusiva]	Lote/Item	Código SIMPAS	Descrição	Unidade de Fornecimento (UF)	Quantitativo	Cronograma/Prazo
Ampla	1/1	02.81.13.00021326	SERVICOS GERENCIADOS DE SEGURANCA DA INFORMACAO, Estruturacao e implantacao de uma Central de Operacoes de Seguranca (Security Operations Center – SOC)	UN	1	Implantação 3 meses
Ampla	1/2	02.81.13.00021296	SERVICOS GERENCIADOS DE SEGURANCA DA INFORMACAO, Operacao de uma Central de Operacoes de Seguranca (Security Operations Center – SOC)	UN	21	21 meses
Ampla	1/3	02.81.13.00021300	LICENCA DE USO DE SOFTWARE Software de Gerenciamento de eventos e informações de segurança (SIEM)	UN	1	24 meses
Ampla	1/4	02.81.13.00021318	LICENCA DE USO DE SOFTWARE Software de Gestao de Vulnerabilidades	UN	1	24 meses

1.1.2 As especificações do objeto constam do anexo integrante deste Termo de Referência.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

1.1.2.1 Na contratação de que trata este Termo de Referência, a contratada deverá realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do Contratante ou da nova empresa que continuará a execução dos serviços.

1.2 O prazo de vigência do Contrato é de 27 (vinte e sete) meses (máximo de 5 anos), a **contar da data (X) da assinatura do Contrato () da subscrição da Autorização de Prestação de Serviços – APS**, prorrogável até atingir o limite de 10 anos, na forma dos artigos 106 e 107 da Lei Federal nº 14.133, de 2021.

1.3 O Contrato apresenta maior detalhamento das regras que serão aplicadas ao prazo de vigência.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1 A fundamentação da contratação, da caracterização do objeto e de seus quantitativos está especificada:

(X) em tópico próprio do Estudo Técnico Preliminar

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

3.1 A descrição da solução como um todo está especificada:

(X) em tópico próprio do Estudo Técnico Preliminar

4. REQUISITOS DA CONTRATAÇÃO

4.1 Sustentabilidade:

4.1.1 Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto e no Estudo Técnico Preliminar, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis

- a) Só será admitida a oferta que cumpra os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 170, de 2012 do INMETRO. Só será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (V1)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs);
- b) O conceito de TI verde é definido como um conjunto de práticas que torna mais sustentável e menos prejudicial o uso da tecnologia e está ligado aos processos de fabricação dos componentes, a administração e a utilização dos ativos de TI, bem como o descarte do "lixo eletrônico". Dentro desse contexto, poderá ser priorizada a utilização de tecnologias de virtualização, as quais podem ser definidas como soluções computacionais que permitem a execução de vários sistemas operacionais e seus respectivos softwares a partir de uma única máquina física. Como benefícios da virtualização podem ser citados o melhor aproveitamento da infraestrutura existente, a redução no consumo de energia elétrica, diminuição na geração de lixo eletrônico e menor emissão de carbono.
- c) Outro critério a ser priorizado nas especificações é a adoção de um plano de descarte ou reuso dos ativos de TI a serem contratados, haja vista que na sua fabricação são usadas substâncias que lhes conferem durabilidade, desempenho e



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

proteção, contudo, quando chegam ao final do seu ciclo de vida esses elementos, tais como mercúrio, chumbo, fósforo e cádmio, podem representar riscos à saúde da natureza e do homem se não forem descartados adequadamente. Também poderá ser priorizada a adoção de processos administrativos na sua forma eletrônica, utilizando softwares aplicativos.

- d) Os documentos deverão ser gerados e mantidos em sua forma digital e, com o objetivo de garantir a integridade dos mesmos, nestes poderão ser utilizados recursos tecnológicos de segurança da informação. O objetivo da referida adoção é reduzir o número de cópias e impressões em papel. Portanto, recomenda-se inserir critérios de sustentabilidade ambiental nas especificações técnicas para aquisição de ativos de TI, os quais deverão atender aos requisitos técnicos que propiciam maior eficiência energética, maior vida útil e menor custo de manutenção.

4.2 Indicação de marcas ou modelos

4.2.1 A Administração **não** indicará marca(s), característica(s) ou modelo(s).

4.3 Exame de adequação do objeto (amostras, avaliação de conformidade, prova de conceito, ou outros testes destinados à aferição da aceitabilidade da proposta)

4.3.1 Não será exigido(a) exame de adequação do objeto.

4.4 Vistoria

4.4.1 A avaliação prévia do local de execução do objeto é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das **09:00** horas às **12:00** horas (art. 63, §2º, da Lei Federal nº 14.133, de 2021).

4.4.1.1 Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.4.1.2 A vistoria prévia deverá ser previamente agendada com a Diretoria de Tecnologia da Informação (DTI) da SEFAZ - BA pelo telefone (071) 3115-2429 e através do e-mail seginfo@sefaz.ba.gov.br.

4.4.1.2.1 A Vistoria deverá ser realizada até o 3º (terceiro) dia útil antes da data de apresentação da proposta, podendo ser realizada por videoconferência, no horário agendado pela CONTRATANTE.

4.4.1.2.2 O(s) representante(s) da(s) empresa(s), deverá(ão) comparecer no período mencionado no item anterior, com vistas à realização da vistoria, ocasião em que lhes será fornecido o "Atestado de Vistoria Técnica", emitido e assinado por representante da CONTRATANTE. Entre outros aspectos, deverão verificar as instalações, normas, padrões, metodologias e configurações do ambiente de tecnologia da informação e comunicação da CONTRATANTE e demais detalhes necessários à execução dos serviços. O atestado será enviado pela CONTRATANTE para o e-mail do preposto da Licitante.

4.4.1.2.3 Para realizar a vistoria, os representantes deverão apresentar documento comprovando estar credenciado pela empresa interessada. Se a vistoria for presencial, os custos da visita são de total responsabilidade da Licitante, incluindo seus deslocamentos em veículo próprio ao local vistoriado. Se for por videoconferência, os documentos comprobatórios deverão ser enviados previamente para o e-mail seginfo@sefaz.ba.gov.br



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

4.4.1.2.4 As Licitantes se obrigam a não divulgar, publicar ou fazer uso das informações recebidas durante a visita. A simples participação na visita caracteriza o compromisso irrevogável de guarda do sigilo dos dados colhidos.

4.4.1.3 Caso o licitante opte por não realizar vistoria, deverá apresentar declaração formal assinada pelo seu responsável técnico acerca do conhecimento pleno das condições e peculiaridades da contratação e da sua opção por não realizar vistoria (art. 63, §3º, da Lei Federal nº 14.133/2021).

4.4.1.3.1 Caso a atividade não esteja submetida à fiscalização de conselho profissional, a declaração formal deverá ser assinada pelo responsável legal do licitante ou por pessoa por ele indicada, que possua condições técnicas de se responsabilizar pela execução dos serviços que serão contratados.

4.4.1.4 A não realização da vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo a contratada assumir os ônus dos serviços decorrentes.

4.5 Subcontratação

4.5.1 Não será admitida a subcontratação do objeto contratual.

4.6 Garantia

4.6.1 Garantia de proposta

4.6.1.1 Não haverá exigência da garantia de proposta de que trata o art. 58 da Lei Federal nº 14.133/2021.

4.6.2 Garantia da contratação

4.6.2.1 Será exigida a garantia da contratação prevista nos arts. 96 e seguintes da Lei Federal nº 14.133/2021, no **percentual de 5 % (cinco por cento) do valor anual** do Contrato, podendo recair sobre qualquer das modalidades indicadas no referido art. 96, §1º.

4.6.2.1.1 A garantia na modalidade caução em dinheiro deverá ser efetuada em favor do Contratante, em conta específica a ser indicada pelo Contratante, com correção monetária.

4.6.2.1.2 Para garantia na modalidade títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia (art. 96, §1º, inc. I, da Lei Federal nº 14.133/2021).

4.6.2.1.3 Para garantia na modalidade fiança bancária, esta deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.

4.6.2.1.4 Na hipótese de opção pela modalidade caução em dinheiro, títulos da dívida pública ou fiança bancária, a prova da garantia, sob pena da caracterização de inadimplemento contratual, deverá ser apresentada no **prazo de 30 (trinta) dias, após** () autorização da contratação direta (**X**) assinatura do Contrato.

4.6.2.1.5 Na hipótese de garantia na modalidade seguro garantia:

a) deverá ser prestada em **até 30 (trinta) dias**, contados da data da homologação da licitação e anteriormente à assinatura do Contrato (art. 96, §3º, da Lei Federal nº 14.133/2021).

b) tratando-se de contratação direta, deverá ser prestada anteriormente à assinatura do Contrato.

c) a apólice vigorará **por 90 (noventa) dias** após o término da vigência do Contrato



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

e continuará em vigor mesmo que a contratada não pague o prêmio nas datas convencionadas, devendo esta cláusula constar expressamente da apólice sob pena de não aceitação da garantia (art. 97, incs. I e II, da Lei Federal nº 14.133/2021).

d) a apólice do seguro garantia deverá acompanhar as modificações referentes à vigência do Contrato principal mediante a emissão do respectivo endosso pela seguradora.

e) será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no subitem 4.6.2.1.8 (art. 97, parágrafo único, da Lei Federal nº 14.133/2021).

f) ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos da regulamentação da Superintendência de Seguros Privados – SUSEP, devendo esta cláusula constar expressamente da apólice sob pena de não aceitação da garantia.

4.6.2.1.6 No caso das modalidades seguro garantia ou fiança bancária, não será admitida a existência de cláusulas que restrinjam ou atenuem a responsabilidade do segurador ou fiador.

4.6.2.1.7 Caso utilizada outra modalidade de garantia diversa do seguro garantia, a sua liberação ou restituição somente ocorrerá após a fiel execução do Contrato ou a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

4.6.2.1.8 Na hipótese de suspensão do Contrato por ordem ou inadimplemento do Contratante, a contratada ficará desobrigada de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pelo Contratante.

4.6.2.1.9 A garantia, qualquer que seja a modalidade escolhida, somente será aceita se, observada a legislação que rege a matéria, contemplar o pagamento de prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações nele previstas, bem como de multas, prejuízos e indenizações decorrentes de inadimplemento, independentemente de outras cominações legais.

4.6.2.1.10 No caso de alteração do valor do Contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, seguindo os mesmos parâmetros utilizados para a contratação.

4.6.2.1.11 Se o valor da garantia for utilizado total ou parcialmente para o pagamento de qualquer obrigação, a contratada obriga-se a fazer a respectiva reposição no mesmo prazo estabelecido para comprovação da garantia originária.

4.6.2.1.12 O Contratante executará a garantia na forma prevista na legislação que rege a matéria.

4.6.2.1.13 O emitente da garantia ofertada pela contratada deverá ser intimado pelo Contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei Federal nº 14.133/2021).

4.6.2.1.14 A liberação ou restituição da garantia ocorrerá após o recebimento definitivo da totalidade do objeto do Contrato, com a demonstração de cumprimento, pela contratada, das obrigações pactuadas.

4.6.2.1.15 O garantidor não é parte em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

4.6.2.1.16 A contratada autoriza o Contratante a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

4.6.2.1.17 Além da garantia de que tratam os arts. 96 e seguintes da Lei Federal nº 14.133/2021, a contratação contempla a garantia de que trata o art. 26 do Código de Defesa do Consumidor (CDC), incluindo manutenção e assistência técnica, conforme condições estabelecidas neste Termo de Referência.

4.6.2.1.18 A garantia de contratação é independente de garantia do produto/serviço prevista especificamente neste Termo de Referência nos termos do CDC.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

4.7 Participação de pessoas jurídicas reunidas em consórcio

Sim

Não, conforme justificativa constante do processo administrativo de que trata este Termo de Referência, **doc. SEI** _____ (art. 15 da Lei Federal nº 14.133/2021).

5. MODELO DE EXECUÇÃO DO OBJETO

5.1 Regime de execução

5.1.1 Condições de execução

5.1.1.1 A execução do objeto se dará da seguinte forma:

5.1.1.1.1 O prazo de execução do objeto será de **15 (quinze) dias**, a contar da data

da assinatura do Contrato

da subscrição da Autorização de Prestação de Serviços – APS.

5.1.1.1.2 Cronograma de realização do objeto:

5.1.1.2.1 Reunião inicial, conforme descrito no “Termo de Referência - Anexo I – Requisitos Gerais e Especificação Técnica”, item 8. ETAPA – IMPLANTAÇÃO DO CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC);

5.1.1.2.1.1 Em até 15 (quinze) dias, contados da data da subscrição da Autorização de Prestação de Serviços – APS, deverá ser realizada reunião inicial, convocada pelo seu gestor, com a participação dos fiscais; da Contratada; e dos demais intervenientes por ele identificados, observando, ao menos:

a) Participação dos representantes da Contratada, que apresentarão o preposto da mesma, bem como os serviços por ela oferecidos, e fará uma explanação sobre as soluções e equipe que atuará nas Etapas de Implantação e Operação dos Serviços do SOC;

b) Entrega, por parte da Contratada, do termo de confidencialidade;

c) Esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do contrato.

5.1.1.2.1.2 Prazo: Em até 15 dias após a data da subscrição da Autorização de Prestação de Serviços – APS.

5.1.1.2.2 Fases do cronograma

5.1.1.2.2.1 As demais fases do cronograma estão descritas no “Termo de Referência - Anexo I – Requisitos Gerais e Especificação Técnica”, item 4. CRONOGRAMA.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

5.2 Local da execução

5.2.1 As especificações do endereço para execução do objeto constam:
() do anexo integrante deste Termo de Referência
(X) da descrição abaixo

Os serviços serão prestados de forma remota nas instalações da Contratada e também de forma presencial na Sede da Sefaz na 2ª Avenida, nº 260 – Centro Administrativo da Bahia – CAB CEP: 41.745-003 – Salvador – Bahia.

5.3 Materiais a serem disponibilizados

5.3.1 Para a perfeita execução do objeto, a contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades suficientes e adequadas.

5.4 Garantia, manutenção e assistência técnica

5.4.1 O prazo legal de garantia será de **30 (trinta) dias**, tratando-se de fornecimento de serviço e, quando houver, de produtos não duráveis, e de **90 (noventa) dias**, tratando-se de fornecimento de serviço e, quando houver, de produtos duráveis, contado da entrega efetiva do produto ou do término da execução dos serviços (art. 26, incs. I e II, e §1º, do CDC).

5.5 Informações relevantes para o dimensionamento da proposta

5.5.1 As informações relevantes para o dimensionamento da proposta constam deste Termo de Referência.

5.5.2 O prazo de validade da proposta será de, no mínimo, 60 (sessenta) dias, a contar da data de sua apresentação.

5.5.2.1 Será considerada não escrita a fixação de prazo de validade inferior ao mínimo, ficando facultado aos licitantes ampliá-lo.

5.5.3 O licitante deverá apresentar a sua proposta e declaração de elaboração independente de proposta, conforme modelo integrante deste Termo de Referência.

5.5.4 Além das informações que já constam neste Termo de Referência, constituem, ainda, informações relevantes para o dimensionamento da proposta as que constam do **anexo** integrante deste Termo de Referência.

6. MODELO DE GESTÃO DO CONTRATO

6.1 O Contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei Federal nº 14.133/2021, e da Lei Estadual nº 14.634/2023, respondendo cada parte pelas consequências de sua inexecução total ou parcial (art. 115, *caput*, da Lei Federal nº 14.133/2021).

6.2 Em caso de impedimento, ordem de paralisação ou suspensão do Contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila (art. 115, §5º, da Lei Federal nº 14.133/2021).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

6.2.1 O impedimento a que se refere o subitem anterior, total ou parcial, da execução do Contrato por fato ou ato de terceiro, deve ser reconhecido pela Administração em documento contemporâneo à sua ocorrência.

6.3 As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, para esse fim, o uso de mensagem eletrônica por meio do Sistema Eletrônico de Informações – SEI.

6.4 O órgão ou entidade poderá convocar representante da contratada para adoção de providências que devam ser cumpridas de imediato.

6.5 O acompanhamento da execução do Contrato compreenderá as atividades de gestão e fiscalização na forma dos arts. 15 a 23 do Decreto nº 22.885/2024, observando-se, ainda, o disposto nos arts. 7º e 17 do Decreto nº 23.059/2024.

6.5.1 Constatando-se a situação de irregularidade da contratada, será providenciada sua intimação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua justificativa.

6.5.2 O prazo de que trata o subitem anterior poderá ser prorrogado uma vez, **por até 5 (cinco) dias úteis**, a critério do Contratante.

6.5.3 Não havendo regularização ou não sendo aceita a justificativa apresentada, a Administração deverá adotar as medidas necessárias à apuração dos fatos nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

6.6 Após a assinatura do Contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para alinhamento da execução do Contrato e demais procedimentos de gestão do ajuste.

7. CRITÉRIOS DE RECEBIMENTO DO OBJETO, LIQUIDAÇÃO E PAGAMENTO

7.1 RECEBIMENTO DO OBJETO

7.1.1 Recebimento provisório

7.1.1.1 O objeto do Contrato será recebido provisoriamente, no prazo de 15 (quinze) dias, pelo(s) fiscal(is) do Contrato, mediante termo(s) detalhado(s), quando verificado o cumprimento das exigências de caráter técnico e administrativo (art. 140, inc. I, "a", da Lei Federal nº 14.133/2021).

7.1.1.1.1 O prazo de que trata este subitem anterior será contado do recebimento de comunicação escrita da contratada com a comprovação da execução do objeto a que se refere a parcela a ser paga.

7.1.1.2 A contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados (art. 119 da Lei Federal nº 14.133/2021).

7.1.1.3 O objeto poderá ser rejeitado, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituído ou corrigido no prazo de 15 (quinze) dias, a contar da intimação da contratada, às suas custas, sem prejuízo da aplicação das penalidades (art. 140, §1º da Lei Federal nº 14.133, de 2021).

7.1.1.4 Para efeito de recebimento provisório, ao final de cada período de faturamento, o(s) fiscal(is) do Contrato deverá(ão) emitir relatório sobre o efetivo cumprimento das obrigações da contratada e, se for o caso, analisar o desempenho na execução do Contrato nos termos do art. 144 da Lei Federal nº 14.133/2021, em consonância com os indicadores que deverão integrar este Termo de Referência como anexo, encaminhando-o ao gestor do Contrato.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.1.1.4.1 A análise do desempenho na execução do Contrato de que trata o art. 144 da Lei Federal nº 14.133/2021 poderá resultar no redimensionamento de valores a serem pagos à contratada, circunstância que deverá ser registrada pelo(s) fiscal(is) em relatório(s) a ser encaminhado ao gestor do Contrato.

7.1.1.5 A fiscalização não efetuará o ateste da última e/ou única medição do objeto até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas durante o recebimento provisório.

7.1.1.6 O recebimento provisório estará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

7.1.1.7 Quando a fiscalização for exercida por um único servidor, o termo detalhado de recebimento provisório deverá conter o registro, a análise e a conclusão sobre todas as ocorrências na execução do Contrato, acompanhado dos demais documentos que julgar necessários, encaminhando-o ao servidor ou comissão designada pela autoridade competente para recebimento definitivo.

7.1.2 Recebimento definitivo

7.1.2.1 O recebimento definitivo ocorrerá no **prazo de 10 (dez) dias úteis**, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais, observados os seguintes procedimentos (art. 140, inciso I, "b" da Lei Federal nº 14.133/2021):

- a) emissão de documento comprobatório da avaliação realizada pelo(s) fiscal(is) sobre o cumprimento de obrigações assumidas pela contratada, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos nos termos do Decreto nº 23.059/2024, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações;
- b) análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicação das cláusulas contratuais correspondentes, solicitando à contratada por escrito, as respectivas correções;
- c) emissão de termo detalhado para efeito de recebimento definitivo dos serviços, com base nos relatórios elaborados e documentações apresentadas;
- d) comunicação à contratada para emissão de nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s), com o valor exato dimensionado pela fiscalização;
- e) envio da documentação correspondente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão;
- f) exigência de apresentação pela contratada do Relatório "AS BUILT", no caso de obras e serviços de engenharia.

7.1.2.1.1 O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.1.2.1.2 O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato (art. 140, §§2º e 6º da Lei Federal nº 14.133, de 2021).

7.1.2.2 No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, a parcela incontroversa, conforme art. 143 da Lei Federal nº 14.133/2021, deverá ser liberada no prazo previsto para pagamento.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.1.2.2.1 Para fins do subitem anterior, o valor da parcela incontroversa deverá ser comunicada à contratada para emissão de nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s).

7.1.2.3 Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pela contratada, de inconsistências verificadas na execução do objeto ou nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s).

7.2 LIQUIDAÇÃO

7.2.1 Recebida(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s), a Administração, no **prazo de 10 (dez) dias úteis**, prorrogáveis por até **10 (dez) dias úteis**, adotará, na forma deste subitem, as providências para fins de liquidação da despesa.

7.2.2 Para fins de liquidação, o setor competente deverá verificar se a(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) apresentado(s) pela contratada possui(em) os elementos necessários e essenciais do documento, tais como: a) o prazo de validade; b) a data da emissão; c) os dados do Contrato e do Contratante; d) o período respectivo de execução do Contrato; e) o valor a pagar; e f) eventual destaque do valor de retenções tributárias cabíveis.

7.3.3 Havendo erro na apresentação da(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s), ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a contratada providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus para o Contratante;

7.4.4 A(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) deverá(ão) ser obrigatoriamente acompanhado(s) da comprovação da regularidade fiscal da contratada mediante consulta aos sítios eletrônicos oficiais ou à documentação de habilitação fiscal, social e trabalhista, na forma exigida neste Termo de Referência.

7.3 PAGAMENTO

7.3.1 Prazo para pagamento

7.3.1.1 O pagamento será efetuado no **prazo de 10 (dez) dias úteis**, contados da finalização da liquidação da despesa, conforme subitem anterior.

7.3.1.2 No caso de atraso pelo Contratante, os valores devidos à contratada serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, de acordo com a variação do Índice Nacional de Preços - INPC do IBGE, *pro rata tempore*.

7.3.2 Forma de pagamento

7.3.2.1 O pagamento será realizado por meio de ordem bancária ou crédito em conta da contratada aberta em instituição financeira contratada pelo Estado da Bahia.

7.3.2.1.1 Optando a contratada por receber os créditos em instituição financeira diversa da indicada neste subitem, deverá arcar com os custos de transferências bancárias, os quais serão deduzidos dos pagamentos devidos.

7.3.2.2 A(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) deverá(ão) atender as exigências legais pertinentes aos tributos e encargos relacionados com a obrigação, inclusive os destaques necessários às retenções tributárias previstas em lei, e, as situações específicas, à adoção da forma eletrônica.

7.3.2.3 Independentemente do percentual de tributo inserido na proposta de preço, serão retidos na fonte, por ocasião da realização do pagamento, os percentuais estabelecidos na legislação vigente, quando houver incidência tributária.

7.3.2.4 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, estando o pagamento condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8. FORMA E CRITÉRIOS DE SELEÇÃO DA PROPOSTA E EXIGÊNCIAS DE HABILITAÇÃO



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

8.1 Forma de seleção e critério de julgamento da proposta

- 8.1.1 O fornecedor do bem, obra ou serviço será selecionado por meio de processo de:
- Contratação direta
 - Licitação, na modalidade pregão, sob a forma eletrônica, com adoção do critério de julgamento
 - menor preço
 - maior desconto
 - Licitação, na modalidade concorrência, sob a forma eletrônica, com adoção do critério de julgamento
 - menor preço
 - maior desconto
 - melhor técnica ou conteúdo artístico, conforme anexo
 - técnica e preço, conforme anexo

8.2 Exigências de habilitação

8.2.1 Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

8.2.1.1 Habilitação jurídica

8.2.1.1.1 Para **Pessoas Jurídicas**:

- a) empresário individual: inscrição no registro público de empresas mercantis;
- b) microempreendedor individual – MEI: certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;
- c) sociedade empresária, sociedade limitada unipessoal: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados, quando for o caso, dos documentos societários comprobatórios de eleição ou designação e investidura dos atuais administradores.
- d) sociedades simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados dos atos comprobatórios de eleição e investidura dos atuais administradores.
- e) empresa ou sociedade estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, observando-se a Instrução Normativa DREI/ME nº 77, de 18 de março de 2020, quando a atividade assim o exigir.
- f) filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

8.2.1.1.2 Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

8.2.1.2 Habilitação fiscal, social e trabalhista

- a) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

b) prova de inscrição no cadastro de contribuintes () Estadual/Distrital (X) Municipal/Distrital relativo ao domicílio ou sede do licitante pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) prova de regularidade com a Fazenda () Estadual/Distrital (X) Municipal/Distrital do domicílio ou sede do licitante, ou outro equivalente, na forma da lei;

Nota: a regularidade diz respeito ao proponente e não ao órgão ou entidade que licita.

c.1) Caso o licitante seja considerado isento dos tributos relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

d) prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social.

e) prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

f) prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de 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;

g) em se tratando de contratação direta, prova de regularidade com a Fazenda do Estado da Bahia, ou o compromisso de sua regularização e sua efetiva realização, como condição para celebração do Contrato, nos termos do art. 65 da Lei estadual nº 14.634/2023.

8.2.1.2.1 As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar nº 123/2006, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

8.2.1.3 Habilitação Econômico-Financeira

Notas:

1. a habilitação econômico-financeira poderá ser dispensada, total ou parcialmente, nas hipóteses do art. 70, inc. III, da Lei Federal nº 14.133/2021, desde que precedida da análise dos riscos envolvidos na sua supressão e seja autorizado pela autoridade competente.

2. Observar o disposto na Instrução Normativa SAEB nº 10/2024.

a) certidão negativa de falência expedida pelo distribuidor da sede do licitante, com data de expedição ou revalidação dos últimos 90 (noventa) dias anteriores à data da realização da licitação ou da contratação direta, caso o documento não consigne prazo de validade;

b) índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante)

Solvência Geral (SG) = (Ativo Total)/(Passivo Circulante + Passivo não Circulante)



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante)

b.1) Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, patrimônio líquido mínimo correspondente a 10% (dez por cento) do valor estimado da contratação;

b.1.1) Na hipótese de licitação por lotes, o patrimônio líquido exigível será calculado em função da soma de tantos quantos forem os lotes em que a interessada tenha apresentado as melhores ofertas.

b.2) O balanço patrimonial, a demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício, caso a pessoa jurídica tenha sido constituída há menos de 2 (dois) anos (art. 69, §6º, da Lei Federal nº 14.133/2021).

b.3) O balanço patrimonial e demonstrações contábeis podem ser atualizados por índices oficiais, quando encerrados há mais de 03 (três) meses da data da apresentação da proposta, vedada a sua substituição por balancetes ou balanços provisórios.

b.4) O licitante apresentará o balanço patrimonial e a demonstração de resultado do exercício mediante, conforme o caso, publicação no Diário Oficial ou Jornal de Grande Circulação ou na Central de Balanços dentro do ambiente Sistema Público de Escrituração Digital – SPED, cópia reprográfica das páginas do Livro Diário numeradas sequencialmente onde eles foram transcritos, com os respectivos Termos de Abertura e Encerramento registrados na Junta Comercial, emissão extraída do SPED, contendo Recibo de Entrega do Livro, os Termos de Abertura, Encerramento e Autenticação.

b.5) O atendimento dos índices econômicos previstos neste subitem será atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo licitante (art. 69, §1º, da Lei Federal nº 14.133/2021).

8.2.1.3.1 Na licitação por lotes, quando for atingido o limite da capacidade econômico-financeira do licitante, esta será declarada inabilitada para o(s) lote(s) subsequentes, observada a ordem sequencial dos lotes constante do instrumento convocatório, sendo vedada a escolha, pelo licitante, dos lotes para os quais deseja a habilitação.

8.2.1.3.2 Na hipótese de participação de pessoas jurídicas reunidas em consórcio, se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte, para fins de habilitação econômico-financeira, haverá um acréscimo no percentual de 10% (dez por cento) para o consórcio em relação ao valor exigido para os licitantes individuais.

8.2.1.4 Qualificação Técnica

a) comprovação de capacitação **técnico-profissional**, através da apresentação de profissional, devidamente registrado no conselho profissional competente, detentor de atestado de responsabilidade técnica por execução de objeto de características semelhantes, para fins de contratação, limitadas estas às parcelas de maior relevância ou valor significativo (art. 67, inc. I, §§1º e 2º, da Lei Federal nº 14.133/2021). **NÃO SE APLICA**

a.1) O vínculo profissional entre o profissional e o licitante poderá ser comprovado através de: a) Carteira de Trabalho; b) Certidão do Conselho Profissional; c) Contrato social; d) Contrato de prestação de serviços; e) Termo através do qual o profissional assumira a responsabilidade técnica pela execução do objeto licitado e o compromisso de integrar o quadro técnico da empresa no caso do objeto contratual vir a ser a esta adjudicado.

a.2) Os profissionais indicados pelo licitante para fins de comprovação da capacitação técnica deverão participar da execução do objeto da licitação, admitindo-se a sua substituição por profissionais de experiência equivalente ou



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

superior, desde que aprovada pela Administração (art. 67, §6º, da Lei Federal nº 14.133/2021);

a.3) Não será admitido que um mesmo profissional indicado como responsável técnico participe de mais de uma proposta apresentada por licitantes diversos.

b) comprovação de capacitação **técnico-operacional**, mediante apresentação de certidões ou atestados, regularmente emitidos pelo conselho profissional competente, que demonstrem capacidade operacional na execução de objeto similar, de complexidade tecnológica e operacional equivalente ou superior, limitada às parcelas de maior relevância ou valor significativo (art. 67, inc. II, §§1º e 2º, da Lei Federal nº 14.133/2021);

b1) na hipótese de atividade não regulada por conselho profissional, a capacitação **técnico-operacional** referida neste item poderá ser demonstrada por certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, preferencialmente conforme modelo anexo a este Termo de Referência.

b2) Será admitida a apresentação de atestados relativos a potencial subcontratado em relação à parcela do objeto cuja subcontratação tenha sido expressamente autorizada neste Termo de Referência, limitada a 25% (vinte e cinco por cento) do objeto a ser licitado, hipótese em que mais de um licitante poderá apresentar atestado relativo ao mesmo potencial subcontratado (art. 67, §9º, da Lei Federal nº 14.133/2021).

b3) Tratando-se de serviços contínuos, deverá haver a comprovação da experiência mínima na prestação dos serviços conforme detalhamento no ENCARTE G – Qualificação Técnica do “Anexo I – Requisitos Gerais e Especificação Técnica”, em períodos sucessivos ou não, sendo aceito o somatório de atestados de períodos diferentes;

c) indicação do pessoal técnico, das instalações e do aparelhamento adequados e disponíveis para a realização do objeto, bem como da qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos, preferencialmente conforme modelo anexo a este Termo de Referência (art. 67, inc. III, da Lei Federal nº 14.133/2021).

c.1) Para fins desta alínea “c”), o licitante deverá apresentar, sob as penas da lei, em especial do disposto no art. 155, inc. VIII, da Lei Federal nº 14.133/2021, a relação explícita e declaração formal de disponibilidade, de acordo com as especificações exigidas;

c.2) Quanto ao pessoal técnico, será observado o que se segue:

c.2.1) relação do pessoal técnico indicado pelo licitante deverá estar acompanhada da demonstração de vinculação à futura execução contratual, mediante a juntada no sistema eletrônico, de quaisquer dos seguintes documentos: a) Carteira de Trabalho; b) Certidão do Conselho Profissional; c) Contrato social; d) Contrato de prestação de serviços; e) Termo através do qual o profissional assumo o compromisso de integrar o quadro técnico da empresa no caso do objeto contratual vir a ser a esta adjudicado.

c.2.2) Os profissionais indicados pelo licitante para fins de comprovação da capacitação técnica deverão participar da execução do objeto da licitação, admitindo-se a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pela Administração (art. 67, §6º, da Lei Federal nº 14.133/2021);

c.2.3) Não será admitido que um mesmo profissional indicado como responsável técnico participe de mais de uma proposta apresentada por licitantes diversos.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

d) prova de atendimento de requisitos previstos em lei especial, se for o caso [indicar a lei especial e os requisitos, se for o caso] (art. 67, inc. IV, da Lei Federal nº 14.133/2021); **NÃO SE APLICA.**

e) registro ou inscrição do licitante na entidade profissional competente, se for o caso [indicar a entidade profissional, se for o caso]; **NÃO SE APLICA.**

e.1) No caso de empresa não registrada no respectivo Conselho no Estado da Bahia, deverá apresentar o registro do Conselho do Estado de origem, ficando o licitante vencedor obrigado a apresentar o visto do Conselho local antes da assinatura do Contrato.

e.2) No caso de Sociedades empresárias estrangeiras, o atendimento da exigência de que trata esta alínea "e" se dará por meio da apresentação, no momento da assinatura do Contrato, da solicitação de registro perante a entidade profissional competente no Brasil.

f) declaração no sistema eletrônico da licitação de que o licitante tomou conhecimento de todas as informações e, quando exigido, das condições locais, para o cumprimento das obrigações objeto da licitação ou da contratação direta (art. 67, inc. VI, da Lei Federal nº 14.133/2021).

f.1) Na hipótese de exigência de realização de vistoria prévia do local da execução, caso o licitante opte por não realizá-la, além da declaração de que trata essa alínea "f", deverá apresentar declaração formal assinada pelo seu responsável técnico de conhecimento pleno das condições e peculiaridades da contratação, preferencialmente conforme modelo anexo a este Termo de Referência.

8.2.1.4.1 Serão consideradas como parcelas de maior relevância ou valor significativo, para fins das alíneas "a", "b" e "c" deste tópico:

PARCELAS DE MAIOR RELEVÂNCIA OU VALOR SIGNIFICATIVO	QUANTITATIVO TOTAL (100%)	COMPROVAÇÃO MÍNIMA (____ %)
Serviços Gerenciados de Segurança da Informação	21 meses	6 meses (28,57%)
Fornecimento de Solução de Gerenciamento de Eventos e Informações de Segurança (SIEM)	914 ativos de TI	457 ativos (50%)
Gerenciamento de Solução de Gerenciamento de Eventos e Informações de Segurança (SIEM)	21 meses	6 meses (28,57%)
Fornecimento de Solução de Avaliação de Vulnerabilidades	914 ativos de TI 5.000 usuários do AD	457 ativos (50%) 2.500 usuários do AD (50%)
Gerenciamento de Solução de Avaliação de Vulnerabilidades	21 meses	6 meses (28,57%)



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

8.2.1.4.1.1 Na hipótese de objeto em que não seja possível distinguir as parcelas de maior relevância ou valor significativo (objeto homogêneo), poderá ser indicada **parcela única**, sendo considerada satisfatória a comprovação da execução de, no mínimo, 50 % (cinquenta por cento) do(s) quantitativo(s) previsto(s) neste Termo de Referência.

8.2.1.4.2 Na hipótese de licitação por lotes, será observado o disposto a seguir:

8.2.1.4.2.1 A demonstração da qualificação técnica deverá ser feita em função da soma de tantos quantos forem os lotes em que o licitante tenha apresentado as melhores ofertas.

8.2.1.4.2.2 Quando for atingido o limite da capacidade técnica do licitante, este será declarado inabilitado para o(s) lote(s) subsequentes, observada a ordem sequencial dos lotes, sendo vedada a escolha, pelo licitante, dos lotes para os quais deseja a habilitação.

8.2.1.4.3 No caso de apresentação por licitante de atestado de desempenho anterior emitido em favor de consórcio do qual tenha feito parte, se o atestado ou o contrato de constituição do consórcio não identificar a atividade desempenhada por cada consorciado individualmente, serão adotados os seguintes critérios na avaliação de sua qualificação técnica (art. 67, §10, da Lei Federal nº 14.133/2021).

8.2.1.4.3.1. Caso o atestado tenha sido emitido em favor de consórcio homogêneo, as experiências atestadas deverão ser reconhecidas para cada empresa consorciada na proporção quantitativa de sua participação no consórcio, salvo nas licitações ou contratações diretas destinadas à contratação de serviços técnicos especializados de natureza predominantemente intelectual, em que todas as experiências atestadas deverão ser reconhecidas para cada uma das empresas consorciadas;

8.2.1.4.3.2. Caso o atestado tenha sido emitido em favor de consórcio heterogêneo, as experiências atestadas deverão ser reconhecidas para cada consorciado de acordo com os respectivos campos de atuação, inclusive nas licitações ou contratações diretas destinadas à contratação de serviços técnicos especializados de natureza predominantemente intelectual.

8.2.1.4.3.3 Na hipótese deste subitem 8.2.1.4.3, para fins de comprovação do percentual de participação do consorciado, caso este não conste expressamente do atestado ou da certidão, deverá ser juntada ao atestado ou à certidão cópia do instrumento de constituição do consórcio.

8.3 Disposições gerais

8.3.1 As empresas criadas no exercício financeiro da licitação ou da contratação direta deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura (art. 65, §1º, da Lei Federal nº 14.133/2021).

8.3.2 Regras acerca da participação de matriz e filial:

- a) se o licitante for a matriz, todos os documentos devem estar em nome da matriz;
- b) se o licitante for filial, todos os documentos devem estar em nome da filial, exceto aqueles que a legislação permita ou exija a emissão apenas em nome da matriz;
- c) a comprovação de capacidade operacional para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação ou da contratação direta poderá ser feita em nome da matriz ou da filial;
- d) se o licitante participar do certame apresentando os documentos de habilitação e qualificação da matriz e desejar executar o Contrato pela filial, ou vice-versa, deverá fazer prova, por ocasião da assinatura do Contrato, da regularidade do estabelecimento que executará o objeto licitado, a qual deverá ser mantida durante todo o curso da avença.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

8.3.3 O Certificado de Registro Cadastral-CRC ou Certificado de Registro Simplificado-CRS poderá substituir os documentos de habilitação, na forma indicada neste Termo de Referência.

8.3.3.1 Caso conste do registro algum documento vencido, o licitante deverá apresentar a versão atualizada do referido documento junto aos demais documentos de habilitação.

8.3.3.2 A substituição dos documentos está condicionada à verificação da regularidade destes, mediante a emissão do extrato do fornecedor pela Administração.

8.3.3.3 O Certificado de Registro Cadastral-CRC ou Certificado de Registro Simplificado-CRS, estando no prazo de validade, poderá substituir os documentos relativos à habilitação constantes do sistema, exceto os concernentes à Qualificação Técnica.

8.3.4 Na hipótese de participação de pessoas jurídicas em consórcio, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado (art. 15, inc. III, da Lei Federal nº 14.133/2021).

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1 O valor estimado total da contratação é de R\$ 8.682.179,07 (oito milhões, seiscentos e oitenta e dois mil, cento e setenta e nove reais e sete centavos), conforme planilha de quantitativos e preços unitários e global abaixo, os quais correspondem **ao critério máximo de aceitabilidade dos preços unitários e global.**

LOTE/ ITEM	Código SIMPAS	Unidade de Fornecimento (UF)	Quantitativo	Cronograma/prazo	PREÇO UNITÁRIO	PREÇO GLOBAL	DEGRAU
1	02.81.13.000021326	UN	1	Implantação (3 meses)	R\$ 171.182,70	R\$ 171.182,70	R\$ 100,00
2	02.81.13.000021296	UN	21	21 meses	R\$ 98.277,42	R\$ 2.063.825,82	R\$ 100,00
3	02.81.13.000021300	UN	1	24 meses	R\$ 3.891.255,27	R\$ 3.891.255,27	R\$ 100,00
4	02.81.13.000021318	UN	1	24 meses	R\$ 2.555.915,28	R\$ 2.555.915,28	R\$ 100,00
				VALOR ESTIMADO TOTAL		R\$ 8.682.179,07	

10. ADEQUAÇÃO ORÇAMENTÁRIA



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

10.1 As despesas para o pagamento da presente contratação correrão à conta de recursos da Dotação Orçamentária a seguir especificada:

UNIDADE ORÇAMENTÁRIA: 13.101 - APG/SEFAZ
AÇÃO: 04.126.441.1451- - Modernização de Tecnologia da Informação e Comunicação
DESTINAÇÃO DA DESPESA: 1.754.0.125.800.112.000000/ 2.754.0.325.800.112.000000
NATUREZA DA DESPESA: 44.90.40.000 – Outros Serviços de Terceiros - Pessoa Jurídica

10.1.1 A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11. PRAZO PARA ASSINATURA DO CONTRATO

11.1 O prazo para assinatura do Contrato ou retirada do instrumento equivalente será de 10 (dez) dias úteis, observado o disposto no art. 90 da Lei Federal nº 14.133/2021.

11.1.1 O prazo de que trata o subitem 11.1 poderá ser prorrogado uma vez, por, no máximo, idêntico período, mediante solicitação do Adjudicatário durante seu transcurso, devidamente justificada, e desde que o motivo apresentado seja aceito pela Administração.

11.2 A assinatura do Contrato se dará por meio do Sistema Eletrônico de Informações - SEI, caso em que o licitante deverá providenciar o cadastramento de seu representante legal ou procurador no endereço eletrônico www.portalseibahia.saeb.ba.gov.br ou através do link disponibilizado no endereço eletrônico www.comprasnet.ba.gov.br.

12. ANEXOS E MODELOS DO TERMO DE REFERÊNCIA

12.1 Vinculam-se a este Termo de Referência, independentemente de transcrição (art. 92, inc. II, da Lei Federal nº 14.133/2021):

- a) ANEXO I – Requisitos Gerais e Especificação Técnica;
- b) ANEXO II – Modelo de Proposta de Preços
- c) Estudo Técnico Preliminar – ETP

Salvador, 19 de fevereiro de 2025



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Ednilson Gimenes Rosa – Matrícula: 13.421.696-9

Gerente de Planejamento e Governança de TIC - SGF\DTI\PGTIC

Secretaria da Fazenda do Estado da Bahia



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

1. OBJETO

O objeto desta contratação é um Centro de Operações de Segurança (SOC), serviços gerenciados de segurança e soluções de TI associados, conforme requisitos definidos no Termo de Referência e seus anexos.

2. CONSIDERAÇÕES

Este documento descreve os requisitos gerais, quantitativos e especificações técnicas dos serviços gerenciados de segurança, componentes e soluções de TI necessárias à implantação e operação do Centro de Operações de Segurança (SOC).

As especificações detalhadas neste documento têm caráter obrigatório, devendo ser atendidas em sua totalidade pela LICITANTE ou CONTRATADA. O não atendimento de qualquer das exigências, sujeitará a LICITANTE ou a CONTRATADA às penalidades previstas.

3. ITENS A SEREM CONTRATADOS

	ITENS	QTDE
1	Centro de Operações de Segurança (SOC) - Estruturação e implantação 3 (três) meses	1
2	Centro de Operações de Segurança (SOC) - Operação 21 (vinte e um) meses	21
3	Software de Gerenciamento de eventos e informações de segurança (SIEM) Licenciamento por 24 (vinte e quatro) meses	1
4	Software de Gestão de Vulnerabilidades Licenciamento por 24 (vinte e quatro) meses	1

4. CRONOGRAMA

Este documento descreve os requisitos gerais, quantitativos e especificações técnicas dos serviços gerenciados de segurança, componentes e soluções de TI necessárias à implantação e operação do Centro de Operações de Segurança (SOC).

CENTRO DE OPERAÇÕES DE SEGURANÇA - SOC		
ITEM	ATIVIDADE	PRAZO



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

A	Centro de Operações de Segurança (SOC) - Estruturação e implantação	Em até 90 (noventa) dias após a Reunião de Kick-off – Aprovação do Plano de Implantação . Conforme definido neste anexo, a Reunião de Kick-off deve ocorrer no prazo máximo de 15 (quinze) dias corridos a contar da data da subscrição da Autorização de Prestação de Serviços – APS .
B	Centro de Operações de Segurança (SOC) - Operação	De forma imediata, por 21 (vinte e um) meses, após a entrega do item A
C	Entrega do Software de Gerenciamento de eventos e informações de segurança (SIEM)	Em até 15 (quinze) dias corridos a contar da data da subscrição da Autorização de Prestação de Serviços – APS .
D	Testes de Aceitação do Software de Gerenciamento de eventos e informações de segurança (SIEM): Aceitação <ul style="list-style-type: none">✦ Instalação básica e pré-configuração do Software de Gerenciamento de eventos e informações de segurança (SIEM)✦ Teste de aceitação do Software do Gerenciamento de eventos e informações de segurança (SIEM)	Em até 15 (quinze) dias corridos após a Reunião de Kick-off – Aprovação do Plano de Implantação .
E	Entrega do Software de Software de Gestão de Vulnerabilidades	Em até 15 (quinze) dias corridos a contar da data da subscrição da Autorização de Prestação de Serviços – APS .
F	Testes de Aceitação do Software de Gestão de Vulnerabilidades <ul style="list-style-type: none">✦ Instalação básica e pré-configuração do Software de Gestão de Vulnerabilidades✦ Teste de aceitação do Software do Gestão de Vulnerabilidades	Em até 15 (quinze) dias corridos após a Reunião de Kick-off – Aprovação do Plano de Implantação .

5. FORMA DE PAGAMENTO

O pagamento será efetuado pela CONTRATANTE em parcelas proporcionais aos objetos/serviços/produtos entregues, conforme cronograma apresentado na tabela abaixo, mediante apresentação pela CONTRATADA da Nota Fiscal/Fatura, e ocorrerá em até **30 (trinta) dias** após a emissão do respectivo **Termo de Aceite**.

CENTRO DE OPERAÇÕES DE SEGURANÇA - SOC		
ITEM	ATIVIDADE	CRONOGRAMA DE PAGAMENTO



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

1	Centro de Operações de Segurança (SOC) - Estruturação e implantação	Após entrega e aprovação dos entregáveis previstos no ENCARTÉ A: Implantação do SOC
2	Centro de Operações de Segurança (SOC) - Operação	Mensalmente, após o início da Etapa – Operação dos Serviços por um período de 21 (vinte e um) meses
3	Software de Gerenciamento de eventos e informações de segurança (SIEM)	75% - Após a emissão do Termo de Aceite do Software de Gerenciamento de eventos e informações de segurança (SIEM) 25% - Após entrega e aprovação dos entregáveis previstos no ENCARTÉ A: Implantação do SOC
4	Software de Gestão de Vulnerabilidades	75% - Após a emissão do Termo de Aceite do Software de Gestão de Vulnerabilidades 25% - Após entrega e aprovação dos entregáveis previstos no ENCARTÉ A: Implantação do SOC

Caso os produtos ou os serviços entregues não atendam às especificações técnicas, o prazo para pagamento terá como termo inicial a data da sua regularização.

6. ESTRUTURA DESTA ANEXO

Os seguintes documentos estão compondo este ANEXO I do Termo de Referência (TR):

- **ENCARTE A:** Implantação do SOC;
- **ENCARTE B:** Nível Mínimo de Serviço (NMS) – Indicadores de desempenho e Penalidades;
- **ENCARTE C:** Ambiente de TI – SEFAZ BA;
- **ENCARTE D:** Perfil Profissional;
- **ENCARTE F:** Plano de Capacitação;
- **ENCARTE G:** Qualificação Técnica;
- **ENCARTE H:** Testes de Aceitação;
- **ENCARTE I:** Modelo para Comprovação Resumida dos Requisitos Técnicos
- **ENCARTE J:** Modelo para Atestado de Vistoria Técnica
- **ENCARTE K:** Modelo de Prova de Qualificação Técnica

7. ESPECIFICAÇÃO TÉCNICA – SERVIÇOS GERENCIADOS DE SEGURANÇA E SOLUÇÕES DE SEGURANÇA

O Centro de Operações de Segurança (SOC) conforme descrito neste Termo de Referência deve seguir as melhores práticas de Segurança da Informação, prover uma infraestrutura física remota para hospedar o SOC, executar todos os serviços gerenciados de segurança previstos e fornecer as soluções de segurança conforme especificados neste documento.

Esta especificação técnica estabelece os conceitos, critérios, condições e requisitos que definem como deve ocorrer a prestação dos serviços gerenciados de segurança assim como o fornecimento de soluções de segurança associadas.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.1. CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)

ESPECIFICAÇÃO TÉCNICA			
1	ESCOPO	1.1	O objeto desta contratação é um Centro de Operações de Segurança (SOC), serviços gerenciados de segurança e soluções de TI associados, conforme requisitos definidos neste Termo de Referência.
		1.1.1	Os serviços gerenciados de segurança objeto deste Termo de Referência devem ser estruturados em duas etapas:
		1.1.1.1	IMPLANTAÇÃO DO SOC: Estruturação do Centro de Operações de Segurança - SOC (infraestrutura física, ambiente, equipe técnica, ferramentas de software, processos, etc.) conforme descrito neste Termo de Referência, Encarte A: Implantação do SOC, para suportar a OPERAÇÃO DOS SERVIÇOS.
		1.1.1.2	OPERAÇÃO DOS SERVIÇOS: Centro de Operações e os serviços gerenciados de segurança descritos no item 2 a seguir em produção com equipe técnica estruturada e alocada, processos estruturados e treinados, soluções de segurança implantadas e integradas ao ambiente de TI da SEFAZ BA.
		1.2	A CONTRATADA deve estruturar, administrar e operar um Centro de Operações de Segurança (SOC) responsável por gerenciar, coordenar e executar os serviços gerenciados de segurança previstos neste Termo de Referência.
		1.2.1	O Centro de Operações de Segurança (SOC) deve funcionar em regime 24x7x365 (24 horas por dia, 7 dias por semana, todos os dias do ano), tendo por objetivo monitorar o ambiente da SEFAZ BA, sustentar e operar soluções de segurança fornecidas e/ou administradas pela CONTRATADA para atender este Termo de Referência que devem ser utilizadas na prestação dos serviços conforme definido neste Termo de Referência. Este Centro de Operações de Segurança (SOC) para fins deste documento será identificado como SOC SEFAZ BA.
		1.2.1.1	Alguns dos serviços gerenciados de segurança associados ao Centro de Operações de Segurança (SOC), conforme descrito neste Termo de Referência, devem ser prestados no período das 08:00 às 18:00 horas, de segunda à sexta-feira, exceto feriados.
		1.2.2	Os serviços gerenciados de segurança prestados pela CONTRATADA através do Centro de Operações de Segurança (SOC) devem atender os Níveis Mínimos de Serviços definidos neste Termo de Referência, ENCARTE B: Nível Mínimo de Serviço (NMS) – Indicadores de desempenho e Penalidades.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		1.3	O SOC SEFAZ BA, objeto desta contratação, tem dois componentes que devem trabalhar de forma integrada para atender os serviços previstos neste Termo de Referência:
		1.3.1	SOC REMOTO - Estruturado e fisicamente localizado nas instalações da CONTRATADA.
		1.3.2	SOC LOCAL - Estruturado e fisicamente localizado nas instalações da SEFAZ BA.
		1.4	O SOC SEFAZ BA funcionará em regimes compatíveis com os serviços a serem prestados e conforme definido neste Termo de Referência.
		1.5	A CONTRATADA deve disponibilizar, organizar e administrar todos os recursos necessários para a realização dos serviços e atividades associadas, conforme definido neste Termo de Referência;
		1.5.1	Entende-se como recursos necessários: equipe técnica, estrutura física, postos de trabalho, equipamentos, conectividade, internet, soluções de TI (HW e SW), metodologias, processos e procedimentos para execução dos serviços, etc.
		1.5.2	Cabe a SEFAZ BA disponibilizar a infraestrutura associada aos postos de trabalhos (mobiliário, computador, conectividade de rede e à internet) das equipes técnicas alocadas no SOC SEFAZ BA (Local) conforme definido neste Termo de Referência.
		1.6	A CONTRATADA deve alocar uma equipe técnica com o conhecimento, experiência e quantitativo necessários para garantir a qualidade dos serviços e informações prestadas, atuando conforme o estado da arte e melhores práticas em termos de segurança da informação, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados neste Termo de Referência.
		1.6.1	Define-se como EquipeSOC a equipe técnica alocada pela CONTRATADA para a execução dos serviços previstos neste Termo de Referência.
		1.6.2	Define-se como EquipeSEFAZ BA a equipe técnica alocada pela CONTRATANTE para interagir com a CONTRATADA na execução dos serviços previstos neste Termo de Referência.
		1.7	A CONTRATADA é responsável pela implementação, configuração e plena operação das soluções de TI sob sua administração necessárias à execução dos serviços previstos.
		1.8	Os serviços gerenciados de segurança da informação a serem prestados pelo SOC SEFAZ BA são identificados a seguir e descritos em detalhe ao longo deste Termo de Referência.
2	SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO	2.1	GERENCIAMENTO TÉCNICO: serviço de gerenciamento técnico dos serviços, da equipe técnica alocada e soluções de TI fornecidas e/ou administradas pela CONTRATADA para atender este Termo de Referência, de acordo com os Níveis Mínimos de Serviços definidos.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		2.2	MONITORAMENTO DE EVENTOS DE SEGURANÇA: serviço de monitoramento e triagem dos eventos de segurança da informação no ambiente da SEFAZ BA, administrando, suportando e operando a ferramenta de SIEM fornecida conforme este Edital, de acordo com os Níveis Mínimos de Serviços definidos neste Termo de Referência.
		2.3	RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO: serviço de resposta aos incidentes de segurança da informação, assim como a orientação, execução, acompanhamento e validação das ações de mitigação e remediação necessárias junto a Equipe Técnica-SEFAZ BA.
		2.3.1	A responsabilidade da execução das ações de mitigação e remediação depende de quem é responsável pelo gerenciamento e administração do(s) ativo(s) a serem ajustado(s) e deve ser conforme descrito na definição do escopo do serviço gerenciado de segurança: RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.
		2.4	GERENCIAMENTO DE VULNERABILIDADES: Serviço de identificação, avaliação e correção de falhas de segurança em dispositivos, redes e aplicações de modo a reduzir os riscos de ataques cibernéticos e violações.
		2.4.1	A responsabilidade da execução da correção das falhas de segurança depende de quem é responsável pelo gerenciamento e administração do(s) ativo(s) com vulnerabilidade(s) e deve ser conforme descrito na definição do escopo do serviço gerenciado de segurança: GERENCIAMENTO DE VULNERABILIDADES.
		2.5	GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA: serviço de administração, configuração, manutenção, monitoramento, operação e suporte técnico às soluções de segurança existentes e integradas ao ambiente da SEFAZ BA.
3	PLATAFORMA DE SEGURANÇA	3.1	PLATAFORMA DE SEGURANÇA: projetada para integrar visibilidade, análise e controles de segurança em uma variedade de camadas de segurança e fontes de dados, aprimorando a proteção, a escalabilidade e o desempenho. Para fins deste Termo de Referência, as soluções de segurança identificadas nos itens abaixo integram a Plataforma de Segurança da SEFAZ BA a ser gerenciada e sustentada pela EquipeSOC.
		3.1.1	A PLATAFORMA DE SEGURANÇA na SEFAZ BA, escopo deste Termo de Referência, é composta das seguintes soluções de segurança e serviços associados:
		3.1.1.1	EPP - Endpoint Protection
			Trellix - EPO e Endpoint Security
Karpesky			
			MS Defender for Endpoint



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		3.1.1.2	Antispam Mail Inspector
		3.1.1.3	Controle de Acesso à Rede ForeScout NAC
		3.1.1.4	Syslog Grafana
		3.1.1.5	IPS Trellix IPS-NS7150
		3.1.1.6	Firewall Fortinet FortiGate NGFW Cisco ASA
		3.1.2	Outras soluções de segurança fornecidas pela CONTRATADA para atender a este Termo de Referência, como por exemplo, a solução de " Gerenciamento de eventos e informações de segurança (SIEM) " e a solução de Avaliação de Vulnerabilidades , também fazem parte da Plataforma de Segurança.
		4	PAINEL DE MONITORAMENTO
4.2	Os dados publicados no Painel de Monitoramento devem poder ser exportados em formato CSV e TXT.		
5	ESTRUTURA FÍSICA - SOC	5.1	O Centro de Operações de Segurança (SOC) deve ser estruturado no ambiente providenciado pela CONTRATADA e atender aos seguintes requisitos mínimos
		5.1.1	Estar localizado fisicamente em território nacional;
		5.1.2	Utilizar sistema de gerenciamento de CFTV, que viabilizem o monitoramento de pessoas, equipamentos e sistemas relacionadas ao contrato da SEFAZ BA e cujas imagens possam ser recuperadas por no mínimo 90 (noventa) dias;
		5.1.3	Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC por no mínimo 90 dias;
		5.1.4	Possuir solução de monitoramento de disponibilidade e desempenho de seus ativos de TIC e de subsistemas;
		5.1.5	O perímetro deve ser protegido contra intrusão e acesso indevido;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		5.1.6	Ser vigiado fisicamente de forma ininterrupta por segurança especializada em regime de 24x7x365;
		5.1.7	Ter controle de acesso físico com pelo menos 2 (dois) fatores de autenticação;
		5.1.8	Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços. Deve ter conexão com a Internet através de pelo menos 2 (dois) prestadores de serviço à Internet.
		5.1.9	Ter sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e UPSs (unidades de alimentação elétrica contínua) para garantir a transição entre o fornecimento normal de energia e o grupo gerador;
		5.1.10	Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
		5.1.11	Deverá possuir processos implementados que garantam a segurança das informações da SEFAZ BA, em conformidade com a norma ABNT NBR ISO/IEC 27001;
6	AUDITORIA	6.1	A SEFAZ BA poderá realizar auditoria nas instalações do Centro de Operações de Segurança (SOC), SOC REMOTO, com o objetivo de verificar as instalações físicas, a segurança física e lógica do ambiente e outros aspectos envolvidos, além dos demais itens exigidos neste Termo de Referência.
7	SISTEMA DE TICKETS	7.1	A CONTRATADA deve fornecer e administrar um Sistema de Tickets necessária à execução dos serviços previstos conforme descrito neste Termo de Referência
		7.2	O Sistema de Tickets deve estar implantado nas instalações da CONTRATADA e será utilizado pelas equipes EquipeSOC e EquipeSEFAZ BA na execução dos serviços e atividades associadas.
		7.2.1	O acesso ao Sistema de Tickets deve ser via WEB, https, e utilizando browsers padrões de mercado Chrome, Firefox e Edge.
		7.3	Deverão ser garantidos a disponibilidade, a integridade, a confidencialidade, a irretratibilidade e a autenticidade das informações da SEFAZ BA que se encontrarem sob custódia do prestador de serviços.
		7.3.1	O acesso e uso de ferramentas de auditoria que interajam com os sistemas de informação do CONTRATANTE deverão estar devidamente segmentados e restritos para evitar comprometimentos e uso indevido de dados de log
		7.4	A solução deve estar disponível em regime 24x7 (24 horas por dia, 7 dias por semana) com disponibilidade mínima de 99,7%.
		7.4.1	A solução deverá manter backup diário por 7 dias, 4 semanais por 30 dias, 12 mensais por 1 ano e 5 anuais por 5 anos, qualquer



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		restauração/recuperação necessária não deve envolver custos a CONTRATANTE
7.5		O Sistema de Tickets deve suportar o registro e procedimentos para triagem e tratamento de eventos e incidentes de segurança da informação, de forma garantir um tratamento de incidentes de segurança de forma completa e ágil.
7.6		O Sistema de Tickets deve suportar a abertura automática de tickets de eventos e incidentes de segurança a partir de integração com a ferramenta de SIEM fornecida conforme descrito neste Termo de Referência.
7.7		O Sistema de Tickets deve prover logs de auditoria que registrem atividades de acesso de usuários privilegiados, tentativas de acesso autorizados e não autorizados, exceções do sistema e eventos de segurança da informação devem ser mantidos em conformidade com as políticas e regulamentos aplicáveis e serem comunicados para a CONTRATANTE.
7.7.1		Disponibilizar meios de replicação de logs de auditoria em formato txt e csv para que o CONTRATANTE possa armazenar cópias de segurança destas informações para futuras consultas e auditorias.
7.8		O Sistema de Tickets da CONTRATADA deverá sempre estar com o horário sincronizado com a ferramenta de SIEM, para correta emissão dos relatórios que serão utilizados na conferência dos indicadores definidos neste Termo de Referência.
7.9		O Sistema de Tickets deve permitir a exportação, em formato CSV e TXT, dos dados associados aos tickets abertos vinculados a execução dos serviços previstos neste Termo de Referência.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.2. SERVIÇO - GERENCIAMENTO TÉCNICO

ESPECIFICAÇÃO TÉCNICA			
1	ESCOPO	1.1	GERENCIAMENTO TÉCNICO: serviço de gerenciamento técnico dos serviços, da equipe técnica alocada e soluções de TI fornecidas e/ou administradas pela CONTRATADA atendendo os requisitos descritos neste Termo de Referência e de acordo com os Níveis Mínimos de Serviços (NMS) definidos.
		1.1.1	Faz parte do escopo o gerenciamento técnico dos serviços, da equipe técnica alocadas e atividades previstas nas ETAPA IMPLANTAÇÃO DO SOC e OPERAÇÃO DOS SERVIÇOS.
		1.2	A CONTRATADA deverá disponibilizar um profissional dedicado, GESTOR TÉCNICO, que será o responsável pelo GERENCIAMENTO TÉCNICO e o ponto de contato formal da CONTRATADA com a CONTRATANTE no que se refere a execução dos serviços previstos neste Termo de Referência.
		1.2.1	O conceito de dedicado é "estar à disposição da SEFAZ BA quando acionado", não significa EXCLUSIVIDADE.
		1.3	Todas as ações do GESTOR TÉCNICO devem ser acordadas e reportadas a SEFAZ BA, através da Gerência da Segurança da Informação (DTI/GSINF).
		1.4	Para o controle e administração dos serviços realizados pela CONTRATADA, a DTI/GSINF indicará representantes autorizados a interagir com ela. Estes representantes serão responsáveis por atividades como, entre outras:
		1.4.1	Definir as estratégias, políticas e regras a serem implantadas, e analisar os relatórios gerados pelos softwares que compõem a solução;
		1.4.2	Auxiliar nas providências necessárias em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência).
		2	EQUIPE TÉCNICA
2.2	Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ou certificações oficiais válidas e ativas, conforme os requisitos específicos para o perfil profissional descritos no ENCARTE D - PERFIL PROFISSIONAL		
3	HORÁRIO DE OPERAÇÃO	3.1	O serviço GERENCIAMENTO TÉCNICO deverá ser prestado no período das 08:00 às 18:00 horas, de segunda à sexta-feira, podendo ser de forma presencial nas dependências da SEFAZ BA, SOC (LOCAL), ou nas dependências da CONTRATADA, SOC (REMOTO).
		3.2	Durante a cobertura desta janela de horário, o GESTOR TÉCNICO deve estar alocado e disponível, atuando na gestão e acompanhamento dos serviços contratados e pronto para ser acionado/demandado de forma imediata conforme necessidade das equipes técnicas EquipeSOC e EquipeSEFAZ BA.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		3.3	Em situações excepcionais, o GESTOR TÉCNICO poderá ser acionado fora dos horários previstos nesta janela, para atuar e/ou auxiliar as equipes técnicas EquipeSOC e EquipeSEFAZ BA na resolução de incidentes e problemas de segurança cibernética.
4	ATIVIDADES PREVISTAS	4.1	Garantir a qualidade dos serviços e informações prestadas, em conformidade com as melhores práticas em termos de segurança da informação e gestão de serviços de TI (ITIL), e de acordo com os Níveis Mínimos de Serviço (NMS) determinados neste Termo de Referência.
		4.1.1	Assegurar que os processos operacionais tenham melhoria contínua e atendam aos Indicadores e metas acordadas em contrato;
		4.1.2	Realizar auditorias dos atendimentos dos eventos e incidentes cibernéticos e tickets realizados pelos perfis profissionais da Equipe SOC, com o objetivo de avaliar e aferir a observância aos padrões, procedimentos e qualidade do serviço prestado, bem como o cumprimento dos scripts, playbooks, padrões de cordialidade e empatia exigidos.
		4.2	Coordenar tecnicamente os profissionais da Equipe Técnica-SOC na execução de suas atividades e nas ações conjuntas com a Equipe SEFAZ BA, garantindo a aplicação das melhores práticas de segurança e o cumprimento de Normas de Segurança da Informação da SEFAZ BA, Política de Segurança da Informação do Estado da Bahia e outros procedimentos vigentes ou que venham a ser criados.
		4.4.1	Orientar e apoiar a atuação da EquipeSOC em situações críticas de trabalho;
		4.4.2	Priorizar os atendimentos críticos, conforme definição e solicitação da SEFAZ BA.
		4.3	Estruturar a EquipeSOC para atuar nos serviços previstos neste Termo de Referência.
		4.3.1	Definir plano de treinamento inicial e contínuo dos profissionais que executam os serviços;
		4.3.2	Organizar a alocação de turnos e de profissionais da EquipeSOC;
		4.3.3	Participar da seleção da EquipeSOC para os casos de reposição de profissionais.
		4.4	Realizar a interface com a EquipeSEFAZ BA e a orquestração entre todos os serviços que são escopo deste Termo de Referência e de eventuais serviços prestados por terceiros cujo uso se faça necessário para atender os objetivos desta contratação.
		4.5	Elaborar e implantar metodologias, processos, procedimentos e instruções associados ao Monitoramento de Eventos, Resposta a Incidentes de Segurança da Informação, Gerenciamento de Vulnerabilidades e Gerenciamento da Plataforma de Segurança (SIEM, NAC, IPS, Firewall, EDR, EPP, etc.).
		4.5.1	Verificar, reportar e garantir o cumprimento destas metodologias, processos, procedimentos e instruções pela sua equipe técnica;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		4.5.2	Verificar e reportar e garantir o cumprimento destas metodologias, processos, procedimentos e instruções pelas áreas vinculadas à DTI ou à outras unidades da SEFAZ BA, quando couber.
		4.6	Apresentar sugestões e atuar na elaboração e melhoria contínua de procedimentos sistematizados e da base de conhecimentos, contemplando todos serviços, processos e soluções de segurança objetos desta contratação.
		4.6.1	Consolidar todas as soluções adotadas na execução das atividades em manuais de procedimentos e em base de conhecimento.
		4.7	Apoiar e participar na implementação dos processos bem como na mensuração dos indicadores de objetivos instituídos pelo CONTRATANTE.
		4.8	Sugerir novas tecnologias para modernizar o ambiente tecnológico, buscando subsidiar a equipe da CONTRATANTE na Gerenciamento de Eventos, Gerenciamento de Vulnerabilidades, Resposta a Incidentes de Segurança da Informação e Gestão de Serviços e Ativos de Segurança (SIEM, NAC, IPS, Firewall, EDR, EPP, etc.)
		4.9	Elaborar e propor plano de execução dos serviços, de acordo com as Ordens de Serviço (OSs) emitidas pela CONTRATANTE.
		4.10	Fornecer relatórios técnicos e gerenciais suficientes para que o fiscal do contrato tenha condições de aferir a realização dos serviços.
5	RELATÓRI O GERENCIAL	5.1	O GESTOR TÉCNICO deverá elaborar mensalmente RELATÓRIO GERENCIAL referente aos serviços prestados, apresentando-o à CONTRATANTE, até o 5o (quinto) dia útil do mês subsequente ao da prestação dos serviços.
		5.2	O RELATÓRIO GERENCIAL MENSAL deve apresentar, entre outras, as seguintes informações:
		5.2.1	Comprovação da execução de todos os serviços objetos desta contratação;
		5.2.2	Painel de volumetria de chamados (requisições de serviço, incidentes, problemas, etc.) divididos por grupos solucionadores e responsáveis, demonstrando graficamente a evolução destas informações;
		5.2.3	Os indicadores e níveis de serviços alcançados em relação ao previsto no Níveis Mínimos de Serviço (NMS);
		5.2.4	Os indicadores e níveis de serviços não alcançados em relação ao previsto no Níveis Mínimos de Serviço (NMS) e glosas associadas;
		5.2.4.1	Apresentar a volumetria de incidentes, problemas e requisições em backlog (incidentes e requisições de serviço em aberto e fora dos Níveis Mínimos de Serviço (NMS) previsto -"estourado") e sugestões para saneamento e redução desta base;
		5.2.5	Manutenções evolutivas e corretivas realizadas, em execução e propostas;
		5.2.7	Erros operacionais ocorridos e plano de ação para evitá-los no futuro;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

5.2.8	Demais informações relevantes para as atividades demandadas e controle da operação;
5.2.9	Estatísticas sobre Eventos de Segurança da Informação: volumetria, tipificação e outros dados associados aos eventos de segurança tratados nas soluções da PLATAFORMA DE SEGURANÇA;
5.2.10	Estatísticas sobre Incidentes de Segurança: volumetria, tipificação e outros dados associados aos incidentes de segurança identificados;
5.2.10.1	Relatório Executivo (RE), com o resumo gerencial dos incidentes encontrados;
5.2.10.2	Relatório Técnico (RT), com os detalhes completos dos incidentes encontrados e com as informações sobre as correções ou mitigações deles;
5.2.10.3	Relatório de Tendências (RTend), que mostre, de forma comparativa, a evolução do nível de detecção e resposta dadas aos alertas, eventos e incidentes cibernéticos no ambiente cibernéticos da SEFAZ BA;
5.2.11	Estatísticas sobre Endpoint Protection: volumetria, tipificação e outros dados associados ao tratamento de malware (vírus, worms, trojan horses, spyware etc.);
5.2.12	Estatísticas sobre Vulnerabilidades: volumetria, tipificação e outros dados associados a vulnerabilidades de segurança encontradas em ativos, aplicativos e serviços de TI;
5.2.12.1	As vulnerabilidades devem ser classificadas, organizadas e com sugestão de priorização para eliminação ou mitigação;
5.2.13	Relatório de análise e diagnóstico das causas (causa raiz) dos top 10 incidentes e problemas de segurança da informação ocorridos;
5.2.14	Proposta de no mínimo 5 (cinco) sugestões de melhorias para os serviços, processos e soluções sob sua responsabilidade, bem como submeter em detalhes os respectivos planos para sua adoção e reportar sua evolução nos relatórios gerenciais subsequentes;
5.2.15	Apresentar ao menos 5 (cinco) ações para otimizar a ingestão, triagem e alertas gerados a partir de eventos coletados no ambiente durante o período mensal a que se refere o relatório gerencial de serviços;
5.3	O GESTOR TÉCNICO realizará reuniões mensais, nas dependências da SEFAZ BA, para dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos e revisão das configurações e procedimentos implementados;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.3. SERVIÇO - MONITORAMENTO DE EVENTOS DE SEGURANÇA

ESPECIFICAÇÃO TÉCNICA			
1	ESCOPO	1.1	MONITORAMENTO DE EVENTOS DE SEGURANÇA: O serviço tem por objetivo a realização de atividades especializadas de monitoramento e triagem dos eventos de segurança da informação atendendo os requisitos descritos neste Termo de Referência e de acordo com os Níveis Mínimos de Serviços definidos.
		1.1.1.	A CONTRATADA será responsável por implantar e operar um processo de "Monitoramento de Eventos de Segurança", que estabelece os fluxos de tratamento e resposta a eventos de segurança, permitindo uma gestão capaz de supervisionar e operacionalizar as ações necessárias à apuração dos eventos e os meios de respostas adequadas a cada situação.
2	EQUIPE TÉCNICA	2.1	Cabe a CONTRATADA a estruturação, administração e supervisão da equipe técnica responsável pelo serviço de MONITORAMENTO DE EVENTOS DE SEGURANÇA: EquipeSOC de MONITORAMENTO DE EVENTOS.
		2.1.1	O dimensionamento da equipe técnica deve ser em quantitativo que garanta o seu funcionamento no horário de operação definido neste Termo de Referência, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados.
		2.1.1.1	A EquipeSOC de MONITORAMENTO DE EVENTOS não precisa ter dedicação exclusiva à prestação dos serviços objeto deste Termo de Referência.
		2.1.1.2	Considerando o horário de operação, ausências eventuais e programação de férias, a EquipeSOC de MONITORAMENTO DE EVENTOS deve ter no mínimo 2 (dois) profissionais previstos por turno de prestação do serviço de "Monitoramento de Eventos de Segurança".
		2.1.2	A capacitação técnica e experiência da equipe técnica deve garantir a qualidade dos serviços e informações prestadas, atuando conforme o estado da arte e melhores práticas em termos de Segurança da Informação, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados neste Termo de Referência.
		2.1.3	Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ou certificações oficiais válidas e ativas, conforme os requisitos específicos para o perfil profissional descritos no ENCARTE D - PERFIL PROFISSIONAL
		2.1.4	A EquipeSOC de MONITORAMENTO DE EVENTOS deve ser alocada no SOC (REMOTO), localizado nas instalações da CONTRATADA.
3	HORÁRIO DE OPERAÇÃO	3.1	O serviço MONITORAMENTO DE EVENTOS DE SEGURANÇA deverá ser prestado de forma ininterrupta, em regime 24x7x365 (24 horas por dia, 7 dias por semana, todos os dias do ano).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

4	SISTEMA DE TICKETS	3.1	A CONTRATADA deverá possuir Sistema de Tickets próprio para registro, controle e triagem dos eventos gerados pela ferramenta de SIEM e/ou soluções da Plataforma de Segurança.
		3.1.1	O Sistema de Tickets da CONTRATADA deverá registrar todas as evidências encontradas no tratamento dos eventos.
		3.1.2	O Sistema de Tickets da CONTRATADA deverá registrar todas as informações necessárias para a emissão dos relatórios de indicadores associados ao serviço de Monitoramento de Eventos de Segurança
5	ATIVIDADES PREVISTAS	5.1	A CONTRATADA será responsável pelas atividades de monitoramento e triagem dos eventos de Segurança da Informação atendendo os requisitos descritos neste Termo de Referência:
		5.1.1	Análise dos eventos de segurança da informação registrados na ferramenta de SIEM e nas soluções de segurança da informação integradas ao ambiente de TI da SEFAZ BA, realizando a triagem dos verdadeiros positivos e falsos positivos;
		5.1.2	Cada evento de segurança alertado na ferramenta de SIEM e/ou nas soluções de segurança da informação integradas ao ambiente de TI da SEFAZ BA, deverá gerar, automaticamente, um novo chamado no Sistema de Tickets da CONTRATADA como evento de segurança a ser tratado;
		5.1.3	Este evento de segurança também deve ser registrado, de forma automática, no Sistema ITSM da SEFAZ BA.
		5.2	Linha de Base: Definição de linha de base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção;
		5.2.1	Revisão da linha de base de eventos de segurança monitorados de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera 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 a SEFAZ BA, sejam detectados através dos serviços em questão;
		5.2.2	Uma vez definida a linha de base, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta;
		5.3	Triagem e Categorização de eventos: os tíquetes registrados devem ser priorizados por categorias, unificando os eventos potenciais de incidentes com as características em comum, que podem receber tratamento padronizado.
		5.4	Análise de eventos: onde o analista deve pesquisar informações adicionais que podem estar relacionadas ao evento em análise, que forneçam algum valor investigativo para identificar comportamentos anômalos ou maliciosos. A análise realizada nessa etapa é preliminar, tendo o objetivo de confirmar a ocorrência de um evento de segurança, eliminando falsos positivos confirmados;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

5.4.1	Detecção por análise de logs, onde o analista realiza pesquisas, revisões e análises estatísticas no histórico de log armazenado nas soluções de segurança disponibilizadas pela SEFAZ BA e/ou CONTRATADA utilizadas pelo SOC, com o objetivo de identificar comportamentos e evidências que indiquem atividades maliciosas ou novas ameaças. A lógica de detecção deve ser ajustada e desenvolvida, podendo passar a utilizar múltiplos eventos e diferentes fontes de dados;
5.4.2	Definir a prioridade dos eventos considerados como verdadeiros positivos de acordo com escala de criticidade definida pela SEFAZ BA.
5.5	Incidente de Segurança: Na análise dos eventos de segurança quando constatado se tratar de um incidente de segurança, escalar para a equipe EquipeSOC de RESPOSTA A INCIDENTES, por meio da abertura um novo chamado no Sistema de Tickets da CONTRATADA como incidente de segurança a ser tratado.
5.5.1	O incidente aberto deve conter as instruções e informações necessárias para o devido tratamento/resposta a ser dado pela EquipeSOC de RESPOSTA A INCIDENTES;
5.5.2	Todo o processo de tratamento do evento, junto com as evidências encontradas, independente de qual etapa e/ou status, deve ser registrado no Sistema de Tickets da CONTRATADA. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso. A análise deve ser realizada com o objetivo de identificar pessoas, locais e eventos relacionados, correlacionando todas as informações reunidas e gerando como produto um laudo sobre o incidente de segurança em questão.
5.5.3	Enriquecer os dados dos eventos e incidentes cibernéticos a partir das fontes de dados especializadas disponibilizadas na internet assim como através dos dados publicados pelas soluções de segurança integradas ao ambiente de TI da SEFAZ BA: SIEM, NAC, IPS, etc.
5.5.4	As informações acima, itens 5.5.2 e 5.5.3 também devem ser registradas, de forma automática, no Sistema ITSM da SEFAZ BA.
5.6	É expressamente proibida a remoção ou alteração de qualquer evento de segurança das ferramentas, independentemente de sua classificação e fase de tratamento.
5.7	Caso a CONTRATADA identifique algum problema na geração de eventos por um item de configuração, será de reponsabilidade da CONTRATADA a correção e/ou habilitação deste problema. Caso a resolução do problema dependa de configuração por parte da SEFAZ BA, a CONTRATADA deverá solicitar e orientar a correção até que os eventos estejam sendo gerados corretamente;
5.8	Gerar painéis dinâmicos e em tempo real da situação atual de segurança da SEFAZ BA informando através de um score o nível de segurança, assim como disponibilizar relatórios referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		5.9	Solicitar e acompanhar a execução de medidas preventivas com objetivo de identificar e conter possíveis ataques e invasões aos ativos da SEFAZ.
6	SIEM - GERENCIAM ENTO E SUSTENTAÇ ÃO	6.1	Gerenciamento e sustentação da ferramenta de SIEM fornecida, conforme requisitos deste Termo de Referência, para suportar a execução do serviço Monitoramento de Eventos de Segurança.
		6.1.1.	Planejar, instalar, implementar e manter ferramenta de SIEM para automatizar e acelerar o tratamento e a resposta aos eventos e incidentes cibernéticos, quer pela implementação de solução SOAR, quer por soluções de automatização implementadas manualmente, desde que garanta a automação e a prontidão das respostas aos eventos e incidentes cibernéticos e não acrescentem custos adicionais para a CONTRATANTE.
		6.1.2.	A ferramenta de SIEM fornecida e gerenciada pela CONTRATADA deve ter contrato de suporte técnico vigente junto ao fabricante da solução durante todo o período de execução do serviço Monitoramento de Eventos de Segurança.
		6.2	Apresentar um conjunto inicial de, no mínimo, 100 (cem) regras ou 30 (trinta) modelo de ameaças de correlação especializadas na detecção de incidentes de segurança, que serão produzidas, configuradas na ferramenta de SIEM, suportadas e atualizadas pelo fabricante da solução ou pela CONTRATADA. As regras só serão ativadas após a aprovação da SEFAZ
		6.2.1	Mensalmente devem ser sugeridas e acrescentadas no mínimo 10 (dez) regras de correlação conforme descrito acima.
		6.3	Sugerir e configurar proativamente novas regras de correlacionamento, baseadas em boas práticas de segurança e bases de conhecimento próprias, customizadas para o ambiente da SEFAZ, monitorando minimamente:
		6.3.1	Detecção de anomalias de comportamento com base em alterações em uma linha de base;
		6.3.2	Detecção de anomalias de comportamento baseado em estatísticas (StatisticalBehavioralAnalysis);
		6.3.3	Detecção de anomalias com base em tendências (Trend BehaviorAnalysis);
		6.3.4	Detecção de padrões em logs observados e não observados;
		6.3.5	Detecção de padrões baseados em uma sinalização específica (thresholds);
		6.3.6	Detecção de padrões baseados em valores unitários;
		6.3.7	Detecção de ameaças que saem de normas básicas (whitelisting);
		6.4	Aprimorar a coleta e a triagem dos logs gerenciados, bem como da construção de alertas e dashboards na ferramenta de SIEM fornecida. As informações advindas de outras fontes, como por exemplo, as geradas pelo Serviço de Gerenciamento de Vulnerabilidades e por outras soluções de segurança, também devem ser utilizadas para esse fim. A integração dessas fontes de informações deve ser alinhada com a SEFAZ BA (GSINF).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		6.5	Propor ajustes nos controles de detecção e prevenção existentes ou novos controles desses tipos para prevenir novos ataques e para diminuir o tempo de detecção e resposta aos mesmos
		6.6	Desenvolver automatização para registro de eventos e criação de regras de bloqueio e de segurança.
		6.6.1	Automatizar as atividades em relação à detecção e bloqueios de IoCs em ferramentas como firewall, web application firewall (WAF), entre outros; independentemente da PLATAFORMA DE SEGURANÇA administrada.
		6.7	A CONTRATADA deve manter as regras atualizadas, de modo a refletir a ocorrência de novas ameaças, novas políticas de alarme, atualizações de padrões de logs de tecnologias, escopo monitorado ou para reduzir a ocorrência de falsos positivos;
		6.8	A SEFAZ BA pode solicitar, a qualquer momento, a implementação de regras de correlacionamento a serem implementadas na ferramenta de SIEM, baseadas na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar as regras na ferramenta. As solicitações devem ser registradas e realizadas por meio dos canais estabelecidos neste Termo de Referência.
7	OUTRAS SOLUÇÕES DE SEGURANÇA DE INFORMAÇÃO	7.1	Caso as ferramentas de propriedade da SEFAZ BA não atendam a completa execução dos serviços objeto da presente contratação a CONTRATADA poderá adotar solução tecnológica complementar em termos de hardware e software;
		7.1.1	A CONTRATADA poderá utilizar soluções de hardware e software proprietárias desde que previamente autorizadas pela SEFAZ BA, arcando a CONTRATADA com todos os custos diretos e indiretos inerentes a utilização de solução tecnológica e seus licenciamentos necessários;
		7.2	Monitorar de forma permanente e avaliar criticamente os produtos e serviços de segurança da SEFAZ BA, sugerindo mudanças em configurações que possam beneficiar o processo de coleta e monitoramento dos eventos de segurança;
8	PLAYBOOKS	8.1	A CONTRATADA deverá apresentar um conjunto inicial de no mínimo 50 (cinquenta) playbooks para serem implementados na etapa de implantação do serviço.
		8.1.1	A SEFAZ BA pode solicitar, a qualquer momento, a implementação de novos playbooks, limitado a 10 (dez) novos playbooks por ano de contrato, para suportar e agilizar a prestação dos serviços associados.
		8.2	A CONTRATADA deverá apresentar um conjunto inicial de, no mínimo, 10 playbooks de remediação automatizados especializados na resposta de eventos/incidentes de segurança, que serão produzidas, configuradas na ferramenta de remediação, suportados e atualizados pelo fabricante da solução ou pela CONTRATADA. Os playbooks só serão ativados após a aprovação da SEFAZ;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		8.2.1	A SEFAZ BA pode solicitar, a qualquer momento, a implementação de novos playbooks de remediação automatizados, limitado a 10 novos playbooks por ano de contrato, a serem implementados na ferramenta de remediação, baseados na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar a criação dos playbooks na ferramenta. As solicitações devem ser registradas e realizadas por meio dos canais de suporte estabelecidos neste edital;
		8.3	É de responsabilidade da Equipe SOC - RESPOSTA A INCIDENTES (N2) atualizar os playbooks para os evento e incidentes cibernéticos tratados no MONITORAMENTO DE EVENTOS e RESPOSTA A INCIDENTES (N1 e N2), de modo que estas equipes possam utilizar os playbooks atualizados;
9	PROCEDIMENTOS ASSOCIADOS	9.1	Tratar os eventos de acordo com os playbooks definidos
		9.2	Sugerir melhorias nos playbooks e alterações em regras e controles de prevenção e detecção, quando for o caso.
		9.3	Gerar relatórios técnicos e executivos dos eventos e incidentes cibernéticos.
		9.4	Encerrar os eventos após sua solução.
10	MELHORIA CONTÍNUA	10.1	Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação da SEFAZ BA, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
		10.2	Sugerir medidas preventivas com objetivo de identificar e conter possíveis ataques e invasões aos ativos da SEFAZ BA.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.4. SERVIÇO - RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

ESPECIFICAÇÃO TÉCNICA			
1	ESCOPO DO SERVIÇO	1.1	RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO - O serviço tem por objetivo a realização de atividades especializadas de Resposta a Incidentes de Segurança da Informação, de acordo com os requisitos definidos neste Termo de Referência.
		1.2	A CONTRATADA será responsável por estruturar, implantar e operar um processo de Resposta a Incidentes de Segurança da Informação, que estabelece os fluxos de tratamento e resposta a incidentes de segurança da informação no ambiente de TI da SEFAZ BA, permitindo uma gestão capaz de supervisionar e operacionalizar as ações necessárias à apuração dos incidentes e os meios de respostas adequadas a cada situação.
		1.2.1	O Processo de Resposta a Incidentes de Segurança da Informação a ser estruturado e implantado, e aprovado pela SEFAZ BA, deve ser compatível com as práticas, recomendações e frameworks do NIST (National Institute of Standards and Technology), SANS Institute, ITIL (Framework Information Technology Infrastructure Library) V4 e políticas, normas e processos vigentes na SEFAZ BA.
		1.3	As atividades associadas a execução do serviço de RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO serão estabelecidas e detalhadas no processo de Resposta a Incidentes de Segurança da Informação a ser estruturado e implantado conforme definido neste Termo de Referência, incluem:
		1.3.1	A Equipe Técnica de RESPOSTA A INCIDENTES será responsável pelas atividades de resposta aos incidentes de segurança da informação, assim como a orientação, execução, acompanhamento e validação das ações de mitigação e remediação necessárias junto a Equipe Técnica-SEFAZ BA.
		1.3.1.1	A responsabilidade da execução das ações de mitigação e remediação depende de quem é responsável pelo gerenciamento e administração do(s) ativo(s) a serem ajustado(s) : - Nos ativos gerenciados pela Central de Serviços - TI da SEFAZ BA, esta é a responsável pelas ações de mitigação e remediação que devem ser indicadas, acompanhadas e validadas pela CONTRATADA; - Nos ativos gerenciados pela CONTRATADA, como as soluções da PLATAFORMA DE SEGURANÇA, as ações de mitigação e remediação são responsabilidade da CONTRATADA.
		2	EQUIPE TÉCNICA - RESPOSTA A INCIDENTES (N1 E N2)
2.2	A capacitação técnica e experiência da equipe técnica deve garantir a qualidade dos serviços e informações prestadas, atuando conforme o estado da arte e melhores práticas em termos de segurança da informação, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados neste Termo de Referência.		



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

	2.3	Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ou certificações oficiais válidas e ativas, conforme os requisitos específicos para o perfil profissional descritos no ENCARTE D - PERFIL PROFISSIONAL
EQUIPE TÉCNICA - RESPOSTA A INCIDENTES (N1)	2.4	O dimensionamento da EquipeSOC de RESPOSTA A INCIDENTES (N1) deve ser em quantitativo que garanta o seu funcionamento no horário de operação definido neste Termo de Referência, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados.
	2.4.1	A EquipeSOC de RESPOSTA A INCIDENTES (N1) não precisa ter dedicação exclusiva à prestação dos serviços objeto deste Termo de Referência.
	2.4.2	Considerando o horário de operação, ausências eventuais e programação de férias, a EquipeSOC de RESPOSTA A INCIDENTES (N1) deve ter no mínimo 2 (dois) profissionais previstos por turno de prestação do serviço de RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO (N1).
	2.5	A EquipeSOC de RESPOSTA A INCIDENTES (N1) deve ser alocada no SOC (REMOTO), localizado nas instalações da CONTRATADA.
	2.6	Considerando a sinergia entre os serviços e sem prejuízo na execução dos mesmos, conforme especificado neste Termo de Referência, os profissionais da EquipeSOC de RESPOSTA A INCIDENTES (N1) podem ser responsáveis também pelo serviço de MONITORAMENTO DE EVENTOS DE SEGURANÇA.
	EQUIPE TÉCNICA - RESPOSTA A INCIDENTES (N2)	2.7
2.8		A EquipeSOC de RESPOSTA A INCIDENTES (N2) deve ser alocada no SOC (LOCAL), localizado nas instalações da SEFAZ BA.
2.9		A EquipeSOC de RESPOSTA A INCIDENTES (N2) deve funcionar no horário de operação definido neste Termo de Referência, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados.
2.10		As EquipesSOC - RESPOSTA A INCIDENTES, N1 e N2, devem atuar de forma integrada, com o N1 atuando nos incidentes de menor criticidade e/ou complexidade conforme playbooks definidos e o N2 atuando nos incidentes de maior criticidade e/o complexidade.
2.11		Cabe a EquipeSOC de RESPOSTA A INCIDENTES (N2) supervisionar e apoiar o trabalho da equipe N1, atuando também na estruturação e melhoria do processo de RESPOSTA A INCIDENTES e do ambiente de TI da SEFAZ BA na prevenção e proteção de ataques cibernéticos.
2.12		A Equipe SOC de RESPOSTA A INCIDENTES (N2) também será responsável pelo serviço de GERENCIAMENTO DE VULNERABILIDADE, conforme descrito neste Termo de Referência. Desta forma, a EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES e a EquipeSOC de RESPOSTA A INCIDENTES (N2) são a mesma equipe.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

3	HORÁRIO DE OPERAÇÃO	3.1	A EquipeSOC de RESPOSTA A INCIDENTES (N1) deve prestar serviço de forma interrupta, em regime 24x7x365 (24 horas por dia, 7 dias por semana, todos os dias do ano).
		3.2	A EquipeSOC de RESPOSTA A INCIDENTES (N2) vai operar em regime comercial de 08:00 às 18:00h, de segunda à sexta-feira, exceto feriados.
		3.3	Em situações excepcionais, a EquipeSOC de RESPOSTA A INCIDENTES (N2) poderá ser acionado fora dos horários previstos nesta janela, para atuar e/ou auxiliar as equipes técnicas EquipeSOC e EquipeSEFAZ BA na resolução de incidentes e problemas de segurança cibernética.
4	SISTEMA DE TICKETS	4.1	A CONTRATADA deverá possuir sistema de Tickets próprio para registro e controle dos incidentes de segurança da informação identificados de forma isolada ou a partir dos eventos gerados pela ferramenta de SIEM e/ou soluções de segurança da informação.
		4.1.1	O Sistema de Tickets da CONTRATADA deverá sempre estar com o horário sincronizado com a ferramenta de SIEM, para correta emissão dos relatórios que serão utilizados na conferência dos indicadores indicados neste Termo de Referência.
		4.1.2	O Sistema de Tickets da CONTRATADA deverá registrar todas as informações necessárias para a emissão dos relatórios de indicadores associados ao serviço de RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.
5	RESPOSTA A INCIDENTES DE SEGURANÇA - ATIVIDADES PREVISTAS	5.1	As atividades associadas a execução deste serviço serão revistas, estabelecidas e detalhadas no Processo de Resposta a Incidentes de Segurança da Informação a ser estruturado e implantado conforme definido neste Termo de Referência, mas incluem atividades como por exemplo, entre outras:
		5.2	A Equipe SOC - RESPOSTA A INCIDENTES (N1) é responsável por tratar os incidentes escalados após o processo de triagem inicial, considerando as orientações e evidências registradas pela equipe técnica de MONITORAMENTO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO.
		5.2.1	Caso um incidente de segurança seja detectado, analisar os logs, pacotes, flow e demais artefatos coletados, a fim de no primeiro instante identificar do que se trata o incidente e avaliar o seu grau de risco;
		5.2.2	Uma vez realizadas as análises iniciais do incidente, identificar quais foram os principais vetores de ataque ao ambiente da SEFAZ BA;
		5.2.3	Uma vez identificado o comportamento e os principais vetores de ataque, deverá definir uma estratégia para a mitigação e contenção do ataque em questão;
		5.2.4	O fluxo de escalção dos incidentes cibernéticos será RESPOSTA A INCIDENTES (N1), RESPOSTA A INCIDENTES (N2), GERENTE TÉCNICO e, por fim, Equipe Técnica - SEFAZ BA (GSINF). A escalção dos incidentes será baseada em critérios como criticidade, complexidade e impacto, a serem definidos previamente junto a SEFAZ BA.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

	5.2.4.1	A Equipe SOC - RESPOSTA A INCIDENTES (N1) deve escalar incidentes cibernéticos que não sejam de sua alçada de acordo com os playbooks definidos pela SEFAZ BA.
	5.3	A Equipe SOC - RESPOSTA A INCIDENTES (N1) deve:
	5.3.1	Encaminhar demandas para a CENTRAL DE SERVIÇOS DE TI (NOC e Suporte N1, N2, N3) através da abertura de tíquetes no software de ITSM da SEFAZ BA solicitando as medidas de contenção e correção necessárias, incluindo configurações nos sensores de segurança ou outros ativos.
	5.3.1.1	Atuar em harmonia com a CENTRAL DE SERVIÇOS DE TI e conforme processos e procedimentos associados e vigentes.
	5.3.1.2	Atuar no sentido de interromper um incidente quando da inoperância do NOC ou Suporte N1, N2 e N3. Para incidentes que requeiram atuação imediata e em circunstâncias onde a equipe do NOC ou suporte N1, N2, N3 não estejam disponíveis ou não possam atuar, serão pré-definidos protocolos de remediação para atuação da CONTRATADA;
	5.3.1.3	Padronização de procedimentos de resposta à incidentes, os incidentes escalados devem incluir procedimentos padronizados contendo as melhores práticas para seu tratamento e contenção, de modo que viabilize a execução das medidas corretivas necessárias pela SEFAZ;
	5.4	A Equipe Técnica-SEFAZ BA vinculada a CENTRAL DE SERVIÇOS DE TI executará as atividades necessárias, conforme processos e procedimentos internos existentes, assim como registrará as ações realizadas nos tíquetes correspondentes aos incidentes, permitindo que a CONTRATADA esteja ciente do fechamento do mesmo.
	5.4.1	A Equipe Técnica-SEFAZ BA da CENTRAL DE SERVIÇOS DE TI (NOC e Suporte N1, N2, N3) responsável pelo tratamento dos tíquetes escalados devem possuir acesso total às informações do incidente relacionado;
	5.4.2	A Equipe Técnica-SEFAZ BA da CENTRAL DE SERVIÇOS DE TI (NOC e Suporte N1, N2, N3) deve poder contatar os analistas da RESPOSTA A INCIDENTES (N1), por telefone ou via software de ITSM, para consulta de informações em caso de qualquer dúvida sobre os eventos escalados e demais procedimentos para tratamento dos incidentes. As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;
	5.5	A Equipe SOC - RESPOSTA A INCIDENTES (N1) deve, ao detectar incidentes que tenham comprometido o ambiente da SEFAZ BA, encaminhar relatório com detalhes do incidente: quando e forma com que foi concretizado, tempo de exposição, impacto e atitudes a serem tomadas. Os destinatários serão definidos posteriormente;
	5.6	A Equipe SOC - RESPOSTA A INCIDENTES (N2) é responsável por tratar os incidentes que foram escalados após análise inicial pela Equipe SOC - RESPOSTA A INCIDENTES (N1)
	5.6.1	O fluxo de escalção dos incidentes cibernéticos será RESPOSTA A INCIDENTES (N1), RESPOSTA A INCIDENTES (N2), GERENTE TÉCNICO e,



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		por fim, Equipe Técnica - SEFAZ BA (GSINF). A escalação dos incidentes será baseada em critérios como criticidade, complexidade e impacto.
		5.6.2 A Equipe SOC - RESPOSTA A INCIDENTES (N2) deve escalar incidentes cibernéticos que não sejam de sua alçada de acordo com os playbooks definidos pela SEFAZ BA.
		5.6.3 No tratamento dos incidentes sob sua responsabilidade a Equipe SOC - RESPOSTA A INCIDENTES (N2) é responsável pelas mesmas atividades que foram listadas acima para a Equipe SOC - RESPOSTA A INCIDENTES (N1)
		5.7 A Equipe SOC - RESPOSTA A INCIDENTES (N2) é responsável adicionalmente pelas seguintes atividades:
		5.7.1 Realizar a gestão dos incidentes tratados pelo N1 e N2, inclusive revisando a prioridade e a probabilidade de impacto dos incidentes tratados, o atendimento dos Níveis Mínimos de Serviço (NMS) que é atrelado à criticidade de cada incidente, entre outras métricas de desempenho dos serviços prestados pelo Centro de Operações de Segurança - SOC.
		5.7.1.1 Reclassificar eventos como falso positivo ou rever a prioridade, quando houver divergência de entendimento com relação ao definido pelas Equipes SOC de MONITORAMENTO DE EVENTOS e RESPOSTA A INCIDENTES (N1). Nesses casos, o GERENTE TÉCNICO deve ser alertado com urgência.
		5.7.1.2 Na ocorrência de eventos de alta criticidade, alertar o GESTOR TÉCNICO formalmente, o mais rapidamente possível.
		5.7.2 Propor à SEFAZ BA, a criação de novos alertas e procedimentos de tratamento de indentes para retroalimentar os processos de "Monitoramento de Eventos de Segurança" e "Resposta à Incidentes de Segurança". Essas proposições devem estar de acordo, no que couber, com a legislação e as normas técnicas aplicáveis como, por exemplo, o NIST SP 800-61 Rev.2.
		5.7.3 Solicitar bloqueios e criação de regras de segurança às equipes técnicas responsáveis pela PLATAFORMA DE SEGURANÇA, e acompanhar a conclusão das solicitações.
		5.7.4 Automatizar as atividades em relação à detecção e bloqueios de Indicators of Compromise (IOC) em soluções e serviços associados à Plataforma de Segurança - SEFAZ BA
		5.7.5 Atender acionamentos, fora da janela de atendimento, para tratamento de incidentes urgentes relacionados ao bom andamento da prestação do serviço ou que representem riscos à segurança cibernético da SEFAZ BA;
		5.7.6 Sugerir ao GESTOR TÉCNICO melhorias nos playbooks e alterações em regras e controles de prevenção e detecção quando for o caso.
6	PLAYBOOKS	6.1 A CONTRATADA deverá apresentar um conjunto inicial de no mínimo 100 playbooks para serem implementados na etapa de implantação do serviço.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		6.1.1	A SEFAZ BA pode solicitar, a qualquer momento, a implementação de novos playbooks, limitado a 10 (dez) novos playbooks por ano de contrato, para suportar e agilizar a prestação dos serviços associados.
		6.2	A CONTRATADA deverá apresentar um conjunto inicial de, no mínimo, 10 playbooks de remediação automatizados especializados na resposta de incidentes de segurança, que serão produzidas, configuradas na ferramenta de remediação, suportados e atualizados pelo fabricante da solução ou pela CONTRATADA. Os playbooks só serão ativados após a aprovação da SEFAZ BA;
		6.2.1	A SEFAZ BA pode solicitar, a qualquer momento, a implementação de novos playbooks de remediação automatizados, limitado a 10 novos playbooks por ano de contrato, a serem implementados na ferramenta de remediação, baseados na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar a criação dos playbooks na ferramenta. As solicitações devem ser registradas e realizadas por meio dos canais de suporte estabelecidos neste edital;
		6.3	É de responsabilidade da Equipe SOC - RESPOSTA A INCIDENTES (N2) atualizar os playbooks para os evento e incidentes cibernéticos tratados no MONITORAMENTO DE EVENTOS e RESPOSTA A INCIDENTES (N1 e N2), de modo que estas equipes possam utilizar os playbooks atualizados;
7	MELHORIA CONTÍNUA	7.1	Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação da SEFAZ BA, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
		7.2	Sugerir medidas preventivas com objetivo de identificar e conter possíveis ataques e invasões aos ativos da SEFAZ;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.5. SERVIÇO - GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA

ESPECIFICAÇÃO TÉCNICA			
1	PLATAFORMA DE SEGURANÇA	1.1	PLATAFORMA DE SEGURANÇA: projetada para integrar visibilidade, análise e controles de segurança em uma variedade de camadas de segurança e fontes de dados, aprimorando a proteção, a escalabilidade e o desempenho. Para fins deste Termo de Referência, as soluções de segurança identificadas nos itens abaixo integram a Plataforma de Segurança da SEFAZ BA a ser gerenciada e sustentada pela EquipeSOC.
		1.1.1	A Plataforma de Segurança - SEFAZ BA, escopo deste Termo de Referência, é composta das seguintes soluções de segurança e serviços associados:
		1.1.1.1	EPP - Endpoint Protection
			Trellix - EPO e Endpoint Security
			Karpesky
		1.1.1.2	Antispam
			Mail Inspector
		1.1.1.3	Controle de Acesso à Rede
			ForeScout NAC
		1.1.1.4	Syslog
			Grafana
		1.1.1.5	IPS
			Trellix IPS-NS7150
		1.1.1.6	Firewall
			Fortinet FortiGate NGFW
Cisco ASA			
1.2	Caso sejam adotadas pela SEFAZ BA outras soluções de segurança em substituição às soluções listadas acima em 1.1.1, as mesmas deverão ser absorvidas pela CONTRATADA como integrantes da Plataforma de Segurança - SEFAZ BA sem ônus adicionais para a CONTRATANTE.		
1.3	Outras soluções de segurança fornecidas pela CONTRATADA para atender a este Termo de Referência, como por exemplo o "Gerenciamento de eventos e informações de segurança (SIEM)" e a solução de Avaliação de Vulnerabilidades, também fazem parte da Plataforma de Segurança.		



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

2	ESCOPO	2.1	GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA - O serviço tem o objetivo de implantação, configuração, manutenção, monitoramento, operação e suporte técnico às soluções de segurança existentes e integradas ao ambiente da SEFAZ BA ou fornecidas para atender este Termo de Referência.
		2.1.1	Executar as tarefas de ativação, implantação, manutenção (corretiva e/ou evolutiva) substituição, melhoria e atualização de soluções de segurança associadas a Plataforma de Segurança da SEFAZ BA.
		2.1.2	Na execução do serviço deverão ser aplicadas as melhores práticas e recomendações associadas à segurança da informação, assim como orientações dos fabricantes das diversas soluções.
		2.2	Por iniciativa própria ou sob demanda, planejar junto com a CONTRATADA, a ativação de novos produtos, funcionalidades e recursos de segurança disponíveis nos equipamentos, softwares e serviços associados a Plataforma de Segurança da SEFAZ BA.
		2.3	As atividades vinculadas ao serviço de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA estão descritas na sequência.
3	EQUIPE TÉCNICA	3.1	Cabe a CONTRATADA a estruturação, administração e coordenação da equipe técnica responsável pelo serviço de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA: EquipeSOC de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA.
		3.1.1	O dimensionamento da equipe técnica deve ser em quantitativo que garanta o seu funcionamento no horário de operação definido neste Termo de Referência, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados.
		3.1.1.1	A EquipeSOC de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA não precisa ter dedicação exclusiva à prestação dos serviços objeto deste Termo de Referência.
		3.1.1.2	Considerando o horário de operação, ausências eventuais e programação de férias, a EquipeSOC de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA deve ter no mínimo 2 (dois) profissionais previstos por turno de prestação do serviço de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA.
		3.1.2	A capacitação técnica e experiência da equipe técnica deve garantir a qualidade dos serviços e informações prestadas, atuando conforme o estado da arte e melhores práticas em termos de segurança da informação, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados neste Termo de Referência.
		3.1.3	Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ou certificações oficiais válidas e ativas, conforme os requisitos específicos para o perfil profissional descritos no ENCARTE D - PERFIL PROFISSIONAL



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		3.1.4	A EquipeSOC de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA deve ser alocada no SOC (REMOTO), localizado nas instalações da CONTRATADA.
		3.2	A EquipeSOC de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA terá acesso às soluções de segurança implantadas na SEFAZ BA pelas quais tem a responsabilidade de sustentação e operação, garantindo o seu pleno funcionamento e integração ao ambiente de TI existente.
		3.2.1	Os perfis a serem criados devem garantir as permissões mínimas necessárias à execução das atividades pelos membros da EquipeSOC, de acordo com as responsabilidades de cada um.
		3.2.1.1	O acesso lógico aos dispositivos administrados dar-se-á por senhas individuais atribuídas a cada profissional envolvido na prestação dos serviços, jamais por senhas compartilhadas. Nos casos onde isso não for possível, as partes deverão designar profissionais para ter acesso (s) à (s) senhas, as quais devem ser trocadas de maneira segura. Caso haja descumprimento desta regra, a CONTRATADA se responsabilizará pelas consequências que porventura possam advir deste acesso.
		3.2.2	Por padrão, a EquipeSOC não deve possuir nenhum tipo de acesso a outras soluções existentes no ambiente da SEFAZ BA. Em casos específicos e por tempo determinado, caso autorizado pela Gerência de Segurança da Informação da SEFAZ, pode ser fornecido acesso de leitura a alguns ativos para auxiliar em pesquisas pontuais de eventos de segurança. Não será fornecido nenhum tipo de acesso a dados ou sistemas da SEFAZ BA, além dos estritamente necessários para a execução dos serviços previstos neste Termo de Referência
		3.3	Para as soluções de segurança fornecidas para atender este Termo de Referência, deverão ser criadas contas de usuários para que a equipe técnica da SEFAZ BA possa verificar as configurações e versões adotadas, bem como promover atividades de auditoria em geral.
4	HORÁRIO DE OPERAÇÃO	4.1	O serviço GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA deverá ser prestado no período das 08:00 às 18:00 horas, de segunda à sexta-feira, exceto feriados, de forma presencial nas dependências da CONTRATADA, SOC (REMOTO).
		4.2	Em situações excepcionais, a EquipeSOC de GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA poderá ser acionado fora dos horários previstos nesta janela, para atuar e/ou auxiliar as equipes técnicas EquipeSOC e EquipeSEFAZ BA na resolução de incidentes e problemas de segurança cibernética.
5	MONITORAMENTO	5.1	Monitorar o ambiente da SEFAZ BA a partir das soluções de segurança gerenciadas integrantes da Plataforma de Segurança identificando de forma proativa possíveis vulnerabilidades, tentativas ou ataques aos ativos da SEFAZ BA.
		5.1.1	Tomar as ações necessárias para tratamento de vulnerabilidades, eventos e/ou incidentes de segurança identificados no monitoramento.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		5.1.1.1	Abertura de tickets de eventos e/ou incidentes de segurança para as equipes responsáveis.
		5.1.1.2	Abertura de tickets de requisição de serviço para as equipes responsáveis.
		5.1.1.3	Configurações necessárias nas soluções da Plataforma de Segurança sob sua responsabilidade.
		5.2	Monitorar de forma permanente e avaliar criticamente os produtos e serviços de segurança, sugerindo mudanças em configurações que possam maximizar o funcionamento e resultados obtidos associados a cada solução de segurança assim com a integração entre estas soluções e o ambiente de TI da SEFAZ BA
		5.3	Monitorar e analisar continuamente os logs das soluções de segurança administradas para identificação e correção de problemas
		5.4	Monitorar da infraestrutura que suporta a Plataforma de Segurança e sua integração com o ambiente de TI da SEFAZ e outros que se fizerem necessários garantindo um pleno funcionamento e conformidade com os níveis de serviço acordados
		5.5	A CONTRATADA deverá colaborar ativamente nas discussões técnicas para a resolução de eventuais problemas de infraestrutura de servidores, redes, segurança, aplicações ou outros serviços de tecnologia que estejam impactando no perfeito funcionamento dos serviços de segurança administrados, em conjunto com a equipe técnica da SEFAZ BA ou outros fornecedores indicados pela SEFAZ BA;
		5.6	A CONTRATADA deverá colaborar ativamente na resolução de eventuais problemas em outros serviços de infraestrutura de servidores, redes, segurança, aplicações ou outros serviços de tecnologia que estejam impactando no perfeito funcionamento dos serviços de segurança administrados, em conjunto com a equipe técnica da SEFAZ BA ou outros fornecedores indicados pela SEFAZ BA;
		5.7	Gerar painéis dinâmicos e em tempo real da situação atual de segurança da SEFAZ BA de acordo com a visão das diferentes soluções de segurança informando através de um score o nível de segurança, assim como disponibilizar relatórios referentes aos indicadores monitorados com periodicidade mínima mensal, ou sob demanda.
		5.8	Consolidar os relatórios de atividades mensais (mês calendário), referente aos serviços e soluções associadas a Plataforma de Segurança, provendo informações gerenciais à SEFAZ BA.
6	CONFIGURAÇÃO DA PLATAFORMA DE SEGURANÇA	6.1	Avaliar, planejar e executar a configuração das funcionalidades necessárias na Plataforma de Segurança para o pleno e correto funcionamento das soluções de segurança: regras no SIEM, políticas no NAC, regras e políticas no IPS, etc.
		6.1.1	No que se refere a Plataforma de Segurança, gerenciada pela CONTRATADA, as configurações necessárias dentro das soluções (aplicação de novas regras, exclusão de regras, criação e administração de políticas, automação de respostas, tuning de



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

	performance, administração de usuários e grupos, etc.) são responsabilidade da CONTRATADA.
6.1.2	As atividades abaixo devem ser indicadas, especificadas, acompanhadas e validadas pela CONTRATADA, mas serão executadas pela Central de Serviços - TI, responsável pelo gerenciamento e administração dos ativos e infraestrutura de TI onde as configurações serão realizadas:
6.1.2.1	Instalação dos componentes das soluções de segurança e as configurações necessárias na infraestrutura de TI que suporta estas soluções de segurança, como no sistema operacional dos servidores onde estas soluções estão instaladas, na infraestrutura de rede, etc.
6.1.2.2	Aplicações de patches e hot-fixes nos componentes das soluções da Plataforma de Segurança gerenciadas e hospedadas no ambiente da SEFAZ BA.
6.1.2.2.1	As aplicações de patches e hot-fixes nos componentes das soluções de "Gerenciamento de eventos e informações de segurança (SIEM)" e de Avaliação de Vulnerabilidades ofertados e hospedados fora do ambiente da SEFAZ BA são responsabilidade da CONTRATADA e/ou fabricante no caso de soluções SaaS (Software as a Service).
6.1.2.2.2	As aplicações de patches e hot-fixes nos componentes das soluções de "Gerenciamento de eventos e informações de segurança (SIEM)" e de Avaliação de Vulnerabilidades ofertados e hospedados no ambiente da SEFAZ BA devem ser indicadas, especificadas, acompanhadas e validadas pela CONTRATADA, mas serão executadas pela Central de Serviços - TI da SEFAZ BA.
6.2	Toda e qualquer mudança na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de correções "patches", etc.) deverá ocorrer mediante autorização da SEFAZ BA, de acordo com os processos de Gestão de Serviços de TI da SEFAZ BA;
6.3	As alterações das configurações deverão ocorrer em horários determinados pela SEFAZ BA e em conformidade com o processo de Gestão de Mudanças vigente.
6.4	Implantar as melhorias solicitadas pela equipe da SEFAZ através da abertura de chamados no sistema de gestão de serviços de TI (software ITSM)
6.4.1	O tempo de atendimento das solicitações de alterações das políticas e regras feitas pela SEFAZ BA não deverá ultrapassar o SLA (acordo de nível de serviço) especificado neste documento, a contar da efetivação da solicitação;
6.5	Acionar e acompanhar o serviço de suporte técnico dos fabricantes das soluções de segurança administradas. A SEFAZ BA disponibilizará acesso ao suporte do fabricante para as soluções existentes no ambiente SEAZ/BA



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7	ATUALIZAÇÃO DA PLATAFORMA DE SEGURANÇA	7.1	Aplicar atualizações de software (melhorias, correção de problemas e atualizações de pequeno impacto) liberadas pelos fabricantes, nas soluções de segurança administradas.
		7.2	As soluções de segurança deverão ser mantidas sempre atualizados, e deverão estar com os firmwares e softwares com versão mais atual disponível no mercado, ou com a versão mais estável;
		7.3	Não poderão permanecer instaladas versões com mais do que 3 (três) meses após lançamento da última versão homologada; ou poderá permanecer instalada por tempo maior, desde que acordado com a SEFAZ BA
8	INTEGRAÇÃO COM A CENTRAL DE SERVIÇOS - TI	8.1	Elaborar scripts, manuais, roteiros, procedimentos passo-a-passo de atendimento para a Central de Serviços - TI da SEFAZ BA, associados a requisições de serviço e incidentes vinculados às soluções de segurança integrantes da Plataforma de Segurança
		8.1.1	Consolidar todas as soluções adotadas na execução das atividades em manuais de procedimentos e em base de conhecimento
		8.2	Demandar (via abertura de requisições de serviço, incidentes, problemas, ou reuniões técnicas, etc.) ao NOC ou ao Suporte N1, N2 e N3 da infraestrutura de TI da SEFAZ, medidas a serem tomadas para tratar situações mapeadas no monitoramento das soluções de segurança.
		8.2.1	Acompanhar e registrar os chamados técnicos, requisições de mudança e requisições de serviços fim-a-fim, ou seja, do momento da sua abertura até o seu encerramento, e comunicar os fiscais técnicos do CONTRATANTE em caso de problemas;
		8.2.2	Abrir chamados técnicos, inclusive na língua inglesa, junto aos provedores de serviços, parceiros e fabricantes das soluções de hardware e software da TI
		8.3	Fornecer sugestões e auxiliar na construção, manutenção e melhoria contínua, com o apoio e aprovação da SEFAZ BA, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
9	GERENCIAMENTO DO SERVIÇO	9.1	Deverão ser entregues e apresentados pelo GESTOR TÉCNICO, relatórios analíticos mensais, técnicos e executivos, para o acompanhamento do serviço contratado, contemplando, dentre outras, as seguintes informações:
		9.1.1	Visão detalhada da cobertura das soluções da Plataforma de Segurança no ambiente da SEFAZ BA, identificando minimamente os ativos cujos componentes estejam instalados, casos de exceção ou falha, % de atualização e versões de produtos.
		9.1.2	Avaliação eletrônica e manual: além das observações e notificações fornecidas pela própria solução (Hardware ou Software) nos logs e relatórios coletados, antes de ser entregue à SEFAZ BA, os relatórios finais devem ser analisados, tratados e comentados por um



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

			especialista da EquipeSOC, agregando valor às informações coletadas dos dispositivos e ambientes gerenciados;
		9.1.3	Diagnóstico dos ambientes monitorados, obtido através do cruzamento das informações coletadas pelos softwares;
		9.1.4	Dados estatísticos: gráficos e tabelas analíticos e comparativos, mostrando a situação do ambiente gerenciado mês a mês
		9.1.5	Alertas: descrição dos eventos de maior relevância que necessitaram de intervenções imediatas ou proativas (em tempo real);
		9.1.6	Recomendações de Segurança: avaliação dos pontos que podem ser modificados e melhorados, de acordo com a estratégia de negócio da SEFAZ BA, levando-se em consideração às boas práticas aplicadas no mercado e nos demais clientes;
		9.2	Os relatórios técnicos deverão estar disponíveis para a SEFAZ BA a qualquer momento, se solicitado, devendo ser disponibilizados em até 24 (vinte e quatro) horas após a solicitação.
10	REQUISIÇÕES DE SERVIÇOS	10.1	A SEFAZ BA poderá ABRIR requisições de serviços para a CONTRATADA sempre que identificar a necessidade de ações corretivas e/ou evolutivas, pedido de informação, pedido de análises ou qualquer outra atividade relacionada aos produtos e contextos de operação inerentes às soluções, produtos de segurança descritas na PLATAFORMA DE SEGURANÇA.
		10.2	A CONTRATADA deverá atender a requisição conforme solicitado e registrado em ferramenta apropriada, sempre atendendo aos padrões e normas estabelecidos pelo CONTRATANTE, e em de acordo com os Níveis Mínimos de Serviços definidos.
		10.3	Será considerada como ATENDIMENTO a uma requisição de serviço de segurança da informação a completitude das ações necessárias a prestação de informação, geração de relatórios, esclarecimento de dúvidas, exportação de dados, análises técnicas básicas e avançadas, além da realização de quaisquer tipos de configuração, parametrização nas ferramentas de segurança da informação da CONTRATANTE ou da CONTRATADA.
		10.4	Após o pleno ATENDIMENTO da requisição de serviços a CONTRATADA deverá submeter o processo para análise do CONTRATANTE, esse confirmará o seu atendimento. Somente após está etapa de avaliação a requisição poderá ser FECHADA.
11	MONITORAMENTO e MANUTENÇÃO DA PLATAFORMA DE SEGURANÇA	11.1	A CONTRATADA deverá monitorar permanentemente e avaliar criticamente os serviços e componentes de segurança da informação do CONTRATANTE, identificando e endereçando (via requisições de serviço ou mudança) as melhorias de configuração, atualizações/correções necessárias, bem como traçando curvas de comportamento, definindo a volumetria média de acessos e identificando comportamentos não usuais, visando antecipar a



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

	identificação de incidentes de segurança e limitações de capacidade antes mesmo de impacto nos serviços.
11.2	As manutenções preventivas e/ou corretivas, que representem risco de interrupção do(s) serviço(s), deverão ser agendadas e realizadas preferencialmente fora do horário regular, salvo quando expressamente autorizado.
11.3	As manutenções programadas, que impliquem em extensiva parada do ambiente, serão realizadas durante um final de semana e feriados. Tais atividades realizadas fora do horário regular não ensejarão qualquer pagamento adicional em relação ao estabelecido no contrato, portanto a CONTRATADA deverá prever esta situação em sua composição de custos.
11.4	Todos os serviços de manutenção corretiva e preventiva são considerados de natureza contínua e deverão minimizar a necessidade de parada do ambiente em produção.
11.5	A CONTRATADA deverá seguir o processo de gerenciamento de mudança estabelecido pela SEFAZ BA. Sempre que solicitado, a CONTRATADA deverá estar disponível para participar das reuniões com o Comitê de Mudanças, para prestar informações sobre os ambientes e serviços por elas executados. Mudanças que impliquem em um conjunto de procedimentos complexos, que envolvam várias equipes ou empresas CONTRATADAS e que implicarem em riscos de paralisação de quaisquer serviços considerados prioritários, deverão ser tratadas como um Projeto.
11.6	A CONTRATADA deverá apresentar ao Comitê de Mudanças da SEFAZ BA a proposta de todas as mudanças no ambiente, conforme níveis de controle estabelecidos. Para todas as mudanças apresentadas, será necessário acompanhar dentre outras informações, as análises de risco relativas às mudanças, descrevendo o impacto da sua realização.
11.7	A CONTRATADA deverá testar todos os serviços após a realização de manutenções preventivas e/ou corretivas, ficando sua aceitação final dependente da área demandante e/ou de fiscalização do CONTRATANTE, que avaliará as características esperadas para o serviço.
11.8	Todos os serviços deverão ser executados em conformidade com as rotinas, processos, procedimentos e preceitos do ITIL definidos pelo CONTRATANTE.
11.9	Fará parte do trabalho da CONTRATADA o teste e a emissão de parecer a respeito de qualquer novo Item de Configuração (IC) que suporte os serviços de segurança adotados pela SEFAZ BA, devendo emitir nota técnica avaliando os riscos deste novo IC para o ambiente tecnológico. Com base na nota técnica elaborada a SEFAZ BA irá aprovar a liberação do IC no ambiente. Se o processo de liberação do



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

			IC implicar em riscos de paralisação de quaisquer serviços considerados prioritários, deverá ser tratado como um Projeto
12	MELHORIA CONTÍNUA	12.1	Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação da SEFAZ BA, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
		12.2	Sugerir medidas preventivas com objetivo de identificar e conter possíveis ataques e invasões aos ativos da SEFAZ BA;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.6. SERVIÇO - GERENCIAMENTO DE VULNERABILIDADES

ESPECIFICAÇÃO TÉCNICA			
1	ESCOPO DO SERVIÇO	1.1	Processo de Gerenciamento de Vulnerabilidades - A CONTRATADA deve estruturar, implantar e operar um processo de Gerenciamento de Vulnerabilidades, que estabelece os fluxos e atividades de monitoramento, detecção, avaliação, priorização e tratamento de vulnerabilidades, permitindo um gerenciamento capaz de supervisionar, coordenar e operacionalizar as ações necessárias à apuração de vulnerabilidades no ambiente de TI da SEFAZ BA e os meios de respostas adequadas a cada situação.
		1.1.1	Este processo tem por objetivo identificar possíveis vulnerabilidades de segurança da informação no ambiente de TI da SEFAZ BA, a fim de evitar que ataques cibernéticos obtenham sucesso explorando fragilidades conhecidas.
		1.1.2	Faz parte deste processo, a avaliação e categorização dos riscos associados às vulnerabilidades identificadas, assim como o planejamento, execução e validação de correções propostas, em conjunto a equipe técnica de segurança da informação da SEFAZ BA.
		1.1.3	A responsabilidade da execução da correção das falhas de segurança depende de quem é responsável pelo gerenciamento e administração do (s) ativo (s) com vulnerabilidade (s): - Nos ativos gerenciados pela Central de Serviços - TI da SEFAZ BA, esta é a responsável pela correção que deve ser indicada, acompanhada e validada pela CONTRATADA; - Nos ativos gerenciados pela CONTRATADA, como as soluções da PLATAFORMA DE SEGURANÇA, a correção é responsabilidade da CONTRATADA.
		1.1.3.1	As aplicações de patches e hot-fixes em ativos, servidores e softwares, por exemplo, devem ser indicadas e acompanhadas pela CONTRATADA, mas serão executadas pela Central de Serviços - TI da SEFAZ BA.
		1.1.3.2	As aplicações de patches e hot-fixes nos componentes das soluções de "Gerenciamento de eventos e informações de segurança (SIEM)" e de Avaliação de Vulnerabilidades ofertados e hospedados fora do ambiente da SEFAZ BA são responsabilidade da CONTRATADA e/ou fabricante no caso de soluções SaaS (Software as a Service).
		1.1.3.3	As aplicações de patches e hot-fixes nos componentes das soluções de "Gerenciamento de eventos e informações de segurança (SIEM)" e de Avaliação de Vulnerabilidades ofertados e hospedados no ambiente da SEFAZ BA devem ser indicadas e acompanhadas pela CONTRATADA, mas serão executadas pela Central de Serviços - TI da SEFAZ BA.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		1.1.3.4	No que se refere a PLATAFORMA DE SEGURANÇA, gerenciada pela CONTRATADA, as correções necessárias dentro das soluções são responsabilidade da CONTRATADA. No entanto, as aplicações de patches e hot-fixes nos componentes das soluções da PLATAFORMA DE SEGURANÇA gerenciadas e hospedados no ambiente da SEFAZ BA devem ser indicadas e acompanhadas pela CONTRATADA, mas serão executadas pela Central de Serviços - TI da SEFAZ BA.
		1.2	Solução de Avaliação de Vulnerabilidades - Faz parte do escopo do serviço de Gerenciamento de Vulnerabilidades o fornecimento e gerenciamento de solução de Avaliação de Vulnerabilidades conforme requisitos técnicos definidos neste Termo de Referência.
		1.2.1	A CONTRATADA é responsável pela implantação, administração, operação e suporte técnico da solução de Avaliação de Vulnerabilidades para descoberta de vulnerabilidades de aplicações e infraestrutura no ambiente de TI da SEFAZ BA.
		1.3	Este serviço deve identificar vulnerabilidades em todo tipo de plataforma, redes, containers, sistemas, aplicações ou aplicativos móveis; mensurando o real impacto e a probabilidade de exploração de uma vulnerabilidade
2	EQUIPE TÉCNICA -	2.1	Cabe a CONTRATADA a estruturação, administração e coordenação da equipe técnica responsável pelo serviço de GERENCIAMENTO DE VULNERABILIDADES: EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES.
		2.2	A EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES será responsável pela implantação e operação do processo de Gerenciamento de Vulnerabilidades.
		2.3	A EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES será responsável pelas atividades de detecção, avaliação, priorização e tratamento de vulnerabilidades, assim como a orientação e acompanhamento das ações de mitigação e remediação necessárias junto a Equipe Técnica-SEFAZ BA.
		2.4	A EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES será responsável pela implantação, administração e configuração da ferramenta de avaliação de vulnerabilidade a fim de realizar o SCAN do ambiente de TI visando a descoberta de vulnerabilidades.
		2.5	A EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES deve ser composta de, pelo menos, 2 (dois) profissionais.
		2.6	A capacitação técnica e experiência da equipe técnica deve garantir a qualidade dos serviços e informações prestadas, atuando conforme o estado da arte e melhores práticas em termos de segurança da informação, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados neste Termo de Referência.
		2.7	Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ou certificações oficiais válidas e



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		ativas, conforme os requisitos específicos para o perfil profissional descritos no ENCARTE D - PERFIL PROFISSIONAL
		2.8 A EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES deve ser alocada no SOC (LOCAL), localizado nas instalações da SEFAZ BA.
		2.9 A EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES também será responsável pelo serviço de RESPOSTA A INCIDENTES (N2), conforme descrito neste Termo de Referência. Desta forma, a EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES e a EquipeSOC de RESPOSTA A INCIDENTES (N2) são a mesma equipe.
3	HORÁRIO DE OPERAÇÃO	3.1 A EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES deve atuar em regime comercial de 08:00 às 18:00h, de segunda à sexta-feira, exceto feriados, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados.
		3.2 Em situações excepcionais, a EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES poderá ser acionada fora dos horários previstos nesta janela, para atuar e/ou auxiliar as equipes técnicas Equipe Técnica - SOC e Equipe Técnica - SEFAZ BA na resolução de incidentes e problemas de segurança cibernética.
4	ATIVIDADES PREVISTAS	4.1 As atividades associadas a execução do serviço de Gerenciamento de Vulnerabilidades serão revistas, estabelecidas e detalhadas no processo de Gerenciamento de Vulnerabilidades a ser estruturado e implantado conforme definido neste Termo de Referência.
5	PROCESSO DE GERENCIAMENTO DE VULNERABILIDADES	5.1 O Processo de Gerenciamento de Vulnerabilidades a ser estruturado e implantado, e aprovado pela SEFAZ BA, deve ser compatível com as práticas, recomendações e frameworks do NIST (National Institute of Standards and Technology), SANS Institute, ITIL (Framework Information Technology Infrastructure Library) V4 e políticas, normas e processos vigentes na SEFAZ BA.
		5.1 O Processo de Gerenciamento de Vulnerabilidades a ser implantado deverá contemplar no mínimo as seguintes etapas:
		PLANEJAMENTO
		5.1.1 Planejamento mensal da avaliação de vulnerabilidades com definição de escopo e detalhamento do impacto e parâmetros usados na análise.
		5.1.1.1 Planejamento deverá definir cronograma das atividades a serem realizadas
		5.1.1.2 Cada atividade poderá conter como escopo um ativo de TIC, um sistema de TIC ou grupo de ativos que façam sentido num agrupamento.
		AVALIAÇÃO DE VULNERABILIDADE
		5.1.2 Execução das avaliações de vulnerabilidades com monitoramento do ambiente para detectar desvios, incluindo:



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

	5.1.2.1	Descoberta de ativos de TIC ou sistemas de TIC na rede e sua classificação;
	5.1.2.2	Identificação, por meio de varreduras, de vulnerabilidades dos ativos de TIC ou sistemas de TIC e de suas configurações;
	5.1.2.3	Análise das vulnerabilidades encontradas;
	5.1.2.4	Classificação das vulnerabilidades encontradas de acordo com a criticidade, o risco e o contexto do ambiente computacional dos ativos de TIC ou sistemas de TIC da SEFAZ BA;
	5.1.2.5	Validação de exposição do ambiente computacional da SEFAZ BA às vulnerabilidades encontradas;
	5.1.2.6	A CONTRATADA deverá realizar uma análise de falso positivo das vulnerabilidades descobertas, isso quer dizer, que devem ser informadas à SEFAZ BA apenas vulnerabilidades que existam de fato em seu ambiente.
		PRIORIZAÇÃO
	5.1.3	As vulnerabilidades classificadas devem ser objeto de agrupamento e de triagem com a criação de score de riscos e priorização das ações com base em riscos mensuráveis, usando métricas como:
	5.1.3.1	Existência de exploit automatizado
	5.1.3.2	Disponibilidade em kits de malwares
	5.1.3.3	Duração de vulnerabilidades conhecidas e não corrigidas;
	5.1.3.4	Contexto do ambiente vulnerável;
	5.1.3.5	Demais critérios definidos pela SEFAZ BA.
		AÇÕES DE CORREÇÃO
	5.1.4	Proposição de ações de correções, caso existam, para as falhas classificadas e mitigações, caso não existam correções disponíveis
	5.1.4.1	Deverão constar as principais remediações para tratamento das vulnerabilidades mais comuns, críticas e de exploits conhecidos
	5.2	Emissão de relatórios analíticos conforme a solicitação da SEFAZ BA.
	5.3	Criação e atualização de Dashboards setoriais conforme definido pela CONTRATANTE
	5.4	Acompanhar, no âmbito da SEFAZ BA, junto a Central de Serviços - TI a correção ou mitigação das vulnerabilidades.
	5.4.1	Acompanhamento do ciclo de vida das vulnerabilidades
	5.4.2	Caso seja necessária alguma alteração no parque computacional da SEFAZ BA para correção e/ou mitigação da vulnerabilidade, a CONTRATADA deverá informar a CONTRATANTE e abrir as requisições



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		de serviço para correção conforme canais de comunicação definidos pela CONTRATANTE.
		5.5 A Gerenciamento de Vulnerabilidades compreende ainda:
		5.5.1 Multiplicação do conhecimento acerca do serviço prestado
		5.5.2 A SEFAZ BA poderá demandar a apresentação do relatório para as equipes de desenvolvimento, de forma a pormenorizar as vulnerabilidades e as correções aplicáveis
		5.5.3 Manutenção preventiva e corretiva da Solução de Gerenciamento de Vulnerabilidades, incluindo a verificação dos ativos do parque que devem ser inseridos ou removidos
		5.5.4 Atualização da Solução de Gerenciamento de Vulnerabilidades
		5.5.5 Análise de Vulnerabilidades demandadas diretamente pela CONTRATANTE a qualquer tempo fora do processo normal
		5.6 As atividades só serão consideradas concluídas após a entrega de relatório analítico nomeando o técnico responsável pelas conclusões
		5.6.1 Os relatórios automatizados pela solução deverão ser a base de uma análise criteriosa pelo técnico responsável para detectar falsos positivos e pontos críticos de correção
		5.6.2 Poderão ser utilizadas ferramentas livres e gratuitas para aprofundar a análise e elaboração de relatórios.
		5.6.3 A CONTRATADA deve realimentar a Solução de Avaliação de Vulnerabilidades com o resultado das análises.
6	EXECUÇÃO DE VARREDURA (SCAN)	6.1 De acordo com planejamento estabelecido e aprovado pela SEFAZ BA, a EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES deve utilizar a solução de avaliação de vulnerabilidades fornecida para executar varredura nos ativos de hardware e software em busca de vulnerabilidades no ambiente de TI da SEFAZ BA.
		6.1.1 O escopo e demais parâmetros a serem configurados na ferramenta de avaliação de vulnerabilidade para realizar o SCAN devem ser discutidos e aprovados pela SEFAZ BA, assim como a frequência de realização do SCAN.
		6.2 Apesar de estar previsto, o fornecimento e utilização de solução de avaliação de vulnerabilidade se espera que a EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES se utilize também de métodos e técnicas assistidas, para identificar possíveis vulnerabilidades no ambiente da SEFAZ BA.
		6.2.1 De acordo com planejamento definido e aprovado pela SEFAZ BA, a EquipeSOC de GERENCIAMENTO DE VULNERABILIDADES deve realizar consultas periódicas, segundo rotinas a serem definidas, junto aos sites dos fabricantes e outros sites de referência em busca de vulnerabilidades publicada.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		6.2.2	As vulnerabilidades publicadas devem ser verificadas com relação a sua existência no ambiente da SEFAZ BA.
7	DASHBOARD	7.1	É necessário que todos os dados dos ativos monitorados sejam concentrados em um dashboard que forneça a SEFAZ BA recursos essenciais para o adequado gerenciamento de vulnerabilidades, incluindo a geração de relatórios, a quantificação dos riscos associados a vulnerabilidades e sua correção pela equipe da CONTRATADA com eventual apoio da equipe do SEFAZ BA, através dos métodos de correção de vulnerabilidades, dentre outros.
8	MONITORAMENTO DE PATCHES	8.1	Monitoramento Contínuo de Patches, Infraestrutura e Atualizações de Segurança - análise contínua à procura por patches e atualizações de segurança não instalados no ambiente de TI da SEFAZ BA.
		8.1.1	A CONTRATADA deve garantir que cada ativo do escopo monitorado será analisado pelo agente de varredura, no mínimo, uma vez a cada 30 (trinta) dias em busca de patches de segurança não instalados;
		8.2	Re-testes: Após a aplicação do patch, o SEFAZ BA, deve ser capaz, diretamente através da interface, de repetir a análise naquele ativo para validação das correções implementadas
9	GERENCIAMENTO DO SERVIÇO	9.1	Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a SEFAZ BA definiu indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue mensalmente
		9.2	O GESTOR TÉCNICO deve apresentar e discutir o relatório e indicadores em reunião mensal com a equipe técnica indicada pela SEFAZ BA.
		9.3	O relatório poderá ser customizado a pedido do CONTRATANTE durante a vigência contratual para melhor acompanhamento do serviço
		9.4	
10	MELHORIA CONTÍNUA	10.1	Fornecer sugestões e auxiliar na construção e manutenção contínua, com o apoio e aprovação da SEFAZ BA, de procedimentos sistematizados e da base de conhecimento, contemplando todas as soluções de problemas resolvidos com respostas padronizadas;
		10.2	Sugerir medidas preventivas com objetivo de identificar e conter possíveis ataques e invasões aos ativos da SEFAZ;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.7. SOLUÇÃO - GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA (SIEM)

ESPECIFICAÇÃO TÉCNICA			
1	ESCOPO	1.1	A CONTRATADA deve fornecer solução de "Gerenciamento de eventos e informações de segurança (SIEM)" para suportar os serviços de "Monitoramento de Eventos de Segurança" e "Resposta a Incidentes de Segurança", e processos associados.
		1.1.1	A CONTRATADA será responsável pela instalação, configuração e administração da solução fornecida considerando as melhores práticas de segurança e o impacto no ambiente a ser avaliado. As estratégias, escopo, políticas e demais configurações necessárias ao uso da solução no ambiente da SEFAZ BA devem ser apresentadas e discutidas com a CONTRATANTE e aplicadas mediante prévia aprovação da mesma.
		1.2	A solução a ser fornecida deve ser uma plataforma inteligente de segurança, com recursos completos de coleta, correlacionamento e análise de eventos do ambiente;
		1.3	As licenças de uso das soluções empregadas na prestação deste serviço pertencerão CONTRATANTE, SEFAZ BA.
		1.4	A solução de " Gerenciamento de eventos e informações de segurança (SIEM) " a ser fornecida deve atender aos requisitos técnicos e operacionais definidos a seguir neste Termo de Referência.
2	ARQUITETURA TÉCNICA	2.1	A arquitetura da solução deve ser distribuída, permitindo que o módulo de gerenciamento e os agentes de coleta estejam em segmentos de rede segregados
		2.2	A solução deve ser implementada observando as seguintes características:
		2.2.1	O módulo de gerenciamento deve ser entregue no modelo SaaS (Software as a Service) ou Nuvem Pública
			O módulo de gerenciamento deve estar disponível em ambiente administrado pelo próprio fabricante ou pela contratada, que é responsável pelas manutenções, atualizações e disponibilidade da solução;
		2.2.2	O agente de coleta deve funcionar no modelo on-premise, sem limitação de licença.
		2.2.2.1	Caso o agente de coleta possa ser instalado em uma VM virtualizada pela plataforma Vmware, a CONTRATADA pode utilizar a infraestrutura de virtualização da SEFAZ BA. Caso contrário, a CONTRATADA deve fornecer o HW necessário.
		2.2.3	A solução deve prover suporte a alta disponibilidade ou disaster recovery para o módulo de gerenciamento.
		2.2.4	Não deve exigir a adição de agentes ou software nos dispositivos monitorados, exceto quando o dispositivo a ser monitorado não



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

	disponibilize nenhum meio nativo de envio de logs citado no item anterior;
2.3	A solução deve possuir suporte ao IP (Internet Protocol) versão 4 e versão 6
2.4	Todas as atividades relativas à administração da solução e de seus componentes, incluindo configurações gerais, acompanhamento de resultados, geração de relatórios, ajustes e configuração dos agentes de coleta, deverão ser executadas através do módulo de gerenciamento
2.5	A solução deve possuir interface gráfica Web centralizada, compatível com os principais navegadores do mercado
2.5.1	Prover uma interface intuitiva, permitindo que em poucos cliques seja possível chegar a uma ação suspeita ou ataque, sem prévio conhecimento dela;
2.5.2	Deve suportar, pelo menos, os navegadores Chrome e Firefox em suas versões mais atuais;
2.6	Deve armazenar os eventos, alertas e incidentes na base de dados da solução, de forma indexada;
2.6.1	Permitir a procura por texto, campos pré-definidos, palavras chaves ou expressões regulares;
2.7	A solução proposta deverá ter sido desenvolvida por um único fabricante de modo que tanto o suporte da solução quanto as funcionalidades sejam integradas e 100% compatíveis.
2.7.1	A solução ofertada não poderá ser do tipo opensource
2.8	A solução deve ser fornecida e dimensionada para a quantidade de ativos a serem monitorados ou para a quantidade de eventos por segundo ou para o volume de armazenamento de logs em ambiente SaaS de forma a abranger o escopo completo de ativos da CONTRATANTE, conforme conceito apresentado nesta especificação técnica. Assim, é obrigatório que a solução cubra 100% do ambiente da CONTRATANTE, incluindo servidores físicos e virtuais, estações de trabalho, firewalls e ativos de rede, etc. e não somente parte do mesmo, de forma a prover uma visibilidade plena da segurança cibernética do ambiente.
2.8.1	O escopo dos ativos a serem monitorados e protegidos está definido no anexo "AMBIENTE DE TI - SEFAZ BA"
2.8.2	A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar de forma sustentada os eventos por segundo (EPS) estimados pela CONTRATADA conforme análise do "AMBIENTE DE TI - SEFAZ BA".



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		2.8.2.1	A solução deve permitir a recepção de eventos que excedam temporariamente os limites estimados pela CONTRATADA, processando o volume excedente assim que volume for normalizado. Mantendo a operação com situações de picos temporários, sem incorrer na perda de eventos e sem incorrer em qualquer cobrança adicional por excesso ou bloqueio da solução.
		2.9	A solução deve possuir retenção mínima de 06 (seis) meses de registros (logs) prontamente acessíveis de forma on-line. Após este período, a solução deve suportar, no mínimo, 12 (doze) meses de registros arquivados, bem como permitir a exportação destes logs/dados de telemetria para armazenamento em ambiente de propriedade da CONTRATANTE.
		2.9.1	Deve armazenar logs por tempo determinado e customizado;
		2.9.2	Deve permitir a exclusão de eventos (metadados e raw) de forma automática, permitindo a customização por diversos fatores, no mínimo: tipo/nome do evento e dispositivo/fonte de log;
		2.9.3	A solução deve possuir um SDK ou API para criação de novos Apps/Plugins, de forma a permitir que o próprio usuário possa desenvolver aplicações e extensões livremente.
		2.9.4	Deve disponibilizar APIs do tipo webservices, do tipo "RESTful API", para acesso externo e integração com a solução, permitindo busca de informações de eventos, manipulação de incidentes e uso de administração da solução;
3	REQUISITOS DE SEGURANÇA	3.1	A comunicação entre os componentes da solução deve ser efetuada por meio de portas seguras e de criptografia;
		3.2	A solução deve ser capaz de criptografar dados em repouso, bem como criptografar dados em trânsito
		3.3	A solução deve suportar multifator de autenticação para os usuários do console de administração;
		3.4	A solução deve permitir a instalação, substituição/atualização ou manter o certificado digital para prover o acesso seguro;
		3.5	Manter seu próprio log de auditoria;
4	COLETA DE LOGS	4.1	Possuir a capacidade de obter logs e eventos de autenticações em serviço de diretório Active Directory;
		4.2	Ser capaz de tratar, no mínimo, os seguintes formatos, protocolos e fontes:
		4.2.1	Firewalls: Fortinet, Cisco/ASA, Checkpoint, Palo Alto e SonicWall
		4.2.2	Network IPS: Trellix, McAfee, Sourcefire, IBM/ISS, HP Tipping Point e Snort;
		4.2.3	Switches/Roteadores: Dell;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

4.2.4	Plataformas de Virtualização: VMware ESXi;
4.2.5	Sistemas Operacionais: Linux (Debian, RedHat, Ubuntu, CentOS, Oracle Linux, IBM/AIX, IBM/RACF, HPUX, Solaris), Windows Server (2008, 2012, 2016, 2019, 2022), Windows 7, Windows 10 e Windows 11;
4.2.6	Segurança de Endpoint: McAfee, Kaspersky, Trellix;
4.2.7	Serviços de Nuvem: Office 365, Azure Active Directory; AWS S3, AWS Cloudwatch, AWS Kinesis, Azure Event Hubs, Kafka, Google Cloud Pub/Sub;
4.2.8	Serviços Windows: Active Directory;
4.2.9	Servidores de Aplicação e Web: Apache2, Nginx, Apache Tomcat, Jboss e Microsoft IIS7 (ou superior);
4.2.10	Servidores Bancos de Dados: PostgreSQL, Oracle, SQL Server, MySQL, IBM/DB2.
4.2.11	McAfee WebGateway, Netscaler, Forescout NAC.
4.2.12	Checkpoint OPSEC/LEA, CISCO NSEL, API REST genérica e Juniper NSM Protocol;
4.2.13	Ser capaz de tratar, no mínimo, os seguintes formatos, protocolos e fontes: Netflow V5 e V9, Sflow, SYSLOG (UDP, TCP), SYSLOG-NG, SYSLOG criptografado com TLS, SNMP (V1, V2 e V3), Microsoft Windows Event Logging, FTP, SCP, SFTP, arquivos de logs em texto formatado (vírgula/tabulação/delimitado) e logs em texto não formatado, API, JSON, CEF, DNS logs, DHCP logs, SSH logs, FTP logs, PROXY logs, MQ Series client, API REST genérica
4.2.14	Possuir suporte nativo, suportado pelo fabricante, para coleta, reconhecimento e normalização de pelo menos, 350 tipos de fontes de dados logs;
4.3	Deve oferecer uma solução para poder adicionar novas fontes de dados, coletores e integrar novos dispositivos não suportados nativamente;
4.4	Ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos. A notificação pode ser de forma nativa, através de agentes ou compondo com outros produtos;
4.5	O servidor coletor da solução deverá ser capaz de armazenar os dados localmente (cache) em caso de indisponibilidade do componente correlacionador;
4.6	O coletor deverá possuir uma interface com o ativo monitorado de forma passiva (recebendo) e ativo (buscando) as informações relevantes para o funcionamento da solução;
4.7	Permitir acrescentar o horário (timestamp) correto da recepção do evento/log na solução, preservando o horário original do evento. Esse horário deve ser obtido pelo sistema através de sincronização com



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		servidores NTP previamente definidos, e sincronizado entre todos os componentes da solução;	
	4.8	Ser capaz de marcar (através de tag, label ou similar) os eventos com base em unidade organizacional: departamento, setor, secretaria ou similar. Essa marcação pode ser feita por atributos da própria mensagem, da origem do log, ou do endereço de origem do evento;	
	4.9	A solução deve permitir a integração de dispositivos ou logs não suportados nativamente;	
	4.10	A integração de logs ou dispositivos deve ser realizada na interface web.	
	4.11	Deve permitir a criação automática de data sources pela detecção do tipo de fonte do log, dentre os tipos de logs customizados na solução, quando enviados via Syslog	
	4.12	Deve identificar e gerar um alerta que avise quando uma fonte de eventos parar de enviar logs.	
5	DETECÇÃO DE EVENTOS	5.1	Ser capaz de demonstrar perfil de tráfego normalizado em tempo real e traçar o comportamento padrão (baseline) dos ativos e fornecer alertas quando ocorrer eventos fora do baseline;
		5.2	Ser capaz de detectar anomalias no comportamento usual de determinado ente (dispositivo e usuário) e no mínimo detectar desvios:
		5.2.1	Relacionado ao tempo ou ações em tempos inexecutáveis;
		5.2.2	Relacionado a volumetria de dados;
		5.2.3	As fontes e destino dos eventos;
		5.2.4	Localização geográfica;
		5.2.5	Direcionamento e serviços de origem e destino;
		5.2.6	Acesso a endereços considerados suspeitos via Threat Feed e IP reputation;
		5.2.7	Contas utilizadas de forma não compatível;
		5.2.8	Ataques de força bruta com e sem sucesso;
		5.2.9	Falhas de autenticação que indiquem suspeita de roubo de identidade;
		5.2.10	Uso não compatível de contas de serviço;
		5.2.11	Acessos à VPN a partir de localidades e/ou horários atípicos.
		5.3	Detectar atividades suspeitas como:
		5.3.1	Port scanning;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		5.3.2	Network service scanning;
		5.3.3	Network share discovery;
		5.3.4	Hoarding de dados (quando um usuário ou dispositivo começa a acumular dados copiados dos servidores da SEFAZ);
		5.3.5	Exfiltração de dados (quando um usuário ou dispositivo começa a enviar dados para fora da rede da SEFAZ);
		5.3.6	Network denial of service (ataque interno aos serviços de rede como AD, DNS, DHCP, etc.);
		5.3.7	Infecção de equipamentos por vírus;
		5.3.8	Realização de ações suspeitas por parte de usuários privilegiados;
		5.3.9	Alertas de operação de serviços, como interrupções e falhas;
		5.3.10	Ataques de negação de serviço;
		5.3.11	Ataques comuns em aplicações WEB, como XSS e SQL Injection;
		5.3.12	Atividades de botnets;
		5.3.13	Exploração de vulnerabilidades;
		5.4	Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de command and control; e
		5.5	Permitir criação de listas de dispositivos confiáveis;
		5.6	Deve ter capacidade de detectar automaticamente padrões de ataques especializados que acontecem ao longo do tempo e que não foram previstos ou observados anteriormente;
		5.7	Utilização de algoritmos de aprendizado de máquina em tempo real para analisar grandes volumes de dados de segurança instantaneamente, permitindo uma detecção ágil de ameaças e comportamentos maliciosos, com a minimização de falsos positivos.
		5.8	Analisar dados provenientes de fontes externas, como feeds de ameaças globais, enriquecendo a análise de segurança e aprimorando a capacidade de detecção.
6	ANÁLISE E CORRELAÇÃO DE EVENTOS	6.1	Correlacionar os eventos coletados objetivando evidenciar incidentes que possam ser caracterizados como ataque;
		6.1.1	A correlação e o armazenamento dos logs e eventos devem ser realizados em processos paralelo;
		6.1.2	Processar e correlacionar logs e eventos próximo ao tempo real;
		6.2	Implementar regras avançadas que ligam eventos sem correlação direta e gerar incidentes caso seja constatado algum desvio;
		6.3	Deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos/tráfego, quando



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		comparados a outros períodos similares (ex. mesmo período do dia, mesmo dia da semana);
6.4		Deve permitir a criação de regras que identifiquem desvios, em qualquer metadado, de limites pré-estabelecidos;
6.5		Deve permitir usar as regras de correlação aplicada de forma histórica, em eventos já mantidos na base de dados da solução, sem afetar a execução das regras online. Deve permitir especificar qual horário a ser utilizado para a correlação, o da recepção do evento na solução ou o horário existente no evento/log.
6.6		Deve possuir mapeamento das regras de acordo com o Framework Mitre ATT&CK, permitindo a gestão das regras (ativação, desativação, customização), ao selecionar uma Tática ou técnica do Framework
6.7		Deve possuir mecanismo para ajuste fino de regras de correlação, exibindo de forma gráfica as regras de correlação que são mais acionadas por eventos (que geram mais alertas) e seus elementos relacionados. Facilitando o refinamento da solução com vistas à redução de falso-positivo e melhoria da performance;
6.8		Propriedades customizadas devem poder ser usadas em regras de correlação online e em regras de correlação histórica
6.9		Gerar alertas/incidentes com base nas regras definidas previamente;
6.10		Deve permitir a criação de regras ilimitadas e a edição das existentes;
6.11		Deve permitir o correlacionamento de qualquer informação que conste no evento, inclusive informações que não sejam referentes a endereçamento IP, portas, etc., tais como dados financeiros;
6.12		Deve ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento;
6.13		Deve possuir no mínimo 450 regras de correlação ou usar modelos de ameaças com base em machine learning e inteligência artificial, especializadas na detecção de incidentes de segurança, produzidas, suportadas e atualizadas pelo fabricante da solução;
6.14		Deve possuir repositório do fabricante da solução que ofereça novas regras de correlação especializada em segurança para atualização e ampliação da capacidade de detecção de incidentes, sem custo adicional;
6.15		A solução deve incluir regras pré-programadas (out-of-the-box) tanto para normalização de logs quanto para correlação de eventos, bem como permitir que se escrevam / definam regras próprias / personalizadas;
6.16		A solução deve possuir um ambiente de construção de regras utilizando query ou assistente da própria solução, visando à redução de erros de lógica e sintaxe;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

	6.17	Para análise dos eventos, deve suportar filtros de eventos, usando filtros simples, pesquisa de expressões e buscas avançadas diretamente na base de dados;
	6.18	Deve permitir filtrar e selecionar os eventos que serão inseridos na solução;
	6.19	Deverá fazer a agregação de eventos, mostrando a contagem de eventos, quando o mesmo evento ocorrer dentro de um período curto. A opção de realizar ou não a agregação de eventos deve ser configurável, por dispositivo integrado;
	6.20	Deve ter capacidade de sumarizar múltiplos alertas idênticos automaticamente;
	6.21	Ser capaz de contextualização, utilizando dados de diferentes origens (rede, servidor, aplicações) em uma única console, otimizando e auxiliando o processo de análise de resposta a incidentes;
	6.22	Implementar a normalização e categorização de logs e flows de rede;
	6.23	Deve permitir a configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados.
	6.24	Implementar análise visual dos correlacionamentos, tráfegos e alertas para auxiliar a identificação gráfica de padrões;
	6.25	Deve permitir pesquisa nos eventos históricos, a partir de metadados, fornecendo capacidade de "drill-down", ou seja, o refinamento da pesquisa a partir da seleção de elementos no resultado, para efetuar nova pesquisa.
	6.25.1	Deve manter o evento bruto ("raw") e seus metadados para o armazenamento e consulta futura, e permitir sua visualização.
	6.26	Armazenar os alertas, incidentes e os eventos, inclusive os normalizados, de forma indexada.
	6.27	Permitir a adição de analisadores personalizados (incluindo dados não syslog);
	6.28	Analisar logs e eventos através do uso de inteligência artificial ou machine learning;
	6.29	Priorizar os eventos e alertas com base nos critérios de severidade do evento e criticidade do ativo;
	6.30	Deve atribuir métrica de prioridade para os eventos e para os alertas/incidentes;
	6.31	Deve permitir a criação de novos tipos de eventos na ferramenta, a fim de integrar logs não suportados nativamente;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		6.32	Um único componente da solução deve ser capaz de coletar, processar e normalizar tanto os eventos de segurança e eventos de negócio (não relacionados à segurança);
		6.33	Possuir a capacidade de automatizar a resposta a incidentes, através da execução de scripts, como ação customizada dentro das regras de correlação.
		6.37	Deve ter capacidade de automatização da interpretação de eventos de segurança, proporcionando resumos detalhados, avaliação do impacto potencial e sugestões de correção imediata.
		6.38	A solução deve incorporar algoritmos de aprendizado de máquina para aprimorar a correlação de eventos de segurança, provenientes de diversas fontes, aumentando a eficácia na detecção de padrões e tendências suspeitas.
7	UEBA	7.1	Deve possuir detecção antecipada de ameaças mediante a análise avançada do comportamento de usuários e entidades na rede baseada em um modelo de inteligência artificial com aprendizagem automática (UEBA);
		7.1.1	O modelo de análise de comportamento do usuário usando modelos de Machine Learning, deve abranger a análise/retenção dos dados no mínimo por 30 dias, permitindo uma análise abrangente do usuário.
		7.1.2	Deve permitir a criação de modelos customizados de machine learning para a identificação de desvios de comportamento do usuário;
		7.1.3	Deve permitir selecionar usuários que não devem fazer parte da análise com modelos de Machine Learning
		7.1.4	Essa funcionalidade poderá ser entregue a partir de uma plataforma única de administração de operações de segurança (junto com o SIEM), ou apartada da solução, desde que seja integrada de forma nativa com a solução de SIEM;
		7.1.5	Entende-se como integrada de forma nativa, o envio de logs de forma automática (sem customizações via programação, scripts ou similares) do SIEM para o módulo de UEBA;
		7.2	Ter capacidade de analisar comportamento baseado em aprendizado das ações de usuários de forma automática e ser capaz de detectar desvios de padrões através de regras automática;
		7.3	A capacidade de detecção deverá operar com base em um modelo de análise avançada para detectar ameaças internas, contas comprometidas e fuga de dados através da aprendizagem profunda e modelos de riscos estatísticos especializados;
		7.4	Deve contar com a capacidade de modelar com precisão o comportamento de usuários, entidades e, inclusive, alertas de segurança de outras soluções de Cibersegurança;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.5	Deve detectar rapidamente ameaças complexas, priorizar a investigação de alertas de segurança e reduzir significativamente o tempo de resposta das investigações de incidentes ao recriar de forma automática cadeias de ataque completas e reconstruir o comportamento normal e anômalo de usuários e entidades;
7.6	Deve criar as linhas do tempo de maneira automática que mostram toda a atividade usual e não-usual em múltiplos endereços IP, dispositivos e credenciais;
7.7	A plataforma deve construir automaticamente uma base de comportamento para todos e cada um dos usuários e entidades na rede baseado em um modelo de inteligência artificial e fundamentado em aprendizagem automática com modelos predefinidos como: uso de ativos, dispositivos, sessões VPN, acessos físicos, horários de atividade, uso de e-mail, entre outros; analisando a atividade na rede, bem como as sessões de usuário; criando linhas de tempo que permitam colocar toda ameaça em clara perspectiva e em ordem cronológica;
7.8	Deve ser capaz de interpretar os comportamentos de usuários, com a finalidade de detectar ameaças modernas, avançadas e/ou complexas, tais como incidentes baseados em credenciais comprometidas, ataques internos, movimentos laterais e Ransomware, proporcionando uma camada de análise sobre estes incidentes;
7.9	Deve possuir como funcionalidade obrigatória a pesquisa de ameaças (threat hunting), que utilize técnicas de aprendizagem automática para notificar a um analista sobre riscos emergentes, permitindo buscar em múltiplas dimensões a atividade do usuário para encontrar sessões que contenham comportamentos não-usuais específicos; ou encontrar usuários que coincidam com determinados critérios;
7.10	Construir automaticamente linhas de tempo para eventos relacionados a usuários e entidades notáveis de interesse ou estatisticamente significativas, que agilizem a investigação de incidentes, priorizando o nível de atenção dos alertas de segurança; que consigam detectar usuários comprometidos apresentando uma imagem integral de seu comportamento, bem como contar com a possibilidade de detectar automaticamente movimentos laterais, troca de credenciais, endereços IP ou de dispositivos;
7.11	Deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo;
7.12	Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux;
7.13	Implementar geração de score de risco ou lista top 10 de entidades com base em eventos coletados pela solução;
7.14	Deve ser capaz de importar dados de usuário em bases LDAP, CSV ou Windows AD para identificação da pessoa associada a conta do



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

			sistema monitorado, deve ser capaz de coletar e associar no mínimo: nome completo, departamento, contas associadas, e-mail ou cargo
		7.15	Permitir criação de lista de observação (watchlist) de entidades para monitoração e rastreamento;
		7.16	Deve possuir dashboards dos usuários com maior pontuação de risco ou top 10 e realizar um drill down para entender quais as categorias de risco e as ações que contribuíram para o score atual.
		7.17	Deve permitir a criação de novas regras de negócio que contribuam a remediação utilizando a pontuação de risco de atividades consideradas suspeitas.
8	THREAT INTELLIGENCE	8.1	Possuir rede de inteligência (threat intelligence) própria da solução para atualização constante de feeds de ameaças e não deve exigir compra separada. A nuvem de inteligência deve ter a capacidade de no mínimo consultas de reputação de IP, Georreferencia, DNS, HASH e Nome de processos;
		8.2	Ter capacidade de obter informações de georreferencia e imputar essa informação nas correlações e pesquisas;
		8.3	Os dados de georreferenciamento devem ser fornecidos pela solução de forma nativa;
		8.4	Ser capaz de inserir nos eventos normalizados metadados sobre georreferencia;
9	DASHBOARDS E RELATÓRIOS	9.1	Implementar funcionalidade de agendar relatórios de segurança. Os relatórios deverão ser gerados automaticamente (agendados) com frequência e intervalo de tempo a serem definidos pela instituição;
		9.1.1	Permitir gerar relatórios em formatos HTML, PDF ou CSV;
		9.2	Apresentar painéis gráficos (dashboards) com indicativos de situações diversas, facilmente configuráveis e com ferramentas que facilitem a criação pelos usuários;
		9.3	Implementar dashboards com visualização de EPS, GB/dia ou outras métricas;
		9.4	Apresentar painéis gráficos (dashboards) com indicativos de situações relacionados à segurança, compliance, aplicações e monitoração do próprio sistema;
		9.5	Deve possuir a capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;
10	PLAYBOOKS	10.1	A solução deve suportar a criação de playbooks (fluxos automatizados) de forma gráfica para permitir a automação de ações baseadas em gatilhos (triggers);
		10.2	Deve possibilitar a recuperação de informações de alertas e de indicadores de ameaças durante a execução do playbook;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		10.3	Deve permitir a checagem automática de condições para decidir o fluxo de ações a ser executado dentro do playbook;
		10.4	Deve ser capaz de aguardar por uma confirmação do administrador para execução de fluxos mais sensíveis ou de maior impacto no ambiente;
11	RESPOSTA A EVENTOS E INCIDENTES	11.1	Como resultado da aplicação de regras, deve ser capaz de executar ações automáticas como: enviar e-mail, enviar mensagem para o usuário conectado ao console, executar comandos, scripts ;
		11.2	Deve ser possível incluir no playbook ações de remediação executadas em soluções externas (Firewalls Fortinet, Forescout NAC, Microsoft Active Directory, entre outros), através de ações como:
		11.2.1	Desativar credencial;
		11.2.2	Desativar conexão VPN;
		11.2.3	Desativar uma porta;
		11.2.4	Criar política no firewall automaticamente;
		11.2.5	Os métodos de correção devem incluir aplicação de políticas, quarentena, bloqueio de usuários, entre outros;
		11.3	A resposta/remediação deve poder ser totalmente automatizada sem intervenção do usuário
		11.4	Permitir a criação e acompanhamento de incidentes de segurança, de forma manual ou automática, com no mínimo as seguintes características:
		11.4.1	Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente;
		11.4.2	Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos etc.;
		11.4.3	Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise; e
		11.4.4	Permitir registrar os resultados de um incidente de segurança incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação.
		11.4.5	Ser capaz de identificar rapidamente a causa raiz dos incidentes detectados no ambiente em console única;
11.5	Deve exibir as táticas/técnicas do Mitre ATT&CK identificadas no incidente		
11.6	Deve permitir a visualização rápida de informações baseadas Threat Feed para endereços IP envolvidos no incidente		



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		11.7	Deve agregar diferentes incidentes que possuam um elemento comum, reduzindo a quantidade de incidentes a serem gerenciados, dando maior contexto para o analista de segurança.
		11.8	Permitir a implementação de funcionalidades de resposta automática a incidentes, onde a IA desencadeia ações predefinidas para conter, mitigar ou neutralizar ameaças de maneira eficiente, proporcionando uma resposta rápida e coordenada.
12	INTEGRAÇÃO COM SOFTWARE ITSM	12.1	A solução deve ser capaz de se integrar a pelo menos um dos seguintes sistemas externos de ITSM: CA SDM, ServiceNow, CitsSmart, BMC Helix e Run2Biz.
13	BACKUP	13.1	Deverá permitir o backup e a restauração da configuração da solução de gerenciamento, assim como a configuração de usuários e grupo de usuários;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.8. SOLUÇÃO – AVALIAÇÃO DE VULNERABILIDADES

ESPECIFICAÇÃO TÉCNICA			
1	ESCOPO	1.1	A CONTRATADA deve fornecer solução de Avaliação de Vulnerabilidades (ou Gestão de Vulnerabilidades) para suportar o serviço de "Gerenciamento de Vulnerabilidades" e processos associados, a serem executados pela Equipe SEFAZ BA
		1.1.1	A CONTRATADA será responsável pela instalação, configuração e administração da solução fornecida considerando as melhores práticas de segurança e o impacto no ambiente a ser avaliado. As estratégias, escopo, políticas e demais configurações necessárias ao uso da solução no ambiente da SEFAZ BA devem ser apresentadas e discutidas com a CONTRATANTE e aplicadas mediante prévia aprovação da mesma.
		1.2	A solução de Avaliação de Vulnerabilidades deve se integrar com a solução de SIEM fornecida para atender este Termo de Referência a fim de dar maior visibilidade sobre as vulnerabilidades dos dispositivos e fazer uma melhor correlação dos eventos.
		1.3	As licenças de uso das soluções empregadas na prestação deste serviço pertencerão a CONTRATANTE, SEFAZ BA.
		1.4	A solução de Avaliação de Vulnerabilidades a ser fornecida deve atender aos requisitos técnicos e operacionais definidos a seguir neste Termo de Referência.
2	ARQUITETURA	2.1	A arquitetura da solução deve ser distribuída, permitindo que o módulo de gerenciamento e os agentes de varredura estejam em segmentos de rede segregados
		2.2	A solução deve ser implementada observando as seguintes características:
		2.2.1	O módulo de gerenciamento deve ser entregue no modelo SaaS (Software as a Service)
		2.2.1.1	O módulo de gerenciamento deve estar disponível em ambiente administrado pelo próprio fabricante, que é responsável pelas manutenções, atualizações e disponibilidade da solução;
		2.2.2	O agente de varredura deve funcionar no modelo on-premise.
		2.2.2.1	Caso o agente de varredura possa ser instalado em uma VM virtualizada pela plataforma Vmware, a CONTRATADA pode utilizar a infraestrutura de virtualização da SEFAZ BA. Caso contrário, a CONTRATADA deve fornecer o HW necessário.
		2.2.3	A solução deve prover suporte a alta disponibilidade para o módulo de gerenciamento



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

2.3	A solução proposta deverá ter sido desenvolvida por um único fabricante de modo que tanto o suporte da solução quanto as funcionalidades sejam integradas e 100% compatíveis.
2.3.1	A solução ofertada não poderá ser do tipo opensource
2.4	A solução deve ser fornecida e dimensionada para monitorar o escopo completo de ativos da CONTRATANTE. Assim, é obrigatório que a solução cubra 100% definido pela CONTRATANTE, incluindo servidores físicos e virtuais, estações de trabalho, firewalls e ativos de rede, aplicações web, etc. e não somente parte do mesmo, de forma a prover uma visibilidade plena da segurança cibernética do ambiente.
2.4.1	O escopo dos ativos a serem monitorados e protegidos está definido no anexo "AMBIENTE DE TI - SEFAZ BA"
2.5	A solução deve possuir suporte ao IP (Internet Protocol) versão 4 e versão 6
2.6	A solução deve possibilitar a execução de verificações a partir de um endereço IP (Internet Protocol) ou de FQDN (Fully Qualified Domain Name);
2.7	Todas as atividades relativas à administração da solução e de seus componentes, incluindo configurações gerais, acompanhamento de resultados, geração de relatórios, ajustes e configuração dos módulos de varredura, deverão ser executadas através do módulo de gerenciamento
2.8	A solução deve possuir interface gráfica Web centralizada, compatível com os principais navegadores do mercado
2.9	A Solução deve possuir uma base de testes que permite identificar vulnerabilidades CVE
2.10	A Solução deve possuir uma base de testes que permite identificar vulnerabilidades NVD
2.11	A Solução deve permitir ajustes e alterações dos níveis severidade da vulnerabilidade
2.12	A Solução deve possuir em sua base de vulnerabilidades, para cada item cadastrado, no mínimo as seguintes informações: nome, descrição, nível de risco, score CVSS BASE, TEMPORAL e ENVIRONMENTAL, a partir da versão 2 e superior, referência (CVE, NVD ou outra fonte), solução e link para o download da correção (se aplicável), contramedidas (se aplicável), informação e fonte de exploit;
2.13	A solução deve ter uma base extensiva de assinaturas de vulnerabilidades
2.14	A solução deve atualizar a base de assinaturas pela internet



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		2.15	A solução deve suportar a atualização da base de assinaturas automaticamente ou através de agendamento
		2.16	Ser compatível com o padrão SCAP - v1.2 ou v1.3 (Security Content Automation Protocol), protocolo essencial e de garantia de qualidade em varreduras automatizadas em ativos de informação;
		2.17	Deve avaliar no mínimo os padrões de segurança OWASP Top 10 e PCI (payment card industry data security standard);
		2.18	Deve possuir integração com VMware vCenter para automaticamente popular bases de ativos do ambiente virtual;
		2.19	Geração de tickets para vulnerabilidades encontradas, permitindo marcar uma vulnerabilidade em determinado ativo como corrigida ou ignorada;
		2.20	Ter API para automação de processos e integração com produtos de terceiros, inclusive soluções PAM.
		2.21	Integração com a base de dados de vulnerabilidades CVE (Common Vulnerabilities and Exposures);
		2.22	Deve ser compatível com avaliação de RESTful APIs, utilizando o padrão OpenAPI (Swagger)
		2.23	Deve possuir nativamente scanners pré-configurados em nuvem, para realização de scans externos. Estes scanners deverão obrigatoriamente possuir IP dedicado, com divulgação pública, para configuração de whitelist em Firewalls, WAFs, ou outros sistemas de proteção.
		2.24	Recurso de base de conhecimento com, no mínimo, 75.000 (setenta e cinco mil) assinaturas de vulnerabilidades, com atualização automática a partir do site do fabricante;
3	REQUISITOS DE SEGURANÇA	3.1	A Solução deve prover o registro de atividades (logs) para fins de auditoria, de maneira a permitir o acompanhamento de todas as atividades executadas no sistema
		3.2	A Solução deve prover método de cópia de segurança (backup) e restauração da cópia de segurança (restore), contemplando, no mínimo, suas informações, configurações, políticas, usuários, credenciais e ativos
		3.3	Dados trafegados entre os agentes de varredura e o módulo de gerenciamento devem estar criptografados
		3.4	Deve ser possível alterar o user agent utilizado pela solução;
		3.5	A solução deve ser multiusuário, com níveis de permissões distintas para administração de funcionalidades, acesso a logs e emissão de relatórios;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		3.6	A solução deve permitir o acesso exclusivamente mediante o uso de MFA (autenticação multifator);
		3.7	O acesso à solução deve ser disponibilizado exclusivamente via interface web.
		3.8	Suportar no mínimo 03 (três) dos seguintes esquemas de autenticação:
		3.9	a) autenticação básica (digest);
		3.10	b) NTLM;
		3.11	c) form de login;
		3.12	d) autenticação de Cookies;
		3.13	e) autenticação através de Selenium;
4	MÓDULO DE GERENCIAMENTO	4.1	Gerenciamento único, centralizado, responsável pela aplicação das políticas de segurança, administração e controle das funcionalidades dos serviços;
		4.2	A solução deve possuir gerenciamento por WebUI (WEB User Interface) via HTTPS (Secure Hypertext Transfer Protocol);
		4.3	Gerenciamento com perfis de acessos distintos para administração de funcionalidades, acesso a logs e emissão de relatórios;
		4.4	Gerenciamento com visualização de status dos serviços;
		4.5	Gerenciamento com recurso de informações estatísticas de fluxo de tráfego, incluindo quantidade de conexões, throughput e desempenho dos serviços;
		4.6	Gerenciamento com recurso de auditoria de alteração de configurações e acesso à ferramenta de administração, incluindo usuário, data e horário de acesso e ações realizadas;
		4.7	Gerenciamento com recurso de replicação de configurações e atualização de software;
		4.8	Gerenciamento com recurso de monitoramento de logs, debugging e captura de pacotes;
		4.9	Gerenciamento com recurso de backup e importação automáticos de arquivos de configuração;
5	TIPOS DE ATIVOS A SEREM AVALIADOS	5.1	Detecção de vulnerabilidades em sistemas operacionais, protocolos e dispositivos de rede, aplicações WEB, ambiente Docker\RANCHER\KUBERNETS, ambiente de nuvem Microsoft, banco de dados, servidores físicos e virtuais, entre outros;
		5.2	Verificar vulnerabilidades em ambiente Windows, Linux e Red Hat, no mínimo: detecção de hot fixes, service packs, registros, backdoors, peer to peer, portas de serviço habilitadas e antivírus;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		5.3	Detectar vulnerabilidades em dispositivos de infraestrutura de redes (cabeadas e sem fio), aplicações baseadas em WEB, bases de dados, aplicações comerciais e sistemas operacionais.
		5.4	Deteção de vulnerabilidades em ambientes Oracle, SQL Server e outras plataformas de banco de dados,
6	VARREDURA	6.1	Deve ser capaz de agendar a varredura e determinar sua frequência entre uma única vez, diária, semanal, mensal e anual;
		6.2	Grupamento de eventos baseada em sistemas operacionais, endereços IP, nome DNS, nome NetBIOS, porta de serviços, porta/protocolo, banners e vulnerabilidades;
		6.3	Efetuar varredura à procura de vulnerabilidades;
		6.3.1	A solução deve possuir a capacidade de determinar quais vulnerabilidades podem ser exploradas, para cada ativo onde são encontradas
		6.4	Varredura de ativos de modo intrusivo e não intrusivo;
		6.5	Capacidade de selecionar e agrupar ativos encontrados, com possibilidade de incluir faixa de exclusão de endereços IP para varredura;
		6.6	Capacidade de definir templates de configuração de scans e de agendamento de scans;
		6.7	Capacidade de configuração de usuário e senha para realização de varredura autenticada de sistemas operacionais e aplicações;
		6.8	Capacidade de detectar congestionamento de rede e limitar os seguintes aspectos da varredura:
		6.8.1	a) limite em segundos para timeout de requisições de rede;
		6.8.2	b) número máximo de timeouts antes que a varredura seja abortada;
		6.9	Atualização automática de tabela de ativos monitorados, contendo informações sobre serviços e vulnerabilidades encontradas por ativo;
		6.10	O sistema deve manter um histórico das varreduras para ajudar a organização em uma jornada de mitigação
7	AVALIAÇÃO DE VULNERABILIDADE APLICAÇÕES	7.1	Para vulnerabilidades de injeção de código (SQL, XSS, XSRF, etc.), deve evidenciar nos detalhes do evento encontrado
		7.1.1	a) payload injetado;
		7.1.2	b) evidência em forma de resposta da aplicação;
		7.1.3	c) detalhes da requisição HTTP;
		7.1.4	d) detalhes da resposta HTTP;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

7.2	Analisar diariamente no mínimo 25 (vinte e cinco) sites contra-ataques, tais como cross-site scripiting, SQL injection e DoS;
7.3	Deve possuir suporte a varreduras de componentes para no mínimo: Wordpress, Blog Designer Plugin for Wordpress, Event CalendarPlugin for Wordpress, Convert Plus Plugin for Wordpress, AngularJS, Apache, Apache Tomcat, Apache Spark e Apache Struts, Atlassian Confluence, AtlassianCrowd e Atlassian Jira, Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla!, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik, ThinkPHP, Webmin e YUI;
7.4	Capacidade de identificação de links em aplicações WEB e de navegação pelos links identificados;
7.5	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;
7.6	Deve permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;
7.7	Deve ser capaz de utilizar scripts customizados de crawl com parâmetros definidos pelo usuário;
7.8	Deve ser capaz de excluir determinadas URLs da varredura através de expressões regulares;
7.9	Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;
7.10	deve ser capaz de instituir no mínimo os seguintes limites:
7.11	a) número máximo de URLs para crawl e navegação;
7.12	b) número máximo de diretórios para varreduras;
7.13	c) tempo máximo para a varredura;
7.14	d) número máximo de conexões HTTP ao servidor hospedando a aplicação Web;
7.15	e) número máximo de requisições HTTP por segundo;
7.16	Deve avaliar sistemas web utilizando frameworks modernos, como AJAX, HTML5 e SPA;
7.17	Deve possibilitar a definição de atributos no cabeçalho (HEADER) da requisição HTTP de forma personalizado a ser enviada durante os testes;
7.18	Deve ser possível excluir a interação com elementos DOM durante o Scan. Esta exclusão poderá ser configurada para cada elemento, sendo possível escolher o Conteúdo do texto ou do Atributo CSS.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		7.19	O sistema deve ser capaz de varrer aplicações web em busca de vulnerabilidades
		7.20	Deve ser possível agendar varreduras em diferentes aplicações
		7.21	Os resultados devem ter a capacidade de se integrar para mostrar o desempenho da organização como um todo e também de uma aplicação específica
8	AVALIAÇÃO DE VULNERABILIDADE IMAGENS E CONTAINERS	8.1	O sistema deve ser capaz de varrer containers baseado em dockers em busca de fragilidades e vulnerabilidades
		8.2	Deve ser capaz de realizar uma análise dinâmica nas diferentes bibliotecas utilizadas em cada imagem de containers, informando os riscos e o que deve ser feito para mitigá-lo
		8.3	O sistema deve ser capaz também de analisar a configuração e vulnerabilidades no sistema de gerenciamento dos containers baseado em Kubernetes
		8.4	O sistema deve manter um histórico das varreduras para ajudar a organização em uma jornada de mitigação
		8.5	Deve possuir capacidade de realizar o escaneamento de vulnerabilidades em imagens e containers, bem como de se integrar com fluxo de integração contínua (Ambiente Docker\Rancher\Kubernetes);
		8.6	Deve possuir capacidade de realizar o escaneamento de vulnerabilidades em imagens e containers, bem como de se integrar com fluxo de integração contínua com pelo menos 2 (dois) dos seguintes ambientes: Ambiente Docker, Rancher e Kubernetes;
		8.7	Deve possuir integração com Microsoft Azure Container, Vmware Harbor ou Sonatype Nexus para importar e analisar imagens;
		8.8	Deve prover integração com pelo menos 4 (quatro) das seguintes plataformas de integração contínua: Bamboo, CircleCI, Codeship, Distelli, Drone.io, Jenkins, Shippable, Solano Labs, Travis CI, Wrecker e Kubernetes;
		8.9	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;
		8.10	Deve possuir conectores e permitir importação de imagens dos seguintes repositórios:
		8.10.2	b) AWS ECR;
		8.10.3	c) JFrog Artifactory;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

9	AVALIAÇÃO DE VULNERABILIDADE NUVEM	9.1	A solução deve realizar uma análise de configuração de grandes provedores de clouds informando um baseline mínimo a ser atendido. Deve ser capaz de analisar pelo menos os seguintes provedores:
		9.1.1	Google Cloud Platform
		9.1.2	Amazon Web Services
		9.1.3	Microsoft Azure
		9.2	A solução deve possuir análise por benchmarks e compliance para os seguintes padrões em formato de Dashboard para o ambiente de nuvem: - CIS; - NIST; - ISO-27001; - HIPAA; - PCI-DSS; - CCM; - GDPR;
10	AVALIAÇÃO DE VULNERABILIDADE ACTIVE DIRECTORY	10.1	A solução deve oferecer uma análise detalhada e contínua da segurança do Active Directory, identificando vulnerabilidades, configurações incorretas e possíveis ataques através de uma abordagem que não depende de agentes ou sensores. Ela deve incluir medidas preventivas de hardening, recomendações de correção específicas, e capacidade de monitoramento de alterações em tempo real, sem armazenar ou sincronizar credenciais. Se integrar facilmente com SIEMs, suportar a criação de dashboards customizados e utilizar um modelo de controle de acesso baseado em funções, e proporcionando gestão eficaz através de uma interface web.
		10.2	A solução deve oferecer a verificação dos possíveis tipos de ataques em tempo real no Active Directory, Zerologon Exploitation, DNSAdmins, DPAPI Domain Backup Keys, NTDS Extraction, Kerberoasting, PetitPotam, DCSshadow, Password Guessing, Golden Ticket, DCSync.
		10.3	A solução deve analisar em detalhes um ataque explorando as descrições através do framework MITRE ATT&CK;
		10.4	A solução deve apresentar alterações no Active Directory, seus objetos e atributos em tempo real.
		10.5	A solução deve produzir regras YARA na detecção de ataques (Ex. DCSync, Golden Ticket) identificados pela ferramenta;
11	AVALIAÇÃO DE VULNERABILIDADE AMBIENTE DE TI	11.1	Apresentação de relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição do parque computacional do CONTRATANTE em relação aos riscos de segurança em TI, contendo: hosts encontrados, topologia de rede, serviços, vulnerabilidades descobertas, nível de risco por plataforma e por vulnerabilidade;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		11.2	A solução deve permitir um acompanhamento histórico do nível de exposição da organização;
12	AVALIAÇÃO DE VULNERABILIDADE CONFIGURAÇÃO DE ATIVOS	12.1	A solução deve suportar funcionalidades de Scan/Análise de compliance de configuração de ativos de TI utilizando framework de compliance SIS, NIST
		12.2	A solução deve realizar verificações de auditoria contendo as de segurança, com indicação de sucesso ou falha, baseado nos principais frameworks reconhecidos pela indústria, pelo menos os seguintes: - Center for Internet Security Benchmarks (CIS); - Defense Information Systems Agency (DISA) STIGs; - Health Insurance Portability and Accountability Act (HIPAA); - Payment Card Industry Data Security Standards (PCI DSS);
		12.3	A solução deve fornecer auditorias de configuração com base benchmarks em CIS (Center for Internet Security) L1 e L2, para ambos os sistemas operacionais Microsoft Windows e Linux;
13	CRITICIDADE DOS ATIVOS	13.1	Classificar criticidade para priorização dos ativos segundo sua importância para os serviços, grau de exposição, serviço hospedado etc.
		13.2	Levantamento e classificação de criticidade de ativos, baseada na importância do ativo e nas vulnerabilidades encontradas.
		13.3	Deve permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução;
		13.4	Definição de, no mínimo, 3 (três) níveis de criticidade de vulnerabilidades;
14	CÁLCULO DE RISCO	14.1	A solução deve ser capaz de calcular o risco da vulnerabilidade não se baseando apenas na ameaça e na sua criticidade (CVSS) mas deve conter aspectos dinâmicos que se adaptam ao ambiente a que a solução esteja analisando
		14.2	O cálculo dos riscos deve levar em consideração:
		14.2.1	Criticidade da Vulnerabilidade baseada no CVSS;
		14.2.2	Idade da vulnerabilidade;
		14.2.3	Disponibilidade e idade do exploit público
		14.2.4	Porcentagem do ambiente afetado
		14.2.5	Proximidade da internet
14.2.6	Tipos de dados que aquele ativo possua, por exemplo, dados pessoais ligados a LGPD (Lei Geral de Proteção de Dados) devem ser caracterizados como ativos críticos		



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		14.2.7	Alertas de inteligência, se aquela vulnerabilidade está sendo usada por uma campanha recente de malware, por exemplo
		14.3	O cálculo dos riscos deve ser periódico, mínimo de 2 (duas) vezes ao dia. Exemplo: o cálculo deve ser recalculado se um exploit for publicado para uma vulnerabilidade específica
		14.4	Apresentação de graduação de riscos, baseada em pontuação, que permite medir o nível de riscos dos recursos e sistemas encontrados;
		14.5	A solução deve permitir configurar, com base na avaliação do risco de ativos e grupos de ativos, a priorização da correção de vulnerabilidades
15	CLASSIFICAÇÃO DOS ATIVOS	15.1	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);
		15.2	Deve permitir ajustar os critérios e pontuações de riscos já existentes na ferramenta como também criar novas regras de negócio que contribuam para a análise e pontuação de risco para atividades consideradas suspeitas ou que precisam ser monitoradas;
		15.3	Deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;
		15.3.1	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;
		15.4	A solução deve gerar uma pontuação global referente a exposição cibernética da organização baseado nas pontuações de cada um dos ativos;
		15.5	A solução deve permitir a segregação lógica entre áreas distintas da empresa afim de obter a pontuação referente exposição cibernética por área;
		15.6	A solução deve permitir a segregação lógica entre aplicações distintas da empresa afim de obter a pontuação referente exposição cibernética por aplicação;
16	RESPOSTA A VULNERABILIDADES	16.1	Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;
		16.2	Apresentação de procedimentos necessários para eliminar, remediar ou mitigar vulnerabilidades encontradas, tais como indicação de atualizações de software;
		16.3	Recurso de alertas por e-mail de vulnerabilidades encontradas;
		16.4	A solução deve possuir a capacidade de indicar um plano de tratamento de vulnerabilidades de forma automática



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

17	INTEGRAÇÃO COM ANTIVÍRUS	17.1	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;
		17.2	A solução deve fornecer auditoria de programas antivírus para determinação de presença e status de inicialização para no mínimo os seguintes produtos: TrendMicro Office Scan, Trellix Endpoint Security, Microsoft Defender for Endpoint e Kaspersky;
18	DASHBOARDS	18.1	A solução deve permitir a visualização de dashboards através de navegador web
		18.2	A interface de dashboards não deve utilizar o plugin do navegador Flash
		18.3	A interface de dashboards não deve utilizar o plug-in do navegador Java
		18.4	A solução deve possuir dashboards pré-definidos para rápida visualização dos resultados
		18.5	A solução deve possibilitar a criação de dashboards personalizados
		18.6	Os dashboards da solução deverão possibilitar a exibição das mesmas informações em diferentes níveis de detalhamento e representação gráfica
		18.7	A solução deve possuir dashboard que informem resultados gerenciais das varreduras de vulnerabilidades, incluindo o nível de risco dos resultados
		18.8	As informações apresentadas nos dashboards deverão ser apresentadas em diversos formatos, incluindo gráficos e tabelas
19	RELATÓRIOS	19.1	A solução deve emitir relatório de vulnerabilidades com os resultados encontrados nas varreduras
		19.2	A solução deve permitir a personalização do formato do relatório de vulnerabilidades
		19.3	A solução deve permitir que uma vulnerabilidade identificada seja suprimida do relatório, e prover a alteração dos resultados no mesmo
		19.4	A solução deve emitir relatório de vulnerabilidades com comparativo ou diferencial entre varreduras
		19.5	A solução deve emitir relatório do histórico de vulnerabilidades, personalizável por ativo e por período;
		19.6	A solução deve emitir relatório indicando os níveis de severidade para as vulnerabilidades encontradas, de modo a priorizar as ações a serem desenvolvidas
		19.7	A solução deve emitir relatório do tipo resumo gerencial



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		19.8	A solução deve emitir relatório do tipo parcial, contendo o resumo das vulnerabilidades encontradas
		19.9	A solução deve emitir relatório do tipo detalhado, contendo o histórico e situação das vulnerabilidades encontradas, as diferentes visões de severidade e risco para ativos verificados
		19.10	A Solução deve disponibilizar relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição dos ativos aos riscos identificados com pelo menos, as seguintes informações
		19.10.1	Indicador de Risco (baseado em especificidades do ambiente);
		19.10.2	Descrição da vulnerabilidade
		19.10.3	Nível de risco
		19.10.4	Cálculo e criticidade CVSS
		19.10.5	Solução e link para o download da correção, caso aplicável
		19.10.6	Contramedidas, caso aplicável
		19.10.7	Informação e fonte do exploit
		19.10.8	A solução deve permitir a exportação dos resultados para arquivo, sob demanda ou agendamento em, pelo menos, 2 (dois) dos seguintes formatos: CSV, XML, HTML, DOCX ou PDF, com possibilidade de seleção das informações que irão compor o arquivo
20	CICLO DE VIDA DE VULNERABILIDADES	20.1	A solução deve permitir acompanhar o ciclo de vida da vulnerabilidade. Identificando o primeiro momento em que ela foi identificada no ambiente e sua propagação a cada scan.
		20.2	A solução deve permitir gerenciar a evolução das vulnerabilidades ao longo do tempo para cada um dos ativos
		20.2.1	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;
		20.3	A solução deve permitir o acompanhamento de todas as vulnerabilidades que estejam em aberto;
		20.4	A solução deve permitir o acompanhamento de todas as vulnerabilidades corrigidas e não corrigidas;
		20.5	A Solução deve prover cálculo de risco das vulnerabilidades identificadas, utilizando variáveis que possam ser personalizadas pelo usuário da solução;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

		20.6	A Solução deve possuir capacidade de classificar e priorizar as vulnerabilidades de acordo com o CVSS (Common Vulnerability Scoring System);
		20.7	A solução deve identificar vulnerabilidades que possuem patches de correção disponíveis
		20.8	A solução deve correlacionar as vulnerabilidades encontradas com bases de dados de exploit, a fim de priorizar as vulnerabilidades que possuem exploits prontos para sua exploração
		20.9	A solução deve permitir aceite de risco de vulnerabilidades
		20.10	A solução deve permitir listar todas as vulnerabilidades aceitas
		20.11	A solução deve prover informação descritiva das vulnerabilidades, com impacto, criticidade, evidências e recomendações
		20.12	A solução deve permitir a inserção de comentários nos ativos ou vulnerabilidades para notas de controles internos e usos diversos
21	SIZING	21.1	A solução deve suportar, pelo menos, 80 (oitenta) varreduras simultâneas
		21.2	A solução deve ser capaz de avaliar, como mínimo, 5.000 (cinco mil) usuários ativos no Active Directory.
22	GERENCIAMENTO E SUSTENTAÇÃO	22.1	Gerenciamento e sustentação da ferramenta de Avaliação de Vulnerabilidades fornecida, conforme requisitos deste Termo de Referência, para suportar a execução do serviço Gerenciamento de Vulnerabilidades a ser executado pela EquipeSEFAZ BA.
		22.2	Planejar, instalar, implementar e manter ferramenta de Avaliação de Vulnerabilidades para automatizar e acelerar o tratamento de vulnerabilidades no ambiente de TI da SEFAZ BA.
		22.3	A ferramenta de Avaliação de Vulnerabilidades fornecida e gerenciada pela CONTRATADA deve ter contrato de suporte técnico vigente junto ao fabricante da solução durante todo o período de execução dos serviços previstos neste Termo de Referência.
		22.4	A CONTRATADA deve manter as regras atualizadas, de modo a refletir a ocorrência de novas ameaças, novas políticas de alarme, atualizações de padrões de logs de tecnologias, escopo monitorado ou para reduzir a ocorrência de falsos positivos;
		22.5	A SEFAZ BA pode solicitar, a qualquer momento, a implementação de regras de correlacionamento a serem implementadas na ferramenta de SIEM, baseadas na necessidade do negócio. A CONTRATADA deve avaliar os requisitos técnicos necessários e operacionalizar as regras na ferramenta. As solicitações devem ser registradas e realizadas por meio dos canais estabelecidos neste Termo de Referência;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

8. ETAPA - IMPLANTAÇÃO DO CENTRO DE OPERAÇÕES DE SEGURANÇA (SOC)

8.1. Reunião de Kick-off – Aprovação do Plano de Implantação.

- 8.1.1. A CONTRATADA deverá se reunir com os gestores do contrato da SEFAZ BA, em local a ser definido pela SEFAZ BA, **no prazo máximo de 15 (quinze) dias corridos a contar da data da subscrição da Autorização de Prestação de Serviços – APS**. A reunião deverá ser agendada em comum acordo com a SEFAZ BA.
- 8.1.2. Nesta reunião, a CONTRATADA deverá:
 - 8.1.2.1. Apresentar quem será o Gestor Técnico e o profissional técnico que atuará como coordenador da Etapa – Implantação do SOC, incluindo as atividades de instalação e implementação das soluções de TI contratadas;
 - 8.1.2.2. Apresentar as características e documentação dos serviços e soluções de TI fornecidos e/ou utilizados, estratégia de implantação e operação além de esclarecer todos os questionamentos técnicos;
 - 8.1.2.3. Apresentar e validar junto à SEFAZ BA o planejamento da etapa de implantação dos serviços, soluções e processos conforme ENCARTÉ A: Implantação do SOC
 - 8.1.2.4. Apresentar quem será o preposto do contrato por parte da CONTRATADA para tratar de questões comerciais e/ou contratuais.

8.2. Execução – Plano de Implantação do SOC

- 8.2.1. As atividades previstas no Plano de Implantação do SOC deverão ser executadas e concluídas em um prazo de 90 (noventa dias) após a reunião de kick-off. Apresentar quem será o preposto do contrato por parte da CONTRATADA para tratar de questões comerciais e/ou contratuais.

9. CONDIÇÕES GERAIS PARA PRESTAÇÃO DOS SERVIÇOS

9.1. Ferramentas utilizadas na prestação de serviços

- 9.1.1. A CONTRATADA deverá possuir, para todas as ferramentas utilizadas na prestação dos serviços, garantia e suporte contratado, para toda a vigência do contrato, com o fabricante dos hardwares e softwares fornecidos, garantindo pronto atendimento pelo Fabricante;
- 9.1.2. A garantia e suporte das ferramentas utilizadas na prestação dos serviços deverá considerar o período contratado a partir da data de emissão do Termo de Aceite e contemplar a prestação dos serviços de atualização de versão das licenças de software e de suporte técnico;
- 9.1.3. A garantia das ferramentas utilizadas na prestação dos serviços pela contratada não deve imputar qualquer custo adicional à SEFAZ BA;
- 9.1.4. A modalidade de atendimento deverá ser em regime 24x7 (24 horas por dia x 7 dias da semana), de segunda a domingo, incluindo os feriados;
- 9.1.5. Durante o período de contratação dos serviços, a contratada deverá manter todas as ferramentas utilizadas atualizadas (atualizações de versões, releases e patches);
- 9.1.6. Caso as condições de licenciamento dos softwares utilizados na prestação do serviço sejam alteradas pelo fabricante durante o período de garantia, as funcionalidades e os quantitativos definidos não deverão ser prejudicados. Nas situações em que a alteração na forma de licenciamento implique em perdas qualitativas e/ou quantitativas, licenças complementares deverão ser fornecidas, sem custo adicional.

9.2. Registro e Atendimento de Ocorrências

- 9.2.1. As informações sobre os canais de atendimento para abertura dos chamados deverão ser apresentadas à SEFAZ BA no prazo máximo de 10 (dez) dias úteis, contados a partir do dia seguinte à assinatura do Contrato;
- 9.2.2. Os chamados para realização de atividades operacionais de segurança devem ser abertos por meio de central de atendimento da CONTRATADA localizado no Brasil, a partir de número de ligação gratuita (0800), em regime 24x7x365 (24 horas por dia, 7 dias na semana, 365 dias no ano), com



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

- atendimento em língua portuguesa, ou por meio de portal de serviços na internet;
- 9.2.3. No provimento deste serviço por meio de telefone (0800) a CONTRATADA fica obrigada a permitir o recebimento de ligações de terminais fixos e móveis;
 - 9.2.4. Para os atendimentos por meio de telefone (0800), o tempo máximo de espera deverá ser de até 03 (três) minutos;
 - 9.2.5. No momento de abertura de chamados, deve ser fornecido à SEFAZ BA um número único de identificação da demanda, com classificação e prioridade de acordo com as melhores práticas de segurança ou a pedido de priorização da CONTRATANTE. Assim, deve ser encaminhada uma notificação, contendo as informações de registro do chamado, para endereço eletrônico de e-mail da SEFAZ BA;
 - 9.2.6. As informações referentes a chamados, incluindo providências e ações de resolução tomadas, devem ser armazenadas em sistema de controle de chamados (SISTEMA DE TICKETS) da CONTRATADA, cujo acesso deve estar disponível à SEFAZ BA. Nesse sentido, devem ser criadas contas de acesso para a equipe de servidores designados pela SEFAZ BA, para fins de acompanhamento e auditoria de chamados, sendo possível a extração de relatórios compreendendo o período integral do contrato;
 - 9.2.7. A CONTRATADA deve realizar os devidos escalonamentos de acordo com a prioridade e nível de atendimento dos chamados, reportados pela SEFAZ BA ou pelo sistema de monitoramento da CONTRATADA;
 - 9.2.8. A critério exclusivo da SEFAZ BA, a contagem de tempo somente pode ser interrompida: caso a CONTRATADA apresente, tempestivamente, razões que comprovem a ocorrência de fatos que fogem do seu controle, aceitas pela SEFAZ BA; quando ações necessárias para a resolução de chamados tenham sido agendadas pela CONTRATADA em conjunto com a SEFAZ BA; e quando forem necessárias ações da SEFAZ BA;
 - 9.2.9. Em qualquer mudança na situação de chamados, deve ser encaminhada uma notificação à SEFAZ BA, contendo as informações de registro do chamado, para endereço eletrônico de e-mail, inclusive quando houver mudança de status;
 - 9.2.10. Os chamados abertos somente podem ser concluídos e fechados após autorização da SEFAZ BA;
 - 9.2.11. Ao encerrar cada chamado o sistema de controle de chamados deve permitir a avaliação da qualidade do atendimento;
 - 9.2.12. Se a SEFAZ BA autorizar a conclusão de chamado devido a CONTRATADA alegar que não pode resolver o chamado ou que o chamado não diz respeito aos serviços que ela presta e depois ficar comprovado que a CONTRATADA poderia ter investigado melhor o chamado e o resolvido, o chamado será reaberto e a contagem de tempo será retomada, considerando também o período em que o chamado ficou fechado indevidamente para computo do SLA e penalidades associadas;
 - 9.2.13. Se o chamado já tiver sido resolvido por servidor da SEFAZ BA a reabertura terá como finalidade apenas a correção da contagem tempo de atendimento e o tempo de encerramento será considerado aquele que o servidor da SEFAZ BA incluir evidência no chamado que comprove que a CONTRATADA deveria ter resolvido o problema. Se o chamado ainda não possuir resolução ele continuará aberto até que a CONTRATADA resolva definitivamente o chamado;
 - 9.2.14. Para que um chamado seja considerado concluído, os serviços executados devem ser adequadamente documentados, evidenciados e arquivados no sistema de controle de chamados (SISTEMA DE TICKETS). A documentação entregue deve ser simplificada para esclarecer os procedimentos executados e permitir que servidores da SEFAZ BA possam repetir as ações tomadas posteriormente;
 - 9.2.15. Caso seja necessária a elaboração de uma documentação detalhada dos procedimentos executados, incluindo justificativas técnicas, esclarecimentos e gráficos, a SEFAZ BA pode solicitar através de abertura de chamado;
 - 9.2.16. Não deverá haver qualquer limitação para o número de técnicos da SEFAZ BA autorizados a abrir chamados;
 - 9.2.17. Não deverá haver qualquer limitação para o número de solicitações;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

10. INDICADORES DE DESEMPENHO E PENALIZAÇÕES

- 10.1. Um dos instrumentos de acompanhamento do contrato será a gestão por indicadores medidos em intervalos mensais. Esses indicadores fornecem parâmetros objetivos através dos quais se busca medir a qualidade dos serviços prestados. A lista dos níveis mínimos de serviço está descrita no **ENCARTE B: Nível Mínimo de Serviço (NMS)**, com a definição detalhada, as condições segundo as quais eles devem ser considerados, a maneira como deve ser efetuada a medição, os valores de referência e as metas a serem alcançadas, assim como as possíveis penalizações;
- 10.2. Os primeiros 90 (noventa) dias da Etapa – Operações dos Serviços, após o início da execução dos serviços serão considerados como período de estabilização, durante o qual a CONTRATADA deverá proceder todos os ajustes que se mostrarem necessários, no dimensionamento e qualificação das equipes, bem como nos procedimentos adotados e demais aspectos da prestação dos serviços de modo a assegurar o alcance das metas estabelecidas. Caso haja prorrogação da vigência contratual, não haverá novo período de estabilização;
- 10.3. O período de estabilização não elimina a possibilidade de a SEFAZ BA aplicar as penalidades previstas;
- 10.4. A frequência de aferição e avaliação dos níveis de serviços será mensal, do primeiro ao último dia de cada mês, devendo a CONTRATADA elaborar relatório gerencial de serviços, apresentando-o à SEFAZ BA até o 5º. (quinto) dia útil do mês subsequente ao da prestação dos serviços;
- 10.5. Devem constar nesse relatório, no mínimo, os indicadores/metras de níveis de serviços definidos e alcançados, quantidade de incidentes, problemas, mudanças ocorridas no período;
- 10.6. O conteúdo detalhado, as formas do relatório gerencial serão definidas pelas partes na Etapa - Implantação do SOC e poderá sofrer ajustes durante a execução do contrato, a critério da SEFAZ BA, visando melhorar a avaliação dos serviços prestados;
- 10.7. O Nível Mínimo de Serviços deve ser considerado e entendido pela CONTRATADA como um compromisso de qualidade que assumirá junto à SEFAZ BA;
- 10.8. A análise dos resultados das avaliações, pela SEFAZ BA, poderá resultar em advertências, penalizações e redução na fatura, caso a CONTRATADA não cumpra os compromissos ou Níveis Mínimos de Serviços acordados em contrato;
- 10.9. Obedecendo a pontuação atribuída na Tabela 1 do **ENCARTE B: Nível Mínimo de Serviço (NMS)** para cada inadimplemento dos Níveis Mínimos de Serviços, o CONTRATANTE aplicará glosa de 1% (um por cento) sobre o valor da nota fiscal a cada 15 pontos, limitada a glosa total ao percentual máximo de 30% (trinta por cento) do valor mensal previsto em contrato, devendo o CONTRATANTE cientificar à CONTRATADA sobre as razões que ensejaram o desconto;
- 10.10. Em caso extremo de descumprimento dos Níveis de Serviço acordados, a SEFAZ BA pode vir a encerrar o Contrato de acordo com o previsto na lei;
- 10.11. No atendimento das solicitações, para efeitos de apuração do tempo gasto pela CONTRATADA para a apuração do Níveis Mínimos de Serviços, serão desconsiderados os períodos em que a SEFAZ BA estiver responsável por executar ações necessárias para a análise e atendimento da solicitação;
- 10.12. À CONTRATADA será garantido o direito à apresentação de defesa prévia, no prazo de 5 (cinco) dias úteis, contados a partir do dia seguinte à confirmação de recebimento da notificação da penalização. Cabe à SEFAZ BA a solução final e definitiva da questão;

11. SANÇÕES ADMINISTRATIVAS

- 11.1. O CONTRATANTE poderá aplicar as seguintes sanções, assegurados o contraditório e a ampla defesa:
- 11.2. Advertência;
- 11.3. MULTA MORATÓRIA de 0,5% (zero vírgula cinco por cento) sobre o valor mensal do contrato, por dia de atraso na apresentação da nota fiscal de faturamento, de acordo com os níveis de serviços e eventuais glosas apuradas pelo CONTRATANTE;
- 11.4. MULTA MORATÓRIA – de 1,5% (um vírgula cinco por cento) sobre o valor mensal do contrato, a cada ocorrência em que a CONTRATADA:
- 11.5. Por motivo de negligência, imprudência ou imperícia na execução das atividades contratuais, causar



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

- qualquer dano físico ou lógico aos equipamentos da SEFAZ BA;
- 11.6. Descumprir Política, Norma ou Procedimento de Segurança da Informação do SEFAZ BA;
 - 11.7. Deixar de comunicar formalmente à SEFAZ BA sobre o desligamento de prestador de serviço (profissional que prestava serviço remotamente);
 - 11.8. MULTA MORATÓRIA de 10% (dez por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto no ENCARTE B: Nível Mínimo de Serviço (NMS), durante 3 (três) meses consecutivos ou 5 (cinco) meses alternados, apurados em um período de 12 (doze) meses);
 - 11.9. MULTA MORATÓRIA de 20% (vinte por cento) do valor mensal do contrato pelo não atingimento de um mesmo nível de serviço previsto no ENCARTE B - NÍVEL MÍNIMO DE SERVIÇO, durante 6 (seis) meses consecutivos ou 10 (cinco) meses não consecutivos, apurados em um período de 12 (doze) meses);
 - 11.10. MULTA COMPENSATÓRIA de 10% (dez por cento) do valor total do contrato, em caso de INEXECUÇÃO PARCIAL das obrigações contratuais;
 - 11.11. MULTA COMPENSATÓRIA de 20% (vinte por cento) do valor total do contrato, em caso de inexecução total das obrigações contratuais;
 - 11.12. Outras sanções previstas em lei;

12. DISPOSIÇÕES GERAIS

- 12.1. Os itens de software deverão constar na Proposta de Preços com os respectivos identificadores (Part Numbers – Códigos dos Produtos) da FABRICANTE e estarem presentes em seus catálogos de produtos ou comprovados através de carta da FABRICANTE.
- 12.2. A apresentação dos Part Numbers – Códigos dos Produtos a serem fornecidos, se faz necessário para comprovação, pela CONTRATANTE, de que os produtos ofertados na Proposta de Preços da LICITANTE serão os efetivamente entregues, além de facilitar a identificação dos produtos nas documentações apresentadas para validação dos requisitos técnicos solicitados.
- 12.3. Todas as licenças e suas extensões necessárias ao cumprimento do descrito e exigido neste Termo de Referência, independentemente da modalidade ou metodologia de licenciamento, visando a garantia e o pleno funcionamento do software, devem ser fornecidas, respeitando todos os demais itens do EDITAL e discriminadas na tabela de itens e identificadores (Part Numbers – Códigos dos Produtos) correspondente.
- 12.4. Todas as características declaradas devem ser descritas pelas LICITANTES e comprovadas através de documentos de domínio público emitidos pela FABRICANTE, tais como: catálogos, manuais, fichas de especificação técnica ou páginas da Internet impressas, onde o produto ou componente ofertado seja claramente descrito em forma visual e/ou escrita.
- 12.5. Os materiais informativos utilizados para comprovar as especificações dos produtos ofertados deverão ser apresentados no idioma português (Brasil) ou inglês.
- 12.6. A comprovação dos requisitos técnicos, a ser apresentada na Proposta de Preços, deverá também ser gravada em mídia com arquivos pesquisáveis - visando facilitar o acesso e agilizar a verificação e a consulta das informações.
- 12.7. A comprovação resumida dos requisitos técnicos, a ser apresentada na Proposta de Preços, deverá seguir o modelo descrito no ENCARTE I: Modelo para Comprovação Resumida dos Requisitos Técnicos, onde as colunas Item/Subitem e Descrição do Requisito Técnico devem conter as referências das Especificações Técnicas deste Edital e a coluna Comprovação Técnica deve conter o Nome e a Página do documento de comprovação, do requisito técnico solicitado, apresentado pela LICITANTE.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA
ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE A
IMPLANTAÇÃO DO SOC

Nesta primeira etapa deve ocorrer a estruturação do Centro de Operações de Segurança - SOC de forma a suportar a operação dos serviços gerenciados de segurança, conforme os requisitos definidos neste Encarte A e no Termo de Referência.

1. ESCOPO

Estruturação do Centro de Operações de Segurança (SOC) conforme descrito abaixo para suportar a Etapa – Operação dos Serviços.

- 1.1. Estruturação do Centro de Operações de Segurança (SOC) conforme descrito a seguir para suportar a Etapa – Operação dos Serviços.
- 1.2. Esta etapa deve ser executada em até 90 (noventa) dias corridos após a reunião de kick-off, contemplando as atividades descritas neste encarte e a produção dos entregáveis associados que devem ser homologados pela SEFAZ BA.

2. EQUIPE TÉCNICA

- 2.1. Cabe a contratada a estruturação, administração e supervisão da equipe técnica responsável pelo serviço de Implantação do SOC, nomeada EquipeSOC de IMPLANTAÇÃO.
- 2.2. O dimensionamento da equipe técnica deve ser em quantitativo que garanta o seu funcionamento no horário de operação definido neste Termo de Referência, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados.
- 2.3. A EquipeSOC de IMPLANTAÇÃO não precisa ter dedicação exclusiva à prestação dos serviços objeto deste Termo de Referência.
- 2.4. A capacitação técnica e experiência da equipe técnica deve garantir a qualidade dos serviços e informações prestadas, atuando conforme o estado da arte e melhores práticas em termos de Segurança da Informação, e de acordo com os Níveis Mínimos de Serviço (NMS) determinados neste Termo de Referência.
- 2.5. Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ou certificações oficiais válidas e ativas, conforme os requisitos específicos para o perfil profissional descritos no ANEXO II - PERFIL PROFISSIONAL

3. HORÁRIO DE OPERAÇÃO

- 3.1. As atividades previstas na Etapa Implantação do SCO deverão ser prestadas no período das 08:00



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

às 18:00 horas, de segunda à sexta-feira, podendo ser de forma presencial nas dependências da SEFAZ BA, ou nas dependências da CONTRATADA, conforme planejamento a ser definido.

4. ATIVIDADES PREVISTAS

- 4.1. Estruturar os processos, procedimentos e instruções necessários a operação dos serviços, entre eles:
 - ITIL - Central de Serviços (Requisições, Incidentes e Problemas);
 - Monitoramento de Eventos;
 - Resposta a Incidentes de Segurança;
 - Gerenciamento de Vulnerabilidades.
- 4.2. Elaborar playbooks para suportar os serviços abaixo e outros que se fizerem necessários à operação do Centro de Operações de Segurança (SOC):
 - Monitoramento de Eventos;
 - Resposta a Incidentes de Segurança;
 - Gerenciamento de Vulnerabilidades.
- 4.3. Linha de Base - Eventos de Segurança
Definição de linha de base (baseline) de forma a entender o comportamento normal do ambiente monitorado, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção.
- 4.4. Estruturar regras de correlacionamento de eventos
Definir 200 (duzentas) regras ou 30 (trinta) modelos de ameaças de correlação especializadas na detecção de incidentes de segurança que serão produzidas e configuradas na ferramenta de SIEM.
- 4.5. Criticidade e priorização
 - Determinar critérios para definir criticidade e priorização de eventos de segurança;
 - Determinar critérios para definir criticidade e priorização de incidentes de segurança;
 - Determinar critérios para definir criticidade dos ativos e priorização das ações de remediação e/ou mitigação de incidentes e vulnerabilidades.
- 4.6. Regras e Políticas
Estruturar e configurar as regras e políticas a serem implementadas nas soluções da Plataforma de Segurança (IPS, NAC, EPP, FW, Antispam, etc. conforme descrito neste Termo de Referência).
- 4.7. Dashboard
Estruturar e configurar dashboards associados ao gerenciamento de eventos, resposta a incidentes, vulnerabilidades e soluções da plataforma de segurança, assim como indicadores e métricas definidas.
- 4.8. Relatórios
Estruturar e implementar os relatórios a serem fornecidos conforme Termo de Referência.
- 4.9. Indicadores e métricas
Estruturar e implementar de forma automática o cálculo e publicação dos indicadores e métricas definidos de acordo com os Níveis Mínimos de Serviço (NMS) determinados.
- 4.10. Indicadores e métricas
Definir, implementar e medir o score de segurança da SEFAZ BA associado as soluções da plataforma de segurança.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

- 4.11. Implantação das ferramentas fornecidas
- Implantar a solução de SIEM, integrando ao ambiente da SEFAZ BA, incluindo plataforma de segurança;
 - Implantar a solução de Avaliação de Vulnerabilidade, integrando ao ambiente da SEFAZ BA, incluindo plataforma de segurança.

Planejamento da Instalação das soluções de TI fornecidas

- a) A SEFAZ BA definirá, com o apoio da equipe técnica da CONTRATADA, de que forma as soluções de TI utilizadas na prestação do serviço deverão ser instaladas, configuradas e integradas ao ambiente da SEFAZ BA. A CONTRATADA e a SEFAZ BA, em comum acordo, deverão fazer um planejamento das atividades de instalação antes de iniciar a instalação propriamente dita.
- b) Tratar das informações sobre a instalação dos componentes on premise das soluções de segurança ofertadas e esclarecer todos os questionamentos técnicos. A SEFAZ BA definirá, com o apoio da equipe técnica da CONTRATADA, de que forma ocorrerá a integração. A CONTRATADA e a SEFAZ BA, de comum acordo, deverão fazer um planejamento das atividades de integração e configuração dos sensores e agentes de coleta antes de iniciar a integração propriamente dita.
- c) O plano de instalação dos produtos/componentes on premise utilizados no fornecimento do serviço deverá conter de forma detalhada:
 - d) Descrição dos componentes que deverão ser instalados;
 - e) Pré-requisitos para a instalação: todos os recursos e condições que deverão ser providos pela SEFAZ BA, necessários para que a CONTRATADA possa realizar os serviços de instalação, quando cabível;
 - f) Relação dos especialistas certificados da CONTRATADA alocados nos processos de instalação;
 - g) Relatórios das visitas técnicas de pré-instalação;
 - h) Visão geral da arquitetura da solução que será implantada;
 - i) Descrição das etapas do processo de instalação, detalhando as opções de configuração adotadas;
 - j) Cronograma de execução;
 - k) Necessidade de atualização de versões dos produtos utilizados no fornecimento do serviço;
 - l) Cronograma de operacionalização dos serviços gerenciados contratados.
- m) No prazo de até 5 (cinco) dias úteis, a partir do recebimento formal do plano de instalação, a SEFAZ BA deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido à CONTRATADA um novo prazo de até 5 (cinco) dias úteis para eventuais ajustes e reapresentação da documentação reprovada. A versão definitiva do plano de instalação será a versão aprovada pela equipe técnica da SEFAZ BA.
- n) Apresentar as informações referentes ao suporte técnico responsável pelo atendimento, tais como: endereço, telefone, e-mail e contato.
- o) Apresentar as informações referentes aos canais de atendimento para abertura dos chamados de suporte e manutenção, caso ainda não o tenha feito.

Instalação das soluções de TI

- a) A CONTRATADA deverá realizar a instalação "assistida", acompanhada por analistas da SEFAZ BA, de todos os sensores, agentes de coleta e outros componentes das soluções contratadas e que serão utilizadas para suportar a operação dos serviços gerenciados de segurança, monitorando o ambiente de TI da SEFAZ BA. Todo processo de instalação deverá atender ao definido no Plano de Instalação previamente discutido e aprovado pela SEFAZ BA.
- b) A CONTRATADA deverá configurar as ferramentas utilizadas para a execução do serviço, de modo que funcionem para atender plenamente os requisitos deste Termo de Referência.
- c) Correrá por conta da CONTRATADA toda e qualquer despesa, independente da sua natureza, decorrente dos serviços de instalação aqui mencionados;
- d) Concluídas a instalação e a configuração dos produtos adquiridos, a CONTRATADA deverá comunicar formalmente à SEFAZ BA sobre a conclusão dos serviços de instalação. A SEFAZ BA terá o prazo de até 10 (dez) dias úteis para verificar a conformidade da instalação e da configuração realizada com as condições constantes neste Termo de Referência;
- e) Caso sejam constatadas anormalidades ou sejam detectados problemas durante a verificação de conformidade realizada pela SEFAZ BA, a mesma comunicará formalmente os problemas detectados e que a instalação não foi concluída. A CONTRATADA terá um novo prazo de até 10 (dez) dias úteis, contados a partir do dia seguinte à confirmação de recebimento da comunicação



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

para sanar os problemas/anormalidades detectados, sem prejuízo do prazo descrito no subitem 1.2 deste Encarte A, sujeitando-se a CONTRATADA às penalidades previstas;

- f) Os serviços de instalação deverão ocorrer em dias úteis, no horário compreendido entre 9:00h e 17:30h, podendo ocorrer atividades fora de horário comercial, com programação realizada em comum acordo entre a SEFAZ BA e a CONTRATADA. Os serviços de instalação deverão ser agendados previamente com a SEFAZ BA;
- g) Os serviços de instalação que não puderem ser executados em horário comercial, por requisitos da SEFAZ BA, deverão ser executados na janela de manutenção definida pela SEFAZ BA;
- h) Todas as atividades de instalação deverão seguir os ritos do Processo de Gerenciamento de Mudanças definidos pela SEFAZ BA.

4.12. Integrações entre Sistema de Tickets e Software de ITSM

Configurar integrações entre as ferramentas fornecidas (Sistema de TICKETS, SIEM, etc.) e software de ITSM da SEFAZ BA.

4.13. Resposta automática

Estruturar e configurar respostas automatizadas nas soluções da plataforma de segurança.

4.14. Capacitação da Equipe Técnica

- Capacitação Técnica da equipe técnica do SOC e SEFAZ BA envolvida nos processos, procedimentos e instruções estruturadas;
- Capacitação Técnica da equipe técnica do SOC no ambiente de TI da SEFAZ BA;
- Capacitação Técnica da equipe técnica da SEFAZ BA nas soluções de SIEM e de Avaliação de Vulnerabilidades. Esta capacitação técnica deve ser para pelo menos 10 (dez) profissionais, com carga mínima de 20 (vinte horas) horas por ferramenta e conteúdo programático compatível com a capacitação em Administração e Operação na ferramenta ofertado pelo fabricante.

Plano de Capacitação

- a) Para definir o plano de capacitação a CONTRATADA deverá se reunir com os gestores do contrato da SEFAZ BA, de forma remota ou presencial, no prazo máximo de até 5 (cinco) dias úteis, contados a partir do dia seguinte da solicitação formal da SEFAZ BA. A data da reunião deverá ser agendada em comum acordo entre a CONTRATADA e a SEFAZ BA;
- b) Nesta reunião a CONTRATADA deverá alinhar junto ao representante da SEFAZ BA, itens referentes à capacitação técnica, tais como: conteúdo programático, perfil dos participantes, carga horária, cronograma de execução, infraestrutura, local de realização, material didático, avaliação e demais informações pertinentes ao processo de capacitação;
- c) Como produto desta reunião, a CONTRATADA deverá encaminhar por meio eletrônico, em até 5 (cinco) dias úteis após a realização da reunião, o Plano de Capacitação;
- d) O Plano de Capacitação deverá conter: instrutoria, conteúdo programático, carga horária, cronograma de execução e demais informações pertinentes ao processo de capacitação, bem como o material didático a ser utilizado na capacitação;
- e) No prazo de até 5 (cinco) dias úteis, a partir do recebimento formal do Plano de Capacitação, a SEFAZ BA deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido à CONTRATADA um novo prazo de até 5 (cinco) dias úteis para eventuais ajustes e reapresentação da documentação reprovada. A versão definitiva do Plano de Capacitação será a versão aprovada pela Equipe Técnica da SEFAZ BA;

Instrutoria

Esta capacitação técnica deve ser para pelo menos 10 (dez) profissionais, com carga mínima de 24 (vinte e quatro) horas por ferramenta e conteúdo programático compatível com a capacitação em Administração e Operação na ferramenta ofertado pelo fabricante.

- a) A CONTRATADA deverá apresentar ao representante da SEFAZ BA os dados do instrutor, que deverá possuir certificação técnica conforme definido no Encarte D – Perfil Profissional, que lhe



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

confira as competências necessárias para ministrar a capacitação. As certificações exigidas são:

- Para Capacitação Técnica da equipe técnica da SEFAZ BA na solução de SIEM: Certificação do fabricante de administrador da solução de "Gerenciamento de eventos e informações de segurança (SIEM)" ofertada a ser implantada. Não serão aceitas certificações comerciais e/ou pré-venda.
 - Para Capacitação Técnica da equipe técnica da SEFAZ BA na solução de Avaliação de Vulnerabilidades: Certificação do fabricante de administrador da solução de "Avaliação de Vulnerabilidade" ofertada a ser implantada. Não serão aceitas certificações comerciais e/ou pré-venda.
- b) A certificação exigida deve estar válida durante o período de prestação do serviço da capacitação técnica;
- c) A entrega da documentação que comprova o atendimento da exigência de certificação deverá ser realizada com antecedência mínima de 5 (cinco) dias úteis do início da realização da respectiva capacitação. A capacitação técnica só será realizada após a CONTRATADA apresentar a devida comprovação;
- d) É vedada a alteração de instrutor sem prévia comunicação e concordância da SEFAZ BA, estando um eventual substituto sujeito ao mesmo processo de verificação descrito anteriormente;
- e) A capacitação técnica deverá ser ministrada em língua portuguesa obrigatoriamente;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA
ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE B
Nível Mínimo de Serviço (NMS)

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.

1. INDICADORES DE DESEMPENHO E PENALIDADES

- 1.1. De modo a facilitar a compreensão dos Níveis Mínimos de Serviços, são apresentadas, na Tabela 1, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela CONTRATADA na execução do contrato, assim como as respectivas glosas aplicadas em caso de inadimplemento;
- 1.2. Para a classificação de severidade dos incidentes de segurança, deve ser utilizada a seguinte:
 - 1.2.1. Gravidade BAIXA: quando se verifica como necessária a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades de programas, porém sem prejudicar diretamente a operação dos programas ou sistemas da SEFAZ;
 - 1.2.2. Gravidade MÉDIA: quando se verifica uma perda de menor relevância de funcionalidades em programas ou sistemas da SEFAZ BA, causando apenas inconveniências para a devida prestação dos serviços pela SEFAZ;
 - 1.2.3. Gravidade ALTA: quando se verifica uma grave perda de funcionalidades em programas ou sistemas da SEFAZ, inexistindo alternativas de contorno, sem, no entanto, interromper em sua totalidade a prestação do serviço;
 - 1.2.4. Gravidade CRÍTICA: quando ocorre a perda ou paralisação de serviços relevantes prestados pela SEFAZ ou atividades exercidas pela mesma, configurando-se como situação de emergência. Uma solicitação de serviço de Severidade CRÍTICA pode possuir uma ou mais das seguintes características:
 - Dados corrompidos;
 - Uma função crítica não está disponível;
 - O sistema se desliga repentinamente causando demoras excessivas e intermitências para utilização de recursos;
 - O sistema falha repetidamente após tentativas de reinicialização;
 - Falha crítica de componentes da solução;
 - 1.2.5. O nível de severidade do incidente de segurança será, inicialmente, definido pela CONTRATADA, podendo ser modificado pela SEFAZ BA, conforme critérios definidos neste Termo de Referência, para avaliação do cumprimento dos Níveis Mínimos de Serviço pela CONTRATADA;



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

#	MÉTRICA	DESCRIÇÃO	DEFINIÇÃO	NMS – VALOR REFERÊNCIA	GLOSA POR INADIMPLEMENTO
MONITORAMENTO DE EVENTOS					
1	Percentual de alertas tratados	Quantidade dos alertas monitorados pela ferramenta de SIEM, que são avaliados e classificados, pela camada de monitoração dos analistas do CONTRATADO.	(total de alertas avaliados e tratados pelo monitoramento/total de alertas gerados pela ferramenta)	0 – 1 meses de operação: 80%; 2 – 3 meses de operação: 90%; 4 – 6 meses de operação: 95%; > 6 meses: 100%;	10 pontos (+3 pontos a cada 1% abaixo do valor de referência)
2	Tempo máximo para triagem de incidentes de segurança	Tempo decorrido entre a ocorrência do alerta no SIEM e confirmação do incidente de segurança	Tempo = Hora da triagem – Hora de entrada do evento de segurança	0 a 1 meses de operação: 12 horas; 2 a 3 meses de operação: 2 horas; 4 a 6 meses de operação: 1 hora; > 6 meses: 15 minutos;	3 pontos (+1 ponto a cada 5 minutos excedentes)



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

3	Tempo máximo para comunicação de incidentes à SEFAZ.		Tempo = Hora da comunicação – hora da triagem	0 a 1 meses de operação: 12 horas; 2 a 3 meses de operação: 2 horas; 4 a 6 meses de operação: 1 hora; > 6 meses: 15 minutos;	5 pontos (+2 pontos a cada 5 minutos excedentes)
4	Time frame Global para notificação de tickets	Quando um alerta de segurança é disparado pelo SIEM, o ticket de incidente associado deve ser criado dentro do prazo fornecido. O período de criação do ticket é definido como o tempo entre o último log que disparou o alerta no SIEM e a SEFAZ foi notificada.	O SLA deve ser calculado como X / Y (X) o número de tickets de segurança criados no prazo pela CONTRATADA dividido por (Y) o número total de tickets de segurança gerados	95% dos tickets devem ser criados dentro do prazo. Relatório mensalmente por meio do relatório de medição da CONTRATADA.	10 pontos (+3 pontos a cada 1% abaixo do valor de referência)
5	Troca de informações	Solicitação de informações realizadas pela SEFAZ aos analistas da CONTRATADA sobre eventos escalados.	Tempo decorrido entre a solicitação até o recebimento da informação pela SEFAZ.	15 minutos para incidentes categorizados como gravidade alta	5 pontos (+1 ponto a cada 5 minutos excedentes)



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

				ou crítica. 30 minutos para demais incidentes.	
RESPOSTA A INCIDENTES DE SEGURANÇA					
6	Tempo máximo para envio do procedimento de resposta de incidentes de segurança de gravidade baixa	Tempo máximo para envio do procedimento inicial para mitigação do incidente de segurança de gravidade baixa	Tempo = Hora do início da resposta – hora da triagem	<= 180 minutos	10 pontos (+3 pontos a cada 10 minutos excedentes)
7	Tempo máximo para envio do procedimento de resposta de incidentes de segurança de gravidade média	Tempo máximo para envio do procedimento inicial para mitigação do incidente de segurança de gravidade média	Tempo = Hora do envio do procedimento de resposta – hora da triagem	<= 120 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
8	Tempo máximo para envio do procedimento de resposta de incidentes de segurança de gravidade alta	Tempo máximo para envio do procedimento inicial para mitigação do incidente de segurança de gravidade alta	Tempo = Hora do envio do procedimento de resposta – hora da triagem	<= 60 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)
9	Tempo máximo para envio do procedimento de resposta de incidentes de segurança de gravidade crítica	Tempo máximo para envio do procedimento inicial para mitigação do incidente de segurança de gravidade crítica	Tempo = Hora do envio do procedimento de resposta – hora da triagem	<= 30 minutos	10 pontos (+3 pontos a cada 5 minutos excedentes)



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

10	Rate Global para Qualificação de tickets dentro do intervalo de tempo	<p>- Quando um ticket de segurança é criado pelo Nível 1, o ticket associado deve ser qualificado dentro do prazo, incluindo:</p> <ul style="list-style-type: none">- Avaliação de gravidade, triagem e escalção, conforme definido nos Procedimentos de alerta para incidentes- Se existente, a aplicação dos procedimentos fornecidos pelos especialistas em segurança do SOC <p>O período de qualificação do ticket é definido como o tempo entre a criação do ticket na ferramenta e sua atualização com a qualificação associada.</p>	O SLA deve ser calculado como X / Y (X) o número de tickets de segurança qualificados CONTRATADA dividido por (Y) o número total de tickets de segurança gerados	95% dos tickets devem ser qualificados dentro do prazo. Relatório mensalmente por meio do relatório da CONTRATADA.	10 pontos (+3 pontos a cada 1% abaixo do valor de referência)
11	Nível de tickets com investigação inicial dentro do intervalo de tempo	Depois que um ticket de segurança é qualificado pelo Nível 1 como "crítico ou P1", o ticket associado pode requerer uma primeira investigação dos analistas do SOC, a fim de fornecer a recomendação adaptada para a SEFAZ. O período da primeira investigação do ticket é definido como o tempo entre a qualificação do ticket na ferramenta e sua atualização com a recomendação associada após a investigação.	O SLA deve ser calculado como X / Y (X) o número de tickets "críticos" de segurança investigados no prazo pela CONTRATADA dividido por (Y) o número total de tickets "críticos" de segurança gerados	95% dos tickets devem ser investigados dentro do intervalo de tempo	15 pontos (+3 pontos a cada 1% abaixo do valor de referência)



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

12	Taxa de tickets de "alto risco" com investigação inicial dentro do intervalo de tempo	<p>Depois que um ticket de segurança é qualificado como "alto risco", o ticket associado pode exigir uma primeira investigação, a fim de fornecer a recomendação adaptada para a SEFAZ. O período da primeira investigação do ticket é definido como o tempo entre a qualificação do ticket na ferramenta e sua atualização com a recomendação associada após a investigação.</p> <p>Se uma classificação de ticket de incidente estiver sendo revisada como "alto risco" pela SEFAZ, o SLA se aplicará da mesma maneira após a qualificação atualizada do incidente.</p>	<p>O SLA deve ser calculado como X / Y (X) o número de tickets de "alto risco" de segurança investigados no prazo pela CONTRATADA dividido por (Y) o número total de tickets de "alto risco" de segurança gerados</p>	<p>95% dos tickets devem ser investigados dentro do intervalo de tempo</p>	<p>10 pontos (+3 pontos a cada 1% abaixo do valor de referência)</p>
GERENCIAMENTO DA PLATAFORMA DE SEGURANÇA					
13	Tempo de integração de novos sensores	Solicitação de inclusão ou retirada de sensores integrados ao SIEM.	Tempo em dias decorridos desde a solicitação até que o sensor de segurança tenha seus alertas sendo tratados pela ferramenta	15 dias	3 pontos (+1 ponto a cada 1 dia excedente)
14	Alteração de configurações	Solicitações de gestão de acesso, registros de auditoria da ferramenta ou outras configurações administrativas.	Tempo decorrido entre a abertura do chamado até a implementação da solicitação.	240 minutos após abertura de chamado	3 pontos (+1 ponto a cada 30 minutos excedentes)



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

15	Configuração de regras de correlação	Solicitações de configuração de regras de correlacionamento para monitoramento de novas métricas.	Tempo decorrido entre a abertura do chamado até a operacionalização da regra.	0 – 3 meses de operação: 7 dias; > 3 meses: 3 dias;	3 pontos (+1 ponto a cada 1 dia excedente)
16	Atualização de segurança da solução	Atualização da solução por meio da implementação de patches e fixes, incluído neste limite o tempo necessário à homologação do pacote pela contratada	Tempo decorrido entre a liberação da atualização até sua implementação.	15 dias após liberação das atualizações pelo fabricante	5 pontos (+1 ponto a cada 1 dia excedente)
17	Tempo máximo para resolução das demais requisições de serviços.		Tempo = Hora da resolução da solicitação – hora da solicitação	<= 24 horas	10 pontos (+3 pontos a cada hora excedente)
18	Índice de disponibilidade das soluções da plataforma de segurança - SEFAZ BA	Disponibilidade das soluções da plataforma de segurança em regime 24x7 (24 horas por dia, 7 dias por semana)	Total de tempo com disponibilidade no mês /total de tempo no mês x 100	>= 99,7%	30 pontos (+5 pontos a cada 0,1% abaixo da meta)
19	Tempo máximo para correção de incidente na plataforma de segurança - SEFAZ BA em caso de indisponibilidade.		Tempo = Hora do restabelecimento – Hora do início da indisponibilidade	<= 60 minutos	30 pontos (+5 pontos a cada 10 minutos excedentes)
GERENCIAMENTO DE VULNERABILIDADES					



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

20	Atualização de bases externas de assinatura de ataques e vulnerabilidades	Atualização da solução com as bases de assinatura divulgadas pelo fabricante ou por serviços especializados do CONTRATADO.	Tempo decorrido entre a liberação da atualização até sua implementação.	12 horas após liberação pelo fabricante	3 pontos (+1 ponto a cada 1 hora excedente)
21	Tempo máximo para requisição de mudança para aplicação de patches e hot fixes de segurança ou indicação de solução de contorno para tratamento de grave vulnerabilidade ou ameaça emergente		Tempo = Hora de conclusão do planejamento da requisição de mudança – hora de disponibilização dos patches e hotfixes ou divulgação de grave vulnerabilidade ou ameaça emergente	<=72 horas	5 pontos (+2pontos a cada hora excedente)
DASHBOARDS E RELATÓRIOS					
22	Atendimento a chamados para esclarecimento de dúvidas	Suporte para dúvidas e questões relacionadas a solução ou serviços contratados.	Tempo decorrido entre a abertura do chamado até a resposta da solicitação.	24 horas após abertura de chamado	3 pontos (+1 ponto a cada 1 hora excedente)
24	Configuração de dashboards	Solicitações de criação de gráficos e disponibilização de dashboards com novas métricas monitoradas. (Limitados a 4 por mês.)	Tempo decorrido entre a abertura do chamado até a disponibilização do acesso ao painel.	5 dias após abertura de chamado	3 pontos (+1 ponto a cada 1 hora excedente)
25	Configuração de relatórios	Solicitações de criação de novos modelos de relatórios automatizados na ferramenta. (Limitados a 4 por mês.)	Tempo decorrido entre a abertura do chamado até a disponibilização do acesso ao relatório.	5 dias após abertura de chamado	3 pontos (+1 ponto a cada 1 dia excedente)



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

26	Relatórios	Customização dos indicadores e informações sobre incidentes apresentados nos relatórios. Limitados a 10 por mês.	Tempo decorrido entre a abertura do chamado até a disponibilização do acesso ao relatório.	5 dias após abertura de chamado	3 pontos (+1 ponto a cada 1 dia excedente)
----	------------	--	--	---------------------------------	--

Tabela 1: Nível Mínimo de Serviço



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA:

Descrição	Referência	Glosa por inadimplemento
Finalizar a requisição de serviço ou incidente sem a devida resolução ou sem realizar os testes necessários para aferir a efetiva resolução.	Por ocorrência	10 pontos
Finalizar uma requisição de serviço sem documentar os procedimentos executados para atendimento da solicitação.	Por ocorrência	5 pontos
Finalizar um incidente sem documentar a causa, a solução de contorno (se houver) ou os procedimentos adotados para solução.	Por ocorrência	5 pontos
Finalizar um problema sem documentar a investigação realizada, a causa-raiz ou a solução aplicada.	Por ocorrência	5 pontos
Fraudar, manipular ou descaracterizar indicadores/metras de níveis de serviço por quaisquer subterfúgios, por indicador/meta de nível de serviço manipulado.	Por ocorrência	30 pontos
Manter profissionais sem formalização ou sem a qualificação exigida para executar os serviços contratados, ainda que em casos de substituição temporária.	Por ocorrência	30 pontos
Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais.	Por ocorrência	30 pontos
Utilizar indevidamente os recursos de TI (acessos indevidos, utilização para fins particulares) ou utilizar equipamento particular.	Por ocorrência	30 pontos
Realizar mudanças de configuração nas soluções de segurança que impactem a SEFAZ, sem seguir o devido Processo de Mudanças.	Por ocorrência	15 pontos



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

Serão aplicadas as referidas pontuações para efeito de glosa, no caso de a CONTRATADA **DEIXAR DE:**

Descrição	Referência	Glosa por inadimplemento
Cumprir ou implementar as rotinas em conformidade com a Política de Segurança ou determinações da equipe de fiscalização do contrato.	Por ocorrência	10 pontos
Cumprir ou implementar as rotinas em conformidade com os Planos de Gerenciamento de Incidentes, de Disponibilidade, de Continuidade e de Recuperação de Desastres das soluções de segurança.	Por ocorrência	10 pontos
Executar testes de continuidade de cada solução de segurança da informação em alta disponibilidade a, no mínimo, cada 6 (seis) meses.	Por ocorrência	10 pontos
Atuar proativamente em caso de identificação de situação de desconformidade com boas práticas de segurança.	Por ocorrência	10 pontos
Apresentar mensalmente plano de tratamento de vulnerabilidades, indicando as ações mais efetivas para redução dos riscos.	Por ocorrência	10 pontos
Apresentar os relatórios consolidados conforme exigências do Termo de Referência até o dia 5º dia útil do mês subsequente.	Por dia de atraso	05 pontos
Apresentar relatórios, levantamentos ou inventários conforme demanda em até 3 dias úteis;	Por ocorrência	05 pontos
Manter o Configuration Management Database (CMDB) atualizado.	Por ocorrência	10 pontos
Manter a documentação e os desenhos das topologias atualizados e completos.	Por ocorrência	05 pontos
Notificar sobre ocorrências recorrentes.	Por ocorrência	05 pontos
Cumprir ou implementar as rotinas em conformidade com os processos de trabalho da Secretaria de Tecnologia da Informação.	Por ocorrência	10 pontos



ESTADO DA BAHIA

SECRETARIA DA FAZENDA

Elaborar auditorias de dados, consultas às bases de logs de transações ou relatórios diversos.	Por ocorrência	15 pontos
Analisar a viabilidade e o impacto da instalação de novas soluções ou correções.	Por ocorrência	05 pontos
Apresentar mensalmente proposta de melhorias no ambiente.	Por ocorrência	05 pontos
Cumprir quaisquer obrigações estabelecidas no contrato e anexos, não previstas nesta tabela, após reincidência formalmente notificada pelo SEFAZ.	Por ocorrência	15 pontos
Cumprir Capacitação Anual de Profissionais	Por ocorrência	30 pontos



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE C

AMBIENTE DE TI – SEFAZ BA

A Tabela a seguir contém informações sobre o ambiente de TI da SEFAZ BA e deve ser utilizada para o dimensionamento da estruturação e operação dos serviços gerenciados de segurança a serem prestados assim como no licenciamento das soluções a serem ofertadas conforme definido neste Termo de Referência.

AMBIENTE SEFAZ BA - INFORMAÇÕES PARA SIZING	
ATIVOS DE TI	QTDE PROJETADA (24 MESES)
FQDNs A SEREM SCANNEADAS	50
USUÁRIOS DO AD (ATIVOS)	5000
DATA CENTER	1
Nuvem Privada	1
SITES REMOTOS	40
DESKTOP WINDOWS	10
Microcomputador	10
SERVIDOR WINDOWS	400
Data Center	364
MS Windows Server 2003, 2007, 2008, 2010, 2012, 2016, 2019 e 2022	364
Unidades remotas	36
MS Windows Server 2022	36
SERVIDOR LINUX/UNIX	150
Data Center	150
AlmaLinux	150
CentOS 7, CentOS 8	
Debian 7, Debian 8	
Red Hat 6.10, 7.4, 7.5, 7.9, 8.5, 8.6, 8.8 e 8.9	



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Oracle Linux	
FreeBSD	
Outros (associados a appliances físicos e virtuais)	
HOST VIRTUALIZAÇÃO	65
Data Center	65
VMware ESXi 6.0, 6.5, 6.7 e 7.0	65
SERVIDOR WEB	100
SERVIDOR AD	5
Data Center	5
SERVIDOR DNS/DHCP	10
Data Center	10
DNS Externo	3
DNS Interno	5
DHCP	2
SERVIDOR BANCO DE DADOS	105
MS SQL Server	66
Oracle	5
MariaDB	7
PostGree	7
MongoDB	12
IBM DB2	3
Outros (Netezza)	5
BASE DE DADOS	205
FIREWALL	43
Fortigate 40F/60F	35
Fortigate 1500D	2 (HA - ativo/passivo)
Fortigate 400F	2 (HA - ativo/passivo)
Fortigate 80E	2 (HA - ativo/passivo)
Fortigate 300D	2 (HA - ativo/passivo)
CISCO ASA 5520	2 (HA - ativo/passivo)



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

IPS	2
Trellix IPS-NS7150	2 (HA - ativo/ativo)
BALANCEADOR DE CARGA	2
FORTIADC700D	2 (HA - ativo/passivo)
SWITCH LAN	35
SWITCH SAN	10
SOFTWARES DE SEGURANÇA e MONITORAMENTO	
EPP - Endpoint Protection	
Trellix - EPO e Endpoint Security	
Kaspersky	
MS Defender for Server	
Antispam	
Mail Inspector	
Controle de Acesso	
ForeScout NAC	
PAM (Privileged access management)	
Beyond Trust	
Controle de Conteúdo WEB	
Trellix WebGateway	
WSUS - Windows Server Update Services	
Monitoramento de Infraestrutura de TI	
Zabbix	
SAST (Static application security testing)	
SonarQube	
APM (Application Monitoring Performance)	
Dynatrace APM	
Sentry	
Inventário	
OCS	
Syslog	



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Grafana	
---------	--



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE D

PERFIL PROFISSIONAL

Este encarte define o perfil profissional exigido para os componentes da equipe técnica da CONTRATADA alocada no Centro de Operações de Segurança (SOC) da SEFAZ BA para prestação dos serviços gerenciados de segurança conforme descrito neste Termo de Referência.

1. A CONTRATADA deverá dimensionar adequadamente a sua equipe de profissionais de forma a atingir os níveis de serviço estabelecidos no contrato, bem como deverá prover capacidade de atuação técnica dos profissionais em todos os produtos e serviços de segurança da CONTRATANTE e demais objetos desta contratação.
2. A formação da equipe de profissionais é de exclusiva responsabilidade da CONTRATADA e serão gerenciados exclusivamente pelo PREPOSTO, GESTOR TÉCNICO da empresa.
3. A experiência comprovada e o conhecimento técnico estabelecidos na tabela PERFIL PROFISSIONAL abaixo constituem requisitos indispensáveis para compatibilização à capacidade de execução do objeto a ser executado, haja vista o caráter do risco e da complexidade serem elevados e que demandam profissionais com um perfil sênior (de experiência comprovada em TIC e Segurança da Informação) e, obrigatoriamente, determinado rol de conhecimentos mínimos quanto à qualificação técnica.
 - 3.1. Os serviços deverão ser executados por profissionais habilitados, com base em programas de formação e/ou certificações oficiais válidas e ativas, conforme os requisitos específicos para o perfil profissional descritos abaixo por serviço a ser prestado.
 - 3.2. Todos os profissionais deverão possuir qualificação e conhecimento técnico compatível com a complexidade das demandas a serem atendidas.
 - 3.3. A SEFAZ BA poderá solicitar, a qualquer tempo, a substituição de quaisquer dos profissionais envolvidos no projeto/serviços que apresentem desempenho insatisfatório na execução dos serviços contratados ou conduta inadequada às regras de conduta vigentes na Instituição. Em qualquer caso, a CONTRATADA deverá substituir mediante solicitação e a critério da SEFAZ BA, qualquer profissional, sem ônus de qualquer natureza.
4. Caso ocorra o desligamento de qualquer um dos profissionais exigidos durante a vigência do contrato, a empresa deverá providenciar um substituto, com as mesmas qualificações ou superiores, no prazo máximo de 15 (quinze) dias.
5. A CONTRATADA deverá prestar os serviços por meio de equipe própria, composta por colaboradores contratados sob o regime CLT, com certificações específicas e comprovadas. É VEDADO o uso de SUBCONTRATAÇÃO para qualquer parte do escopo deste projeto.
 - 5.1 O salário base mínimo para o profissional da Equipe SOC de GERENCIAMENTO DE VULNERABILIDADES e de RESPOSTA A INCIDENTES (N2) é de R\$ 12.297,39 (doze mil e duzentos e noventa e sete reais e trinta e nove centavos).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

- 5.2 O valor acima tem como referência o contrato SF/PS/DA/22/23 vigente na SEFAZ BA que inclui a alocação de profissional "Analista Especialista – Segurança da Informação" com perfil profissional similar ao profissional da Equipe SOC de GERENCIAMENTO DE VULNERABILIDADES e de RESPOSTA A INCIDENTES (N2) e com salário base mínimo de R\$ 11.700,66 (onze mil e setecentos reais e sessenta e seis centavos). Existe processo SEI 013.1417.2024.0060960-91 em andamento reajustando em 5,01% os preços do contrato o que reajusta o salário base mínimo deste profissional para R\$ 12.297,39 (doze mil e duzentos e noventa e sete reais e trinta e nove centavos).
- 5.3 Este salário base mínimo será corrigido sempre que houver qualquer reajuste ou reequilíbrio no valor do contrato, seguindo o mesmo índice de atualização adotado. Não se aplica, entretanto, para as situações em que ocorrer alterações de valor decorrentes de aditivos para a ampliação ou redução do escopo do serviço.
- 5.4 Com relação aos profissionais das demais Equipes SOC, por se tratar de profissionais que poderão ser compartilhados com outros contratos, não há determinação de salário base para estes perfis.
6. O atendimento dos requisitos obrigatórios de qualificação profissional mínima para a execução dos serviços, para cada perfil, descritos neste ENCARTE D - PERFIL PROFISSIONAL, do Termo de Referência inserido no presente edital, deverá ser comprovado em até 90 (noventa) dias corridos após a assinatura do contrato, durante a ETAPA DE IMPLANTAÇÃO ou até o início efetivo da operação do serviço, mediante apresentação de diplomas, certificados ou certificações de empresas de treinamento autorizadas e credenciadas, registros em carteira de trabalho, contratos de trabalho ou outro meio equivalente e idôneo e, somente no momento em que a CONTRATADA entregar todos os comprovantes previstos para qualificação profissional, este item será considerado atendido em sua totalidade para o início da operação dos serviços.
 - 6.1 Exceção para os perfis profissionais GESTOR TÉCNICO e Equipe SOC de IMPLANTAÇÃO, cujo atendimento aos requisitos obrigatórios de qualificação profissional mínima para a execução dos serviços, descritos neste ENCARTE D - PERFIL PROFISSIONAL, deverá ser comprovado após a assinatura do contrato e antes do início da ETAPA DE IMPLANTAÇÃO.
7. O profissional que não realizar a apresentação completa da documentação comprobatória exigidas ou que não atender completamente a qualificação exigida, conforme PERFIL PROFISSIONAL definido, não será aceito pelo CONTRATANTE para a execução de qualquer atividade conforme previsto nos serviços definidos neste Termo de Referência.
8. A CONTRATADA se obriga, durante a execução do contrato, a manter todos os profissionais com as qualificações válidas designadas neste anexo.
9. Após o início da execução dos serviços, a documentação dos profissionais residentes deve ser apresentada toda vez que ocorrer uma substituição, e a relação e documentação do restante dos profissionais deve ser apresentada uma vez por semestre.
10. A comprovação da experiência profissional, requerida para cada um dos perfis acima descritos, dar-se-á mediante a apresentação de documento emitido pela (s) empresa (s) onde o técnico realizou tarefas típicas da função pleiteada, exigindo-se similaridade com as tarefas relacionadas para cada perfil profissional.
11. A comprovação da capacitação técnica dar-se-á mediante a apresentação, para cada profissional, de original ou cópia autenticada dos certificados, conforme perfil exigido, dentro do período de validade.
12. A critério da SEFAZ BA, as certificações exigidas neste ENCARTE D - PERFIL PROFISSIONAL poderão ser substituídas por outras certificações equivalentes às estabelecidas previamente ou de nível mais avançado.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

13. Os documentos comprobatórios mencionados acima deverão ser apresentados na alocação dos profissionais à execução dos serviços, e deverão vir acompanhados do Curriculum Vitae.
14. A CONTRATADA deverá promover a suas despensas, no prazo máximo de 6 (seis) meses, atualização das certificações de seus profissionais caso haja atualização de versão ou migração para uma nova solução de TI devido a modernização do ambiente tecnológico do CONTRATANTE. Este prazo se iniciará a partir da comunicação formal do CONTRATANTE.
15. Para todos os itens solicitados neste ENCARTE D - PERFIL PROFISSIONAL a comprovação dos requisitos deverá ser composta de:
 - 15.1 Documento digitalizado com apresentação do documento original, cópia autenticada ou documento digital em que seja possível comprovar a autenticidade em site do emissor;
 - 15.2 Cópia autenticada de certificados ou diplomas que comprovem a conclusão dos cursos exigidos. No caso dos cursos de nível superior deverão ser apresentados os diplomas;
 - 15.3 Todos os documentos apresentados estarão sujeitos à diligência do CONTRATANTE para fins de confirmação das informações prestadas;
 - 15.4 Caso uma certificação não seja mais válida, será aceita a nova certificação que substituiu a anterior;
 - 15.5 Caso alguma das certificações esteja vencida, será dado prazo de 60 (sessenta) dias meses para revalidar.
 - 15.6 Caso ocorra um termo aditivo para contratação de mais profissionais para atuação neste contrato, as certificações serão definidas nesse momento futuro.

TABELA - PERFIL PROFISSIONAL	
1	PERFIL PROFISSIONAL - GESTOR TÉCNICO
1.1	FORMAÇÃO ACADÊMICA
1.1.1	Diploma de nível superior completo, com pelo menos 12 (doze) anos de formação , em Tecnologia da Informação ou curso superior completo em qualquer área, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
1.2	EXPERIÊNCIA PROFISSIONAL
1.2.1	Tempo de atuação mínima de 9 (nove) anos na área de segurança da informação, com pelo menos 05 (cinco) anos na coordenação e liderança de equipes técnicas na área de segurança da informação;
1.2.2	Experiência comprovada de pelo menos 3 (três) anos em Gestão de Serviços Gerenciados de Segurança da Informação;
1.2.3	Experiência mínima de 1 (um) ano trabalhando como analista de segurança de CSOC desenvolvendo todas as atividades inerentes ao cargo de analista de CSOC, ou seja, N1, N2 ou N3.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

1.2.4	Experiência em estruturação e implantação de processos ITIL - Central de Serviços (Requisições, Incidentes e Problemas), Monitoramento de Eventos, Resposta a Incidentes de Segurança e Gerenciamento de Vulnerabilidades
1.3	HABILIDADES TÉCNICAS
1.3.1	Ter conhecimentos, habilidades e experiências cumulativas em pelo menos 80% das habilidades técnicas abaixo relacionadas:
1.3.1.1	a) Planejar, coordenar e acompanhar as atividades das equipes N1 e N2 de CSOC.
1.3.1.2	b) Inteligência de Ameaças Cibernéticas;
1.3.1.3	c) Tratamento e Resposta a Eventos e Incidentes Cibernéticos;
1.3.1.4	d) Análise de Logs;
1.3.1.5	e) Detecção de intrusões;
1.3.1.6	f) Mitigação de ataques;
1.3.1.7	g) Verificação de vulnerabilidade;
1.3.1.8	h) Monitoramento de redes;
1.3.1.9	i) Análise de tráfego de redes;
1.3.1.10	j) Criptografia;
1.3.1.11	k) Segurança de redes;
1.3.1.12	l) Ferramentas de análise de malware.
1.3.1.13	m) Capacidade de empregar linguagens de programação como Python, Power Shell, Bash e Perl.
1.3.1.14	n) Forense Digital;
1.3.1.15	o) Administração e suporte a ativos de segurança de rede tais como firewall, IPS e IDS.
1.3.1.16	p) Administração e suporte a softwares de segurança da informação tais como antivírus, antispam e filtro de conteúdo.
1.3.1.17	q) Detecção de vulnerabilidades da rede, sistemas, servidores e aplicações.
1.3.1.18	r) Administração e suporte de softwares voltados para a segurança de endpoints, ou terminais.
1.3.1.19	s) Administração e suporte a VPN (virtual private network).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

1.3.1.2 0	t) Realização de análises de riscos e definição de planos para mitigá-los.
1.3.1.2 1	u) Realização de auditoria e controle de processos para identificação de não conformidades ou falhas, com fornecimento de propostas para correção.
1.3.1.2 2	v) Definição de rotinas e procedimentos para prevenção a ataques.
1.3.1.2 3	x) Definição de políticas de segurança de rede.
1.3.1.2 4	y) Definição de processos para disaster/recovery de sistemas e de ambientes.
1.3.1.2 5	w) Definição de planos ou processos para a gestão de continuidade do negócio.
1.3.1.2 6	z) Conhecimentos avançados em LGPD (Lei Geral de Proteção de Dados).
1.4	CERTIFICAÇÃO TÉCNICA
1.4.1	CISSP (Certified Information System Security Professional), CISM (Certified Information Security Manager) ou CompTIA Security+ ou certificação sênior equivalente validada pela SEFAZ BA.
1.4.2	ITIL Foundation V4, ITIL Intermediate V4 ou superior ITIL Specialist V4
2	PERFIL PROFISSIONAL - Equipe SOC de MONITORAMENTO DE EVENTOS e RESPOSTA A INCIDENTES (N1)
2.1	FORMAÇÃO ACADÊMICA
2.1.1	Diploma de nível superior completo, com pelo menos 05 (cinco) anos de formação , em Tecnologia da Informação ou curso superior completo em qualquer área, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC);
2.2	EXPERIÊNCIA PROFISSIONAL
2.2.1	Tempo de atuação mínimo de 5 (cinco) anos em Tecnologia de Informação nas áreas de infraestrutura ou segurança da informação com pelo menos 03 (três) anos no cargo de Analista de Segurança da Informação.
2.3	HABILIDADES TÉCNICAS
2.3.1	Ter conhecimentos, habilidades e experiências cumulativas em pelo menos 7 (sete) das habilidades técnicas abaixo relacionadas:
2.3.1.1	a) Inteligência de Ameaças Cibernéticas;
2.3.1.2	b) Monitoramento de redes;
2.3.1.3	c) Análise de tráfego de redes;
2.3.1.4	d) Criptografia;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

2.3.1.5	e) Segurança de redes;
2.3.1.6	f) Ferramentas de análise de malware.
2.3.1.7	g) Tratamento e Resposta a Eventos e Incidentes Cibernéticos;
2.3.1.8	h) Análise de Logs;
2.3.1.9	i) Verificação de vulnerabilidade;
2.4	CERTIFICAÇÃO TÉCNICA
2.4.1	Pelo menos 2 (dois) profissionais em cada turno de operação do serviço de Monitoramento de Eventos e Resposta a Incidentes (N1) que possuam individualmente as seguintes certificações
2.4.1.1	ITIL - Possuir certificação ITIL Foundation ou superior emitido pelo EXIN ou ISEB;
2.4.1.2	ISO/IEC 270001:2022 FOUNDATION;
2.4.1.3	GSEC GIAC Security Essentials ou Lead Cybersecurity Professional Certification LCSPC ou GCIH GIAC Incident Handler ou EC-Council Certified Incident Handler ou CompTIA CySA+ ou Certified SOC Analyst v1;
3	PERFIL PROFISSIONAL - Equipe SOC de GERENCIAMENTO DE VULNERABILIDADES e de RESPOSTA A INCIDENTES (N2)
3.1	FORMAÇÃO ACADÊMICA
3.1.1	Diploma de nível superior completo, com pelo menos 09 (nove) anos de formação , em Tecnologia da Informação ou curso superior completo em qualquer área, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC);
3.2	EXPERIÊNCIA PROFISSIONAL
3.2.1	Tempo de atuação mínima de 07 (sete) anos em Tecnologia de Informação nas áreas de infraestrutura ou segurança da informação, com pelo menos 04 (quatro) anos no cargo de Analista de Segurança da Informação.
3.3	HABILIDADES TÉCNICAS
3.3.1	Ter conhecimentos, habilidades e experiências cumulativas em pelo menos 80% das habilidades técnicas abaixo relacionadas:
3.3.1.1	a) Conhecimentos em LGPD (Lei Geral de Proteção de Dados).
3.3.1.2	b) Inteligência de Ameaças Cibernéticas;
3.3.1.3	c) Tratamento e Resposta a Eventos e Incidentes Cibernéticos;
3.3.1.4	d) Análise de Logs;
3.3.1.5	e) Detecção de intrusões;
3.3.1.6	f) Mitigação de ataques;
3.3.1.7	g) Verificação de vulnerabilidade;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

3.3.1.8	h) Monitoramento de redes;
3.3.1.9	i) Análise de tráfego de redes;
3.3.1.10	j) Criptografia;
3.3.1.11	k) Segurança de redes;
3.3.1.12	l) Ferramentas de análise de malware.
3.3.1.13	m) Capacidade de empregar linguagens de programação como Python, Power Shell, Bash e Perl.
3.3.1.14	n) Forense Digital;
3.3.1.15	o) Administração e suporte a ativos de segurança de rede tais como firewall, IPS e IDS.
3.3.1.16	p) Administração e suporte a softwares de segurança da informação tais como antivírus, antispam e filtro de conteúdo.
3.3.1.17	q) Detecção de vulnerabilidades da rede, sistemas, servidores e aplicações.
3.3.1.18	r) Realização de auditoria e controle de processos para identificação de não conformidades ou falhas, com fornecimento de propostas para correção.
3.3.1.19	s) Definição de rotinas e procedimentos para prevenção a ataques.
3.4	CERTIFICAÇÃO TÉCNICA
3.4.1	A composição da Equipe SOC de GERENCIAMENTO DE VULNERABILIDADES e de RESPOSTA A INCIDENTES (N2) deve garantir que todos os profissionais da equipe técnica tenham as certificações abaixo:
3.4.1.1	ITIL - Possuir certificação ITIL Foundation ou superior emitido pelo EXIN ou ISEB;
3.4.1.2	ISO/IEC 270001:2022 FOUNDATION;
3.4.1.3	GSEC GIAC Security Essentials ou Lead Cybersecurity Professional Certification LCSPC ou GCIH GIAC Incident Handler ou EC-Council Certified Incident Handler ou CompTIA CySA+ ou Certified SOC Analyst v1;
3.4.1.4	Certificação do fabricante de administrador da solução de "Avaliação de Vulnerabilidade" ofertada a ser implantada. Não serão aceitas certificações comerciais e/ou pré-venda.
3.4.2	A composição da Equipe SOC de GERENCIAMENTO DE VULNERABILIDADES e de RESPOSTA A INCIDENTES (N2) deve garantir no somatório dos profissionais pelo menos 4 (quatro) das certificações abaixo:
3.4.2.1	Trellix Certified Product Specialist;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

3.4.2.2	Trellix ePolicy Orchestrator (ePO);
3.4.2.3	ForeScout Certified Administrator;
3.4.2.4	Fortinet Certified Professional;
3.4.2.5	Certified Professional: Kaspersky Endpoint Security and Management.
4	PERFIL PROFISSIONAL - Equipe SOC de GERENCIAMENTO DE PLATAFORMA DE SEGURANÇA
4.1	FORMAÇÃO ACADÊMICA
4.1.1	Diploma de nível superior completo, com pelo menos 09 (nove) anos de formação, em Tecnologia da Informação ou curso superior completo em qualquer área, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
4.2	EXPERIÊNCIA PROFISSIONAL
4.2.1	Tempo de atuação mínima de 07 (sete) anos em Tecnologia de Informação nas áreas de infraestrutura ou segurança da informação, com pelo menos 04 (quatro) anos no cargo de Analista de Segurança da Informação.
4.2.2	Deverá ter experiência comprovada de no mínimo (três) anos em instalação, customização, configuração e suporte técnico em pelo menos 3 (três) dos tipos de soluções (EPP - Endpoint Protection, AntiSpam, Controle de Acesso à Rede, Syslog, IPS e Firewall) componentes da Plataforma de Segurança - SEFAZ BA a ser administrada.
4.2.2.1	A composição da Equipe SOC de GERENCIAMENTO DE PLATAFORMA DE SEGURANÇA deve garantir profissionais com experiência, conforme descrito acima, em todos os tipos de soluções da Plataforma de Segurança (EPP - Endpoint Protection, AntiSpam, Controle de Acesso à Rede, Syslog, IPS e Firewall).
4.2.2.2	A composição da Equipe SOC de GERENCIAMENTO DE PLATAFORMA DE SEGURANÇA deve garantir pelo menos 2 (dois) componentes da equipe técnica com experiência, conforme descrito acima, por tipo de soluções da Plataforma de Segurança (EPP - Endpoint Protection, AntiSpam, Controle de Acesso à Rede, Syslog, IPS e Firewall).
4.3	HABILIDADES TÉCNICAS
4.3.1	Ter conhecimentos, habilidades e experiências cumulativas em pelo menos 80% das habilidades técnicas abaixo relacionadas:
4.3.1.1	Administração e suporte a ativos de segurança de rede tais como balanceadores de carga, firewall, IPS e IDS.
4.3.1.2	Administração e suporte a softwares de segurança da informação tais como antivírus, antispam e filtro de conteúdo.
4.3.1.3	Detecção de vulnerabilidades da rede.
4.3.1.4	Detecção de vulnerabilidades em sistemas, servidores e aplicações.
4.3.1.5	Administração e suporte de softwares voltados para a segurança de endpoints.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

4.3.1.6	Administração e suporte a VPN (virtual private network).
4.3.1.7	Realização de auditoria e controle de processos para identificação de não conformidades ou falhas, com fornecimento de propostas para correção.
4.3.1.8	Definição de rotinas e procedimentos para prevenção a ataques.
4.3.1.9	Definição de políticas de segurança de rede.
4.3.1.10	Conhecimentos em LGPD (Lei Geral de Proteção de Dados).
4.3.1.11	Inteligência de Ameaças Cibernéticas;
4.3.1.12	Tratamento e Resposta a Eventos e Incidentes Cibernéticos;
4.3.1.13	Análise de Logs;
4.3.1.14	Detecção de intrusões;
4.3.1.15	Mitigação de ataques;
4.3.1.16	Monitoramento de redes;
4.3.1.17	Análise de tráfego de redes;
4.3.1.18	Criptografia;
4.3.1.19	Segurança de redes;
4.3.1.20	Ferramentas de análise de malware.
4.3.1.21	Capacidade de empregar linguagens de programação como Python, Power Shell, Bash e Perl.
4.4	CERTIFICAÇÃO TÉCNICA
4.4.1	A composição da Equipe SOC de GERENCIAMENTO DE PLATAFORMA DE SEGURANÇA deve garantir que todos os componentes da equipe técnica tenham as certificações abaixo:
4.4.1.1	ITIL - Possuir certificação ITIL Foundation ou superior emitido pelo EXIN ou ISEB;
4.4.1.2	ISO/IEC 270001:2022 FOUNDATION;
4.4.1.3	GSEC GIAC Security Essentials ou Lead Cybersecurity Professional Certification LCSPC ou GCIH GIAC Incident Handler ou EC-Council Certified Incident Handler ou CompTIA CySA+ ou Certified SOC Analyst v1;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

4.4.2	A composição da Equipe SOC de GERENCIAMENTO DE PLATAFORMA DE SEGURANÇA deve garantir pelo menos 2 (dois) componentes da equipe técnica certificados para cada certificação técnica listada abaixo:
4.4.2.1	Trellix Certified Product Specialist;
4.4.2.2	Trellix ePolicy Orchestrator (ePO);
4.4.2.3	ForeScout Certified Administrator;
4.4.2.4	Fortinet Certified Professional;
4.4.2.5	Certified Professional: Kaspersky Endpoint Security and Management;
4.4.2.6	Certificação do fabricante de administrador da solução de "Gerenciamento de eventos e informações de segurança (SIEM)" ofertada a ser implantada. Não serão aceitas certificações comerciais e/ou pré-venda.
4.4.2.7	Certificação do fabricante de administrador da solução de "Avaliação de Vulnerabilidade" ofertada a ser implantada. Não serão aceitas certificações comerciais e/ou pré-venda.
5	PERFIL PROFISSIONAL - Equipe SOC de IMPLANTAÇÃO
5.1	A composição da Equipe SOC - ETAPA IMPLANTAÇÃO responsável pelas atividades previstas na implantação do Centro de Operações de Segurança (SOC) e serviços gerenciados de segurança associados deve garantir que os requisitos abaixo sejam atendidos por pelo menos um dos componentes desta equipe técnica:
5.2	FORMAÇÃO ACADÊMICA
5.2.1	Diploma de nível superior completo, com pelo menos 09 (nove) anos de formação, em Tecnologia da Informação ou curso superior completo em qualquer área, sendo necessário, nesse último caso, possuir certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida, ou validada, pelo Ministério da Educação (MEC).
5.3	EXPERIÊNCIA PROFISSIONAL
5.3.1	Tempo de atuação mínima de 07 (sete) anos em Tecnologia de Informação nas áreas de infraestrutura ou segurança da informação, com pelo menos 04 (quatro) anos no cargo de Analista de Segurança da Informação.
5.3.2	Experiência comprovada de no mínimo (três) anos em instalação, customização, configuração e suporte técnico em nas soluções "Gerenciamento de eventos e informações de segurança (SIEM)" e "Avaliação de Vulnerabilidade" ofertadas.
5.3.3	Experiência em estruturação e implantação de processos ITIL - Central de Serviços (Requisições, Incidentes e Problemas), Monitoramento de Eventos, Resposta a Incidentes de Segurança e Gerenciamento de Vulnerabilidades
5.3.2.2	Experiência comprovada de no mínimo (três) anos em instalação, customização, configuração e suporte técnico nos tipos de soluções da Plataforma de Segurança (EPP - Endpoint Protection, AntiSpam, Controle de Acesso à Rede, Syslog, IPS e Firewall).
5.4	HABILIDADES TÉCNICAS



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

5.4.1	Ter conhecimentos, habilidades e experiências cumulativas em pelo menos 80% das habilidades técnicas abaixo relacionadas:
5.4.1.1	Administração e suporte a ativos de segurança de rede tais como balanceadores de carga, firewall, IPS e IDS.
5.4.1.2	Administração e suporte a softwares de segurança da informação tais como antivírus, antispam e filtro de conteúdo.
5.4.1.3	Detecção de vulnerabilidades da rede.
5.4.1.4	Detecção de vulnerabilidades em sistemas, servidores e aplicações.
5.4.1.5	Administração e suporte de softwares voltados para a segurança de endpoints.
5.4.1.6	Administração e suporte a VPN (virtual private network).
5.4.1.7	Realização de auditoria e controle de processos para identificação de não conformidades ou falhas, com fornecimento de propostas para correção.
5.4.1.8	Definição de rotinas e procedimentos para prevenção a ataques.
5.4.1.9	Definição de políticas de segurança de rede.
5.4.1.10	Conhecimentos em LGPD (Lei Geral de Proteção de Dados).
5.4.1.11	Inteligência de Ameaças Cibernéticas;
5.4.1.12	Tratamento e Resposta a Eventos e Incidentes Cibernéticos;
5.4.1.13	Análise de Logs;
5.4.1.14	Detecção de intrusões;
5.4.1.15	Mitigação de ataques;
5.4.1.16	Monitoramento de redes;
5.4.1.17	Análise de tráfego de redes;
5.4.1.18	Criptografia;
5.4.1.19	Segurança de redes;
5.4.1.20	Ferramentas de análise de malware.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

5.4.1.2	
1	Capacidade de empregar linguagens de programação como Python, Power Shell, Bash e Perl.
5.5	CERTIFICAÇÃO TÉCNICA
5.5.1	A composição da Equipe SOC - ETAPA IMPLANTAÇÃO deve garantir que as certificações abaixo sejam garantidas por pelo menos um dos componentes da equipe técnica:
5.5.1.1	ISO/IEC 270001:2022 FOUNDATION;
5.5.1.2	GSEC GIAC Security Essentials ou Lead Cybersecurity Professional Certification LCSPC;
5.5.1.3	GCIH GIAC Incident Handler ou EC-Council Certified Incident Handler ou CompTIA CySA+;
5.5.1.4	Certificação do fabricante de administrador da solução de "Gerenciamento de eventos e informações de segurança (SIEM)" ofertada a ser implantada. Não serão aceitas certificações comerciais e/ou pré-venda.
5.5.1.5	Certificação do fabricante de administrador da solução de "Avaliação de Vulnerabilidade" ofertada a ser implantada. Não serão aceitas certificações comerciais e/ou pré-venda.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE F

PLANO DE CAPACITAÇÃO

1. Com vistas a manutenção da excelência dos serviços prestados, a CONTRATADA, sem custos adicionais para a SEFAZ BA, deverá promover continuamente o desenvolvimento e aperfeiçoamento de seus perfis profissionais com foco em aspectos técnicos, comportamentais, motivacionais e de relacionamento com os usuários.
2. "A CONTRATADA deverá elaborar, anualmente, o Plano de Capacitação de Profissionais às suas expensas, nas áreas de interesse dos serviços, considerando as mudanças de plataforma tecnológica ou processos de trabalho, de acordo com as orientações da SEFAZ BA.
3. O Plano de Capacitação deverá ser entregue pela CONTRATADA no prazo máximo de 30 (trinta) dias corridos após o início efetivo dos serviços, e depois anualmente, devendo contemplar no mínimo:
 - 3.1 Ementa das ações de capacitação e número de horas propostas, sendo obrigatório uma média global de 20 horas anuais por perfil profissional alocado na prestação de serviços.
 - 3.2 Cada um dos perfis profissionais alocados na prestação de serviços deve passar por, no mínimo, 8 horas de capacitação por ano, sem prejuízo da média global.
4. Após aprovação pela SEFAZ BA, a CONTRATADA ficará responsável pela execução integral do plano, que deverá ser distribuído ao longo do ano e não poderá prejudicar ou impactar o andamento dos serviços contratados.
5. A CONTRATADA deverá solicitar aprovação da SEFAZ BA sempre que houver modificação no Plano de Capacitação.
6. A cada 12 (doze) meses, a partir do início da operação dos serviços gerenciados de segurança conforme contrato assinado, a SEFAZ BA avaliará a execução do Plano de Capacitação e o considerará não executado caso o número de horas previstas, treinamentos ministrados ou as certificações efetivas sejam inferiores a 90% (noventa por cento) do planejado.
7. Adicionalmente, na hipótese de identificação de lacuna de competência esperada e/ou necessária para a execução dos serviços a contento, a SEFAZ BA poderá solicitar à CONTRATADA proposta de ação de capacitação específica que possa reparar a lacuna identificada, mesmo que não haja ação de capacitação relacionada no Plano Anual de Capacitação aprovado.
8. Considera-se como lacuna de competência esperada e/ou necessária, a identificação pela SEFAZ BA, durante a execução dos serviços, do não atendimento do perfil profissional aos requisitos de Conhecimentos Técnicos, Habilidades e Competências Comportamentais, Experiência, Certificação e Formação demandados na Requisição de Perfil Profissional que resultou na sua alocação para prestação de serviços.
9. Uma vez solicitado pela SEFAZ BA, a CONTRATADA deverá apresentar a proposta de ação de capacitação específica contemplando, no mínimo, ementa, duração e cronograma, em um prazo máximo de 10 dias corridos e submetê-la à aprovação do Banco.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

10. A ação de capacitação específica para reparar lacuna de competência não implica ajuste no Plano de Capacitação vigente, sendo ônus da CONTRATADA visando ajustar a capacitação do perfil profissional aos requisitos previamente solicitados
11. O descumprimento do prazo de 10 dias corridos, bem como a não realização da ação de capacitação específica aprovada, ensejarão a sinalização do não atendimento à demanda de reparação de lacuna de competência.
12. A sinalização de descumprimento do Plano de Capacitação ou o não atendimento à demanda de reparação de lacuna de competência, implicará a indicação de descumprimento das ações de capacitação continuada e, conseqüentemente, o não atingimento do nível de serviço previsto para o indicador de Capacitação Anual de Profissionais



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE G

QUALIFICAÇÃO TÉCNICA

1. A comprovação de aptidão da LICITANTE para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, deve ser através da apresentação de um ou mais atestados, em seu nome, fornecidos por pessoas jurídicas de direito público ou privado, preferencialmente de acordo com o modelo constante do ENCARTE K deste Anexo I.

A LICITANTE deve apresentar atestado(s) que enderecem todos os itens descritos abaixo, sob pena de desclassificação, caso não apresente tal(ais) documento(s) em tempo hábil.

1.1 **SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO**

Atestado(s) de capacidade técnica que comprovem ter a LICITANTE prestado, durante pelo menos 6 (seis) meses, serviços gerenciados de segurança semelhantes a todos os serviços previstos no objeto desta licitação, conforme definidos no Termo de Referência e seus anexos.

- 1.1.1 Serão aceitos apenas atestados de capacidade técnica que comprovem em um único atestado a prestação de todos os serviços gerenciados de segurança previstos no objeto desta licitação, conforme definidos no Termo de Referência e seus anexos.
- 1.1.2 Os serviços devem ter sido prestados em organizações com ambiente de TI compatíveis com o da SEFAZ BA, com pelo menos 50% dos quantitativos dos itens de configuração referentes a infraestrutura de TI existentes e em operação na SEFAZ BA, conforme tabela "AMBIENTE DE TI - SEFAZ BA" abaixo.
- 1.1.3 Além dos quantitativos citados acima, o ambiente de TI destas organizações deve possuir:
 - 1.1.3.1 Soluções de Gerenciamento de eventos e informações de segurança (SIEM) e Avaliação de Vulnerabilidades, implantadas e em operação;
 - 1.1.3.2 Pelo menos 4 (quatro) das seguintes soluções de segurança implantadas e em operação: EPP (Endpoint Protection), PAM (Privileged access management), Controle de Conteúdo WEB, NAC (Network Access Control), AntiSpam, SYSLOG e WSUS.

1.2 **FORNECIMENTO DE SOLUÇÃO DE GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA (SIEM)**

Atestado(s) de capacidade técnica que comprove(m) ter a LICITANTE fornecido a solução de "Gerenciamento de eventos e informações de segurança (SIEM)" ofertada para atender este Termo de Referência e seus anexos.

- 1.2.1 A solução deve ter sido fornecida para organizações com ambiente de TI compatíveis com o da SEFAZ BA, com pelo menos 50% dos quantitativos dos itens de configuração existentes e em operação na SEFAZ BA, conforme tabela "AMBIENTE DE TI - SEFAZ BA" abaixo.

145/174



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

1.3 GERENCIAMENTO DE PLATAFORMA DE SEGURANÇA - SOLUÇÃO DE GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA (SIEM)

Atestado(s) de capacidade técnica que comprove(m) ter a LICITANTE prestado, durante pelo menos 6 (seis) meses, o serviço de gerenciamento de plataforma de segurança da solução de "Gerenciamento de eventos e informações de segurança (SIEM)" ofertada para atender este Termo de Referência e seus anexos, incluindo as atividades de implantação, configuração, manutenção, monitoramento, operação e suporte técnico associadas.

1.3.1 Os serviços devem ter sido prestados em organizações com ambiente de TI compatíveis com o da SEFAZ BA, com pelo menos 50% dos quantitativos dos itens de configuração existentes e em operação na SEFAZ BA, conforme tabela "AMBIENTE DE TI - SEFAZ BA" abaixo.

1.4 FORNECIMENTO DE SOLUÇÃO DE AVALIAÇÃO DE VULNERABILIDADES - Atestado(s) de capacidade técnica que comprove(m) ter a LICITANTE fornecido a solução de "Avaliação de Vulnerabilidades" ofertada para atender este Termo de Referência e seus anexos.

1.4.1 A solução deve ter sido fornecida para organizações com ambiente de TI compatíveis com o da SEFAZ BA, com pelo menos 50% dos quantitativos dos itens de configuração existentes e em operação na SEFAZ BA, conforme tabela "AMBIENTE DE TI - SEFAZ BA" abaixo.

1.4.1.1 Além dos quantitativos acima a organização deve possuir pelo menos 50% da quantidade de usuários do AD ativos na SEFAZ BA. A SEFAZ BA possui 5.000 (cinco mil) usuários do AD ativos.

1.5 GERENCIAMENTO DE PLATAFORMA DE SEGURANÇA - SOLUÇÃO DE AVALIAÇÃO DE VULNERABILIDADES

Atestado(s) de capacidade técnica que comprove(m) ter a LICITANTE prestado, durante pelo menos 6 (seis) meses, o serviço de gerenciamento de plataforma de segurança da solução de Avaliação de Vulnerabilidades ofertada para atender este Termo de Referência e seus anexos, incluindo as atividades de implantação, configuração, manutenção, monitoramento, operação e suporte técnico associadas.

1.5.1 Os serviços devem ter sido prestados em organizações com ambiente de TI compatíveis com o da SEFAZ BA, com pelo menos 50% dos quantitativos dos itens de configuração existentes e em operação na SEFAZ BA, conforme tabela "AMBIENTE DE TI - SEFAZ BA" abaixo:

1.5.1.1 Além dos quantitativos acima a organização deve possuir pelo menos 50% da quantidade de usuários do AD existentes e em operação na SEFAZ BA. A SEFAZ BA possui 5.000 (cinco mil) usuários do AD ativos.

1.6 A LICITANTE deverá possuir nível de parceria equivalente a intermediário/avançado com a fabricante da solução de "Gerenciamento de eventos e informações de segurança (SIEM)" ofertada. Esta parceria deve ser comprovada através de certificado ou documento emitido pelo fabricante.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

- 1.7 A LICITANTE deverá possuir nível de parceria equivalente a intermediário/avançado com a fabricante da solução de "Avaliação de Vulnerabilidades" ofertada. Esta parceria deve ser comprovada através de certificado ou documento emitido pelo fabricante.

TABELA – AMBIENTE DE TI – SEFAZ BA

	INFRAESTRUTURA DE TI - ITENS DE CONFIGURAÇÃO	QTDE
1	SERVIDORES - WINDOWS, LINUX, HOSTS DE VIRTUALIZAÇÃO	914
2	BASE DE DADOS	
3	ATIVOS DE REDE LAN/SAN	
3.1	SWITCH LAN	
3.2	SWITCH SAN	
4	ATIVOS SEGURANÇA	
4.1	FIREWALL	
4.2	IPS	
4.3	BALANCEADOR DE CARGA	



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE H

TESTES DE ACEITAÇÃO

TESTES DE ACEITAÇÃO

Nesta etapa será verificado se o produto fornecido atende aos requisitos básicos e fundamentais identificados para sua aceitação. Esta aceitação deve ser pré-requisito para qualquer desembolso a ser realizado pela SEFAZ/BA com relação ao produto fornecido.

1. INSTALAÇÃO BÁSICA

Nesta atividade deverá ser realizada a instalação dos componentes do produto necessários e a verificação da sua adequação aos requisitos básicos e fundamentais conforme escopo definido acima e no **Termo de Referência**.

2. PRÉ-CONFIGURAÇÃO

Nesta atividade deverá ser realizada a configuração dos componentes instalados na atividade anterior e os ajustes necessários no ambiente existente para se verificar a adequação do produto ao **Termo de Referência**.

3. TESTES DE ACEITAÇÃO

Nesta atividade deverão ser realizados os testes de aceitação do produto verificando o pleno funcionamento, conforme **Termo de Referência**, dos itens identificados no escopo definido acima. A aceitação do produto depende da regularização de todos os problemas encontrados.

4. PRAZO ESTIMADO

O prazo estimado para execução desta etapa é de **15 (quinze) dias corridos**, prorrogáveis por mais **15 (quinze) dias corridos** a critério da CONTRATANTE.

Em caso de resultado satisfatório dos Testes de Aceitação será emitido **Termo de Aceite** do produto fornecido, pré-requisito para qualquer desembolso a ser realizado pela SEFAZ/BA para pagamento do produto.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE I

MODELO PARA COMPROVAÇÃO RESUMIDA DOS REQUISITOS TÉCNICOS

Software de Gerenciamento de eventos e informações de segurança (SIEM)		
ITEM SUBITEM	DESCRIÇÃO DO REQUISITO TÉCNICO	COMPROVAÇÃO TÉCNICA

Software de Gestão de Vulnerabilidades		
ITEM SUBITEM	DESCRIÇÃO DO REQUISITO TÉCNICO	COMPROVAÇÃO TÉCNICA



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE J

MODELO PARA ATESTADO DE VISTORIA TÉCNICA

ATESTADO DE VISTORIA TÉCNICA

Atesto que o preposto da _____ [indicar nome da Pessoa Jurídica licitante], CNPJ nº _____, Sr.(a) _____, CPF nº _____, interessado em participar da _____ (indicar modalidade de licitação: pregão/concorrência/tomada de preço/convite) nº _____, vistoriou _____ (indicar a Unidade Administrativa vistoriada) e tomou ciência do estado das condições locais para o cumprimento das obrigações relativas ao objeto licitado.

Salvador ____ de _____ de 20__.

(assinatura, identificação do servidor público e respectivo cadastro)



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO I - REQUISITOS GERAIS E ESPECIFICAÇÃO TÉCNICA

ENCARTE K

MODELOS DE PROVA DE QUALIFICAÇÃO TÉCNICA

COMPROVAÇÃO DE APTIDÃO PARA O DESEMPENHO

Declaramos, para fins de habilitação em processo licitatório, que a empresa
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, CNPJ XXXXXXXXXXXXXXX, com endereço na
XXXXXXXXXXXXXXXXXXXXXXXXXXXX, prestou serviço de xxxxxxxxxxxxxxx, atendendo integralmente as
especificações contratadas, inexistindo, até a presente data, registros negativos que comprometam a
prestação.

ESPECIFICAÇÃO	QUANTITATIVO	PRAZO DE EXECUÇÃO

Salvador ____ de _____ de 20__.

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

TERMO DE REFERÊNCIA

ANEXO II – MODELO DE PROPOSTA DE PREÇOS

MODELO DE PROPOSTA DE PREÇOS					
	ITENS	QTDE	UNIDADE	VALOR UNITÁRIO R\$	VALOR TOTAL R\$
1	Centro de Operação de Segurança (SOC) - Estruturação e implantação 3 (três) meses	1	ETAPA DE SERVIÇO		
2	Centro de Operação de Segurança (SOC) - Operação 21 (vinte e um) meses	21	SERVIÇO MENSAL		
3	Software de Gerenciamento de eventos e informações de segurança (SIEM) Licenciamento por 24 (vinte e quatro) meses	1	PACOTE (POR 24 MESES)		
4	Software de Gestão de Vulnerabilidades Licenciamento por 24 (vinte e quatro) meses	1	PACOTE (POR 24 MESES)		
				TOTAL (R\$)	

O degrau de valor no modo de disputa aberto será de R\$100,00 (cem reais), na forma do artigo 57 da Lei Federal nº 14.133/2021.

[Identificação completa do representante do licitante], como representante devidamente constituído de **[Identificação completa do licitante]**, doravante denominado LICITANTE, para fins de participação no certame licitatório acima identificado, declaro, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

(a) a proposta apresentada para participar desta licitação foi elaborada de maneira independente por mim e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato desta licitação, por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta elaborada para participar desta licitação não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato desta licitação, por qualquer meio ou por qualquer pessoa;

(c) que não tentei, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato desta licitação quanto a participar ou não dela;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

(d) que o conteúdo da proposta apresentada para participar desta licitação não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato desta licitação antes da adjudicação do objeto;

(e) que o conteúdo da proposta apresentada para participar desta licitação não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante do órgão licitante antes da abertura oficial das propostas; e

(f) que estou plenamente ciente do teor e da extensão desta declaração e que detenho plenos poderes e informações para firmá-la.

Salvador, ____ de _____ de 20__.

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

IV. MINUTA DO CONTRATO SERVIÇOS SEM DEDICAÇÃO EXCLUSIVA DE MÃO DE OBRA

(x) LICITAÇÃO

CONTRATO Nº ____/____ QUE ENTRE SI CELEBRAM O [ESTADO DA BAHIA] E A [PESSOA JURÍDICA] PARA OS FINS QUE NELE SE DECLARAM.

O **ESTADO DA BAHIA**, neste ato representado pelo(a) Dr(a). _____, titular da Secretaria _____, CNPJ nº _____, situada na _____, autorizado pelo Decreto de delegação de competência publicado no D.O.E. de ____/____/____, doravante denominado Contratante, [utilizar a menção ao Estado somente se for órgão da Administração Direta] e a _____ [pessoa jurídica], inscrita no CNPJ/MF sob o nº _____, sediada na _____, doravante representada pelo Sr(a). _____, portador da cédula de identidade nº _____, emitida por _____, inscrito(a) no CPF/MF sob o nº _____, conforme atos constitutivos da empresa ou procuração apresentada nos autos, doravante denominada Contratada, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº ____/____, processo administrativo nº _____, que se regerá pela Lei nº 14.634, de 28 de novembro de 2023, pela Lei Federal nº 14.133, de 1º de abril de 2021, e mediante as cláusulas e condições a seguir ajustadas.

CLÁUSULA PRIMEIRA – OBJETO

1.1 O objeto do presente instrumento é a prestação de serviços Centro de Operações de Segurança (SOC) com infraestrutura e operação remota para prover serviços gerenciados de segurança, processos e ferramentas de TI associadas, nas condições estabelecidas no Termo de Referência.

1.2 Vinculam-se a esta contratação, independentemente de transcrição neste instrumento:

- a) Termo de Referência;
- b) Proposta da Contratada;
- c) Edital da Licitação;
- d) Eventuais anexos dos documentos supracitados.

1.3 O modelo de execução do objeto observará o disposto no Termo de Referência.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1 O prazo de vigência do Contrato é de 27 (vinte e sete) meses a **contar da data** da (x) **assinatura do Contrato**, prorrogável até atingir o limite de 10 anos, na forma dos arts. 106 e 107 da Lei Federal nº 14.133/2021.

2.2 A prorrogação de que trata esta Cláusula está condicionada à justificativa e autorização da autoridade competente para celebrar o ajuste, devendo as condições e preços permanecerem vantajosos para o Contratante, permitida a negociação com a Contratada, observando-se, ainda, o cumprimento dos seguintes requisitos:

- a) comprovação de que a forma de execução do objeto tem natureza continuada;
- b) apresentação de relatório que discorra sobre a execução do Contrato e sua regularidade;
- c) apresentação de justificativa e motivo, por escrito, de que a Administração mantém interesse na continuidade da execução contratual;
- d) manifestação expressa da Contratada informando o interesse na prorrogação;
- e) comprovação de que a Contratada mantém as condições iniciais de habilitação.

2.3 A Contratada não tem direito subjetivo à prorrogação contratual.

2.4 A prorrogação do Contrato deverá ser promovida mediante celebração de termo aditivo.

154/174



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

2.5 Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6 O Contrato não poderá ser prorrogado, quando for aplicada à Contratada (art. 44, §3º, inc. III, do Decreto nº 23.113, de 9 de outubro de 2024):

- a) a sanção de impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do Estado da Bahia;
- b) a sanção de declaração de inidoneidade para licitar e contratar, nos termos do art. 156, §5º, da Lei Federal nº 14.133/2021.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1 As regras de execução e de gestão do contrato constam no Termo de Referência, anexo a este Contrato (art. 92 da Lei Federal nº 14.133/2021).

3.2 Fica indicado como gestor deste Contrato o servidor _____, matrícula:

Nota: alternativamente, a nomeação do gestor do contrato pode ser feita por portaria.

3.3 Fica(m) indicado(s) como fiscal(is) deste Contrato o(s) servidor(es): _____
matrícula(s): _____

Notas: alternativamente, a nomeação do fiscal e/ou comissão pode ser feita por portaria.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1 Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA – PREÇO

5.1 O Contratante pagará à Contratada os valores estimados especificados no quadro abaixo:

	ITENS	QTDE	UNIDADE	VALOR UNITÁRIO R\$	VALOR TOTAL R\$
1	Centro de Operação de Segurança (SOC) - Estruturação e implantação 3 (três) meses	1	ETAPA DE SERVIÇO		
2	Centro de Operação de Segurança (SOC) - Operação 21 (vinte e um) meses	21	SERVIÇO MENSAL		
3	Software de Gerenciamento de eventos e informações de segurança (SIEM) Licenciamento por 24 (vinte e quatro) meses	1	PACOTE (POR 24 MESES)		
4	Software de Gestão de Vulnerabilidades Licenciamento por 24 (vinte e quatro) meses	1	PACOTE (POR 24 MESES)		
				TOTAL (R\$)	

5.1.1 Estima-se para o Contrato o valor global de R\$ _____ (_____)

5.2. Nos preços contratados estão incluídos todos os custos com material de consumo, salários, encargos sociais, previdenciários, fiscais, comerciais e trabalhistas de todo o pessoal da Contratada, como também



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela Contratada das obrigações.

5.3 O valor do Contrato referido nesta Cláusula é meramente estimativo, dependendo os pagamentos devidos à Contratada dos quantitativos efetivamente executados.

5.4 Os pagamentos com recursos do Contrato de Empréstimo nº4970/OC-BR somente serão realizados em decorrência de serviços realizados durante a vigência do Contrato de Empréstimo nº4970/OC-BR. Após o encerramento do Contrato de Empréstimo nº4970/OC-BR, caso ainda haja pagamentos decorrentes dos serviços deste Contrato, ou necessidade de aditivos, tais pagamentos poderão ser realizados por outras fontes de recursos.

CLÁUSULA SEXTA – PAGAMENTO

6.1 O prazo para pagamento à Contratada e as demais condições a ele referentes encontram-se definidos no Termo de Referência, que constitui anexo deste Contrato (art. 92, incs. V e VI, da Lei Federal nº 14.133/2021).

CLÁUSULA SÉTIMA – MANUTENÇÃO DO EQUILÍBRIO ECONÔMICO FINANCEIRO DO CONTRATO

Reajustamento em sentido estrito

7.1 Os preços inicialmente contratados são fixos e irremovíveis no prazo de 1 (um) ano contado de 07/03/2025, **data do orçamento estimado** (art. 92, inciso V, e §3º, da Lei Federal nº 14.133/2021).

7.2 Após o interregno de 1 (um) ano, independentemente de pedido da Contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do índice INPC/IBGE.

7.2.1 Na hipótese de não reajustamento dos preços pelo Contratante, o requerimento de reajuste deverá ser formulado durante a vigência do Contrato e antes de eventual prorrogação nos termos do art. 131, parágrafo único, da Lei Federal nº 14.133/2021, sob pena de preclusão.

7.3 Nos reajustamentos subsequentes ao primeiro, o interregno mínimo de 1 (um) ano será contado a partir dos efeitos financeiros do último reajuste.

7.4 Na hipótese de atraso ou não divulgação do(s) índice(s) de reajustamento, o Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

7.4.1 A Contratada deverá apresentar a memória de cálculo referente ao reajustamento de preços correspondente a eventual valor remanescente.

7.5 Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.6 Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço no período remanescente do Contrato, por meio de termo aditivo.

7.7 O reajustamento será realizado por apostilamento, na forma do art. 136, inc. I, da Lei Federal nº 14.133/2021.

Outras causas de reequilíbrio econômico-financeiro

7.8 O reestabelecimento do equilíbrio econômico-financeiro dependerá de requerimento da Contratada quando visar recompor o preço que se tornou insuficiente, devendo ser instruído com a documentação que comprove o desequilíbrio econômico-financeiro do Contrato.

7.8.1 O requerimento de restabelecimento do equilíbrio econômico-financeiro inicial do Contrato, nas hipóteses do art. 124, inc. II, "d", da Lei Federal nº 14.133/2021, deverá ser formulado pelo interessado no prazo máximo de 1 (um) ano do fato que o ensejou, sob pena de decadência, em consonância com o art. 211 da Lei Federal nº 10.406, de 10 de janeiro de 2002.

7.8.2 Na hipótese de contratos de fornecimento ou serviços contínuos, o requerimento de

156/174



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

restabelecimento do equilíbrio econômico-financeiro deverá ser formulado durante a vigência do Contrato e antes de eventual prorrogação nos termos do art. 107 da Lei Federal nº 14.133/2021, sob pena de preclusão (art. 131, parágrafo único, da Lei Federal nº 14.133/2021).

7.8.2.1 Fica convencionado que, nos casos de contrato de fornecimento ou serviços contínuos com prazo de vigência superior a 1 (um) ano, o requerimento de restabelecimento do equilíbrio econômico-financeiro do Contrato deverá observar a disposição da subcláusula 7.8.1.

7.9. O Contratante, no prazo máximo de 60 (sessenta) dias, prorrogável por igual período mediante justificativa, responderá a eventuais pedidos de manutenção do equilíbrio econômico-financeiro do Contrato apresentado pela Contratada (art. 92, inc. XI, c/c art. 123, parágrafo único, da Lei Federal nº 14.133/2021).

7.10 O processo de reestabelecimento do equilíbrio econômico-financeiro em favor do Contratante deverá ser instaurado quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no Contrato.

7.11 A Contratada não fará jus à recomposição do equilíbrio econômico-financeiro caso quaisquer dos riscos por ela assumidos no Contrato venham a se materializar (art. 124, inc. II, "d", parte final, da Lei Federal nº 14.133/2021);

7.12 No caso de contratações de obras e serviços de engenharia, a hipótese de que trata a subcláusula 7.8.1 abrange as situações em que a execução contratual seja obstada pelo atraso na conclusão de procedimentos de desapropriação, desocupação, servidão administrativa ou licenciamento ambiental, por circunstâncias alheias à Contratada (art. 124, §2º, da Lei Federal nº 14.133/2021).

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE E DA CONTRATADA

Obrigações do Contratante

8.1 O Contratante, além das determinações contidas no instrumento convocatório, bem como daquelas decorrentes de lei, obriga-se a:

- a) exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com este Contrato e seus anexos, fornecendo por escrito as informações necessárias para a execução do objeto contratado;
- b) receber o objeto no prazo e condições estabelecidas no Termo de Referência;
- c) acompanhar e fiscalizar a execução do Contrato e o cumprimento das obrigações pela Contratada;
- d) intimar a Contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto do Contrato, para que seja por ela substituído, reparado ou corrigido, no total ou em parte, às suas expensas, no prazo indicado, certificando-se de que as soluções propostas pela Contratada são as mais adequadas;
- e) comunicar-se com a Contratada para emissão de nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) relativamente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei Federal nº 14.133/2021;
- f) efetuar o pagamento à Contratada do valor correspondente à execução do objeto, conforme prazo, forma e condições estabelecidos no Termo de Referência;
- g) aplicar à Contratada as sanções previstas em lei e neste Contrato;
- h) explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato apresentadas pela Contratada, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste, no prazo definido na subcláusula 8.1.1;
- i) responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro apresentados pela Contratada no prazo definido na subcláusula 7.9;
- j) intimar os emitentes das garantias relativamente ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, §4º, da Lei Federal nº 14.133/2021);
- k) assegurar-se, na hipótese de execução do objeto contratado em suas dependências ou em local por ele designado, que o ambiente de trabalho, inclusive seus equipamentos e instalações, apresentem condições adequadas ao cumprimento, pela Contratada, das normas de segurança e saúde no trabalho;

8.1.1 O Contratante, no prazo de 30 (trinta) dias, a contar da data do protocolo do(s) requerimento(s) relacionado(s) à execução do Contrato, decidirá sobre todas as solicitações e reclamações apresentadas pela Contratada, admitida a prorrogação motivada do prazo, por igual período (art. 123 da Lei Federal nº 14.133/2021).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Notas:

1. Nos termos do art. 123, caput, da Lei Federal nº 14.133/2021, a Administração tem o dever de decidir questões contratuais que lhe são apresentadas.

2. O prazo a que se refere a subcláusula 8.1.1 deve ser definido conforme a complexidade do objeto contratual e os trâmites internos das áreas envolvidas na execução do Contrato. Caso não haja especificação, o prazo será de 1 (um) mês, conforme o art. 123, parágrafo único, da Lei Federal nº 14.133/2021.

8.1.2 Além das determinações acima descritas, o Contratante deverá atender às seguintes obrigações específicas indicadas no Termo de Referência.

Obrigações da Contratada

8.2 A Contratada deve cumprir todas as obrigações constantes neste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações decorrentes de lei e aquelas a seguir dispostas:

- a) designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução do Contrato, inclusive para atendimento de emergência, servindo de interlocutor e canal de comunicação entre as partes, observado o art. 118 da Lei Federal nº 14.133/2021, cuja designação ou manutenção poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, hipótese em que a Contratada designará outro profissional para o exercício da atividade;
- b) atender às determinações regulares emitidas pelo Contratante e prestar o(s) esclarecimento(s) ou informação(ões) por ele solicitado(s) (art. 137, inc. II, da Lei Federal nº 14.133/2021);
- c) reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo Contratante, os bens e serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- d) responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, nos termos das normas de regência, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;
- e) não contratar, durante a vigência do Contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do Contratante ou do fiscal ou gestor do Contrato, nos termos do art. 48, parágrafo único, da Lei Federal nº 14.133/2021;
- f) quando não for possível a verificação da regularidade no Cadastro de Fornecedores, entregar ao setor responsável pela fiscalização do Contrato, junto com a nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda estadual, municipal ou distrital do domicílio ou sede da Contratada; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;
- g) manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação ou no procedimento de contratação direta;
- h) prestar todo esclarecimento ou informação solicitados pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do objeto;
- i) executar o objeto sem solução de continuidade durante todo o prazo da vigência do Contrato e comunicar ao Contratante qualquer anormalidade ou acidente que interfira no bom andamento do Contrato;
- j) paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;
- k) promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do Contrato;
- l) conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local da execução do objeto e nas melhores condições de segurança, higiene e disciplina;
- m) reparar, repor ou restituir, nas mesmas condições e especificações, dentro do prazo determinado pelo Contratante, os equipamentos e utensílios eventualmente recebidos para uso nos serviços objeto



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

deste contrato, deixando-os em perfeita condição de funcionamento;

n) assegurar a seus trabalhadores ambiente de trabalho em condições adequadas ao cumprimento às normas de saúde, segurança e bem estar no trabalho e fazer com que seus empregados as respeitem, bem como atentar para as regras de cortesia no local onde serão executados os serviços;

o) responsabilizar-se pelo cumprimento das obrigações trabalhistas, sociais, previdenciárias, tributárias, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

p) submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência e/ou Projeto Básico;

q) cumprir, durante todo o período de execução do Contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas em outras normas específicas, devendo, sempre que solicitado pelo Contratante, indicar os empregados que preencherem as vagas correspondentes (art. 116 da Lei Federal nº 14.133/2021);

r) atender as obrigações concernentes à aprendizagem de que trata o art. 429 do Decreto-Lei nº 5.452/1943 (Consolidação das Leis do Trabalho - CLT), Lei nº 14.395/2021, e normas regulamentares, em especial:

1) recrutar, preferencialmente, para a contratação de aprendizes, os estudantes indicados no art. 38, §2º, da Lei nº 14.395/2021, no percentual mínimo de 10% (dez por cento) do quadro de aprendizes da Contratada;

2) apresentar ao fiscal ou responsável pela gestão e acompanhamento do Contrato, no prazo de até 05 (cinco) dias úteis contado do início efetivo da execução do objeto, a lista completa dos aprendizes, indicando aqueles selecionados no banco de dados de que trata a Lei nº 14.395/2021, devendo justificar, perante o Contratante, a eventual impossibilidade de seu cumprimento.

s) guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato;

t) arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, inc. II, "d", da Lei Federal nº 14.133/2021;

u) observar a legislação federal, estadual e municipal, relativa ao objeto do Contrato, bem como as normas internas do Contratante;

v) alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste Contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

x) não permitir a utilização de qualquer trabalho do menor de 16 (dezesesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze) anos, nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;

y) providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução do Contrato, arcando com os custos para sua obtenção;

w) efetuar pontualmente o pagamento de tributos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do presente Contrato;

z) emitir nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente(s) de acordo com a legislação, contendo descrição dos bens, obras e/ou serviços, com o valor exato dimensionado pela fiscalização, indicando, conforme o caso, sua quantidade, preço unitário e valor total;

aa) realizar os serviços de manutenção e assistência técnica conforme prescrições do Termo de Referência;

bb) fornecer as instalações, aparelhamento e pessoal técnico exigidos na licitação ou no procedimento de contratação direta;

cc) alocar, durante todo o período de execução do objeto, profissional, devidamente registrado no conselho profissional competente, quando for o caso, detentor de atestado de responsabilidade técnica e a equipe técnica mínima exigida no Termo de Referência, admitindo-se a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pelo Contratante;

dd) responder por quaisquer compromissos assumidos com terceiros, bem como por qualquer dano causado a terceiros em decorrência de ato próprio, de seus empregados, prepostos ou subordinados;

ee) promover, por sua conta e risco, transporte de bens;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

- ff) executar, quando for o caso, a montagem dos equipamentos, de acordo com as especificações e/ou normas exigidas, utilizando ferramentas apropriadas e dispendo de infraestrutura e equipe técnica necessárias à sua execução;
- gg) ressarcir o Contratante pelos danos decorrentes de paralisação ou interrupção da execução do objeto contratado;
- hh) realizar, quando exigido no Termo de Referência, a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo ser exigida, inclusive, a capacitação dos técnicos do Contratante ou da nova empresa que continuará a execução dos serviços.
- ii) tratando-se de obras, serviços e fornecimento de grande vulto, implantar Programa de Integridade, na forma do Decreto nº 23.356, de 17 de janeiro de 2025;
- jj) providenciar o cadastramento de seu representante legal ou procurador no site www.comprasnet.ba.gov.br ou outro que venha a substituí-lo, para a prática de atos através do Sistema Eletrônico de Informações – SEI;
- kk) manter atualizados os seus dados cadastrais, com a apresentação de documentos comprobatórios de mudança de endereços, inclusive eletrônicos (e-mail), telefones, composição societária, endereço dos sócios, contratos sociais e alterações;
- ll) atender às obrigações de que tratam os Anexos deste Contrato;

Matriz de risco

8.3 A Matriz de Risco constitui parte integrante deste Contrato, independentemente de transcrição, na forma do Anexo 5 deste Contrato.

8.3.1 A Contratada não é responsável pelos riscos relacionados ao objeto do ajuste cuja responsabilidade tenha sido atribuída ao Contratante na Matriz de Risco, sem prejuízo da responsabilidade deste pelo cumprimento das obrigações elencadas na subcláusula 8.1.

8.3.2 A Contratada é integral e exclusivamente responsável por todos os riscos relacionados ao objeto do ajuste a ela atribuídos na Matriz de Risco, sem prejuízo da sua responsabilidade pelo cumprimento das obrigações elencadas na subcláusula 8.2.

CLÁUSULA NONA – GARANTIA DA CONTRATAÇÃO

9.1 As disposições sobre a garantia da contratação estão disciplinadas no Termo de Referência.

CLÁUSULA DÉCIMA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

10.1 Constituem infrações administrativas para os fins deste Contrato, as condutas tipificadas no art. 155 da Lei Federal nº 14.133/2021.

10.2 Serão aplicadas à Contratada que incorrer nas infrações tipificadas no art. 155 da Lei Federal nº 14.133/2021, as sanções previstas no art. 156 da mesma norma, observados os arts. 48 e 49 da Lei nº 14.634/2023 e a disciplina constante no Decreto nº 23.113/2024.

10.3 No que concerne à multa, será observado o que se segue:

11.1. Constituem infrações administrativas para os fins deste Contrato, as condutas constantes do art. 155 da Lei Federal nº 14.133, de 2021.

11.2. Serão aplicadas à Contratada que incorrer nas infrações constantes do art. 155 da Lei Federal nº 14.133, de 2021, as sanções previstas no art. 156 da mesma norma, observado os arts. 48 e 49 da Lei nº 14.634, de 2023 e a disciplina constante do Regulamento do Estado da Bahia.

11.3. No que concerne à multa, será observado o que se segue:

11.3.1. Multa compensatória:

- a) No caso de descumprimento total da obrigação principal, será aplicada multa compensatória no percentual de 10% (dez por cento) incidente sobre o valor global do contrato.
- b) Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicada multa compensatória no percentual de 10% (dez por cento) incidente sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento já realizado.
- c) No caso de descumprimento da obrigação acessória, será aplicada multa compensatória no

160/174



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

percentual de 5% (cinco por cento) incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo.

d) No caso de recusa injustificada do adjudicatário em assinar o termo de contrato, em aceitar ou retirar o instrumento equivalente, ou, quando for o caso, em assinar a ata de registro de preços, ou praticar condutas a elas equiparadas, será aplicada multa compensatória no percentual de 10% (dez por cento) incidente sobre o valor correspondente ao objeto adjudicado ou, quando for o caso, da estimativa da contratação.

11.3.1.1. Considera-se acessória, para os fins deste Contrato, a obrigação contratual de natureza instrumental, secundária ou meramente formal.

11.3.1.2. O inadimplemento de obrigação acessória que retarde, comprometa ou impeça a execução da obrigação principal será considerado descumprimento da obrigação principal, sujeitando-se às cominações legais respectivas.

11.3.2. Multa moratória:

a) O atraso injustificado na execução do Contrato ensejará a aplicação de multa moratória no percentual de 0,2% (dois décimos por cento) ao dia, incidente sobre o valor da obrigação descumprida ou da estimativa arbitrada do seu custo, observado o percentual máximo total de 30% (trinta por cento).

b) O atraso injustificado do prazo fixado para apresentação, suplementação ou reposição de garantia contratual ensejará a aplicação de multa moratória no percentual de 0,3% (três décimos por cento) ao dia, incidente sobre o valor global do contrato.

11.3.2.1. A aplicação de multa moratória não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do Contrato com a aplicação cumulada de outras sanções previstas na Lei Federal nº 14.133, de 2021.

11.3.2.2. Na hipótese do subitem anterior, se o cálculo da multa moratória atingir o patamar correspondente ao valor máximo da multa compensatória, o recebimento do objeto deverá ser recusado, salvo justificativa escrita devidamente fundamentada, sem prejuízo da aplicação das demais sanções previstas em lei.

11.4. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante, observado o disposto na Lei Estadual nº 12.209, de 20 de abril de 2011 (art. 156, §9º, da Lei Federal nº 14.133, de 2021).

11.5. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei Federal nº 14.133, de 2021).

11.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei Federal nº 14.133, de 2021):

- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;
- d) os danos que dela provierem para o Contratante;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.7. Os atos previstos como infrações administrativas na Lei Federal nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e a autoridade competente definidos na referida Lei e no Regulamento do Estado da Bahia (art. 159 da Lei Federal nº 14.133, de 2021 e §3º do art. 47 da Lei nº 14.634, de 2023).

11.8. A personalidade jurídica da Contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos em lei e neste Contrato ou para provocar confusão patrimonial.

11.8.1. Com a desconsideração da personalidade jurídica, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com a Contratada.

11.8.2 Em todos os casos de desconsideração da personalidade jurídica deverão ser observados o

161/174



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

11.9. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ele aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal (art. 161 da Lei Federal nº 14.133, de 2021 e §1º do art. 55 da Lei nº 14.634, de 2023).

11.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei Federal nº 14.133, de 2021, conforme disciplinado no Regulamento do Estado da Bahia (art. 60 da Lei nº 14.634, de 2023).

11.11. A apuração das infrações administrativas será realizada em processo administrativo sancionatório, com a observância das garantias da ampla defesa e do contraditório, na forma do regulamento, conforme disciplina constante do Regulamento do Estado da Bahia.

11.11.1 Será admitida medida cautelar destinada a garantir o resultado útil do processo administrativo sancionatório, de forma antecedente ou incidental à sua instauração, inclusive a retenção provisória do valor correspondente à estimativa da sanção de multa.

11.11.2 O valor da retenção provisória a que se refere o subitem anterior deste artigo não poderá exceder ao limite máximo estabelecido no §3º do art. 156 da Lei Federal nº 14.133, de 2021.

CLÁUSULA DÉCIMA PRIMEIRA – EXTINÇÃO CONTRATUAL

11.1 O Contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes.

11.1.1 O Contrato pode ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o Contrato não mais lhe oferece vantagem (art. 106, inc. III, da Lei Federal nº 14.133/2021).

11.1.1.1 Na hipótese de que trata a subcláusula 11.1.1, a extinção ocorrerá na próxima data de aniversário do Contrato, condicionada à intimação da Contratada sobre a não continuidade do pacto com, no mínimo, 2 (dois) meses de antecedência da referida data (art. 106, §1º, da Lei Federal nº 14.133/2021).

11.1.1.1.1 Caso a intimação de que trata a subcláusula 11.1.1 ocorra com menos de 2 (dois) meses da data de aniversário do Contrato, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

11.2. O Contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no art. 137 da Lei Federal nº 14.133/2021, assegurados o contraditório e a ampla defesa.

11.2.1. A extinção do contrato poderá ser:

a) determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta (arts. 138, inc. I, e 139 da Lei Federal nº 14.133/2021);

b) consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração (art. 138, inc. II, da Lei Federal nº 14.133/2021);

c) determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial (art. 138, inc. III, da Lei Federal nº 14.133/2021).

11.2.2. A alteração social, da finalidade ou da estrutura da empresa Contratada não ensejará a extinção contratual se não restringir sua capacidade de concluir o Contrato (art. 137, inc. III, da Lei Federal nº 14.133/2021).

11.2.2.1. Se a alteração de que trata a subcláusula 11.2.2 implicar mudança da pessoa jurídica Contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

11.2.3. O Contrato será extinto caso se constate que a Contratada mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou da entidade Contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do Contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inc. IV, da Lei Federal nº 14.133/2021).

11.3 O termo de extinção, sempre que possível, será precedido de:

a) balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

- b) relação dos pagamentos já efetuados e ainda devidos;
- c) indenizações e multas.

11.4 A extinção do Contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, observada a Cláusula Sétima deste Contrato, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131 da Lei Federal nº 14.133/2021).

CLÁUSULA DÉCIMA SEGUNDA – DOTAÇÃO ORÇAMENTÁRIA

12.1 As despesas para o pagamento do presente Contrato correrão à conta de recursos da Dotação Orçamentária a seguir especificada (art. 92, inc. VIII, da Lei Federal nº 14.133/2021):

Unidade Orçamentária	13.101	Unidade Gestora	0003
Destinação da Despesa	1.754.0.125.800112 / 2.754.0.325.800112	Natureza da Despesa	4.4.90.40.00
Projeto / Atividade	04.126.441.1451 - Modernização de Tecnologia da Informação e Comunicação		

12.2 A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e a liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA TERCEIRA – ALTERAÇÕES

13.1 Eventuais alterações contratuais se regerão pela disciplina dos arts. 124 e seguintes da Lei Federal nº 14.133/2021.

13.2 A Contratada é obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato que se fizerem nas obras, nos serviços ou nas compras, e, de até 50% (cinquenta por cento), no caso de reforma de edifício ou de equipamento (art. 125 da Lei Federal nº 14.133/2021).

13.3 As alterações unilaterais não poderão transfigurar o objeto da contratação (art. 126 da Lei Federal nº 14.133/2021).

13.4 Caso o Contrato não contemple preços unitários para obras ou serviços cujo aditamento se fizer necessário, esses serão fixados por meio da aplicação da relação geral entre os valores da proposta e o do orçamento-base da Administração sobre os preços referenciais ou de mercado vigentes na data do aditamento, respeitados os limites estabelecidos na subcláusula 13.2 (art. 127 da Lei Federal nº 14.133/2021).

13.5 Nas alterações contratuais para supressão de obras, bens ou serviços, se a Contratada já houver adquirido os materiais e os colocado no local dos trabalhos, estes deverão ser pagos pela Administração pelos custos de aquisição regularmente comprovados e monetariamente reajustados, podendo caber indenização por outros danos eventualmente decorrentes da supressão, desde que regularmente comprovados (art. 129 da Lei Federal nº 14.133/2021).

13.6 Caso haja alteração unilateral do Contrato que aumente ou diminua os encargos da Contratada, a Administração deverá restabelecer, no mesmo termo aditivo, o equilíbrio econômico-financeiro inicial (art. 130 da Lei Federal nº 14.133/2021).

13.7 Os preços contratados serão alterados, para mais ou para menos, conforme o caso, se houver, após a data da apresentação da proposta, criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços contratados (art. 134 da Lei Federal nº 14.133/2021).

13.8 Nas contratações de obras e serviços de engenharia, a diferença percentual entre o valor global do Contrato e o preço global de referência não poderá ser reduzida em favor da Contratada em decorrência de aditamentos que modifiquem a planilha orçamentária (art. 128 da Lei Federal nº 14.133/2021).

13.9 As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação do órgão de assessoramento jurídico do Contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

prazo máximo de 1 (um) mês (art. 132 da Lei Federal nº 14.133/2021).

13.10. Registros que não caracterizam alteração do Contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, conforme art. 136 da Lei Federal nº 14.133/2021.

CLÁUSULA DÉCIMA QUARTA – PUBLICAÇÃO

14.1. Incumbirá ao Contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei Federal nº 14.133/2021.

CLÁUSULA DÉCIMA QUINTA – COMUNICAÇÃO ELETRÔNICA

15.1. Fica pactuado que os atos de comunicação processual com a Contratada poderão ser realizados por meio eletrônico, na forma da Lei nº 12.209/2011 e do Decreto nº 15.805, de 30 de dezembro de 2014.

15.1.1. A Contratada deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais, conforme Decreto nº 17.983, de 24 de outubro de 2017, devendo atender às convocações da Administração para a prática de atos nos prazos indicados.

CLÁUSULA DÉCIMA SEXTA - OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

16.1 As partes se comprometem a cumprir a Lei Federal nº 13.709/2018 (Lei de Proteção de Dados Pessoais - LGPD), bem como regras e regulamentos que lhe forem aplicáveis e que tenham por objeto os dados pessoais tratados no âmbito do objeto contratado.

16.2 A Contratada deverá utilizar os dados pessoais recebidos em função do objeto do Contrato somente para a finalidade pactuada, não podendo, em caso algum, utilizar esses dados pessoais para finalidade distinta, sob pena de extinção imediata da contratação.

16.3 A Contratada se obriga a não armazenar, arquivar, reproduzir, transmitir, distribuir, transferir ou de qualquer forma compartilhar os dados pessoais disponibilizados pelo Contratante com terceiros, salvo nas hipóteses legalmente previstas.

16.4 Em caso de incidente de vazamento de dados pessoais, a Contratada deverá enviar comunicação ao Contratante, por escrito, no prazo máximo de 24 (vinte e quatro) horas contado a partir da ciência do vazamento, contendo, no mínimo, as seguintes informações: a) data e hora do incidente; b) data e hora da ciência pela Contratada; c) relação dos tipos de dados afetados pelo incidente; d) relação de titulares afetados pelo incidente; e e) indicação de medidas que estiverem sendo tomadas para sanar e mitigar o incidente, bem como para reparar eventuais danos e evitar novos incidentes.

16.5 O Contratante deverá ser informado no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pela Contratada.

16.6 A Contratada deverá exigir de suboperadores e subcontratados o cumprimento dos deveres desta Cláusula, permanecendo integralmente responsável por garantir sua observância.

16.7 Encerrado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da Contratada eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

16.8 A Contratada deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações sobre os dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

16.9 Em caso de descumprimento de qualquer obrigação prevista nesta Cláusula, a Contratada ficará sujeita à integral responsabilização, inclusive por perdas e danos, aplicação das sanções cabíveis e da extinção do Contrato.

CLÁUSULA DÉCIMA SÉTIMA – DISPOSIÇÕES GERAIS

17.1 Constatada irregularidade no procedimento licitatório, de contratação direta ou na execução contratual, caso não seja possível o saneamento, a decisão sobre a suspensão da execução ou sobre a declaração de nulidade do Contrato observará o disposto no art. 147 da Lei Federal nº 14.133/2021.

17.2 O Contratante não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do Contrato.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

17.3 Os casos omissos serão dirimidos pelo Contratante, segundo as disposições contidas na Lei Federal nº 14.133/2021, na Lei nº 14.634/2023 e demais normas aplicáveis.

17.4 Na contagem dos prazos estabelecidos neste Contrato, será observado o art. 183 da Lei Federal nº 14.133/2021 e o art. 67 da Lei nº 14.634/2023.

CLÁUSULA DÉCIMA-OITAVA – DAS PRÁTICAS PROIBIDAS

A CONTRATADA deverá observar os mais altos padrões éticos durante a execução do Contrato, estando sujeitas às sanções previstas na legislação brasileira e nas normas do BID.

O BID reserva-se o direito de, diretamente ou por agente por ele designado, realizar inspeções ou auditorias nos registros contábeis e nos balanços financeiros da CONTRATADA relacionados com a execução do Contrato.

Se, de acordo com o procedimento administrativo do Banco, ficar comprovado que um funcionário da CONTRATADA ou quem atue em seu lugar incorreu em práticas corruptas, o Banco poderá declarar inelegíveis a CONTRATADA e/ou seus funcionários diretamente envolvidos em práticas corruptas, temporária ou permanentemente, para participar em futuras licitações ou contratos financiados com recursos do Banco.

Aplicam-se à CONTRATADA todas as disposições referentes às Práticas Proibidas (Anexo 4 do Edital) e à incorporação do reconhecimento recíproco de sanções por parte de Instituições Financeiras Internacionais (IFI).

CLÁUSULA DÉCIMA NONA – FORO

18.1 As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para solucionar quaisquer dúvidas oriundas deste instrumento que não puderem ser dirimidas por quaisquer dos meios alternativos de resolução de controvérsias de que trata a Lei Federal nº 14.133/2021.

[Local], [dia] de [mês] de [ano].

Representante legal do Contratante

Representante legal da Contratada

TESTEMUNHAS:

1-



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Anexo 3 - RELAÇÃO DOS PAÍSES MEMBROS DO BID - BANCO INTERAMERICANO DE DESENVOLVIMENTO
Elegibilidade para Provisão de Bens, Obras e Serviços em Contratos Financiados pelo Banco

Nota: O termo "Banco" usado neste documento inclui o BID, o Fumin e outros fundos administrados por ele.

.....

1) Países Membros quando o financiamento provém do Banco Interamericano de Desenvolvimento.

a) Países Mutuários:

(i) Argentina, Bahamas, Barbados, Belize, Bolívia, Brasil, Chile, Colômbia, Costa Rica, Equador, El Salvador, Guatemala, Guiana, Haiti, Honduras, Jamaica, México, Nicarágua, Panamá, Paraguai, Peru, República Dominicana, Suriname, Trinidad e Tobago, Uruguai e Venezuela.

b) Países não Mutuários:

(i) Alemanha, Áustria, Bélgica, Canadá, República Popular da China, República da Coreia, Croácia, Dinamarca, Eslovênia, Espanha, Estados Unidos, Finlândia, França, Israel, Itália, Japão, Noruega, Países Baixos, Portugal, Reino Unido, Suécia e Suíça.

c) Territórios elegíveis:

- (i) Guadalupe, Guiana Francesa, Martinica, Reunião - como Estado da França
- (ii) Ilhas Virgens dos EUA, Porto Rico, Guam - como Território dos EUA
- (iii) Aruba - como um país integrante do Reino dos Países Baixos, assim como, Bonaire, Curaçao, Santa Marta, Saba, Santo Eustáquio - como Estados do Reino dos Países Baixos
- (iv) Hong Kong - Região Administrativa Especial da República Popular da China.

2) Critérios para determinar a nacionalidade e origem dos bens e serviços

As disposições das políticas tornam necessário estabelecer critérios para determinar: a) a nacionalidade das firmas e indivíduos elegíveis para participar em contratos financiados pelo Banco; e b) o país de origem dos bens e serviços. Nessas determinações, serão utilizados os seguintes critérios:

A) Nacionalidade

a) Um indivíduo é considerado nacional de um país membro do Banco se satisfaz um dos seguintes requisitos:

- i. é cidadão de um país membro; ou
- ii. estabeleceu seu domicílio em um país membro como residente de boa fé e está legalmente autorizado para trabalhar nesse país.

b) Uma firma é considerada nacional de um país membro se satisfaz os dois seguintes requisitos:

- i. está legalmente constituída ou estabelecida conforme as leis de um país membro do Banco; e
- ii. mais de cinquenta por cento (50%) do capital da firma é de propriedade de indivíduos ou firmas de países membros do Banco.

Todos os membros de um consórcio e todos os subempreiteiros devem cumprir os requisitos acima estabelecidos.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

B) Origem dos Bens

Os bens têm origem em um país membro do Banco se foram extraídos, desenvolvidos, cultivados, colhidos ou produzidos em um país membro do Banco. Considera-se que um bem é produzido quando, mediante manufatura, processamento ou montagem, o resultado é um artigo comercialmente reconhecido cujas características, funções ou utilidades básicas são substancialmente diferentes de suas partes ou componentes.

No caso de um bem que consiste de vários componentes individuais que devem ser interconectados (pelo fornecedor, comprador ou um terceiro) para que o bem possa ser utilizado, e sem importar a complexidade da interconexão, o Banco considera que este bem é elegível para financiamento se a montagem dos componentes for feita em um país membro, independente da origem dos componentes. Quando o bem é uma combinação de vários bens individuais que normalmente são empacotados e vendidos comercialmente como uma só unidade, o bem é considerado proveniente do país onde este foi empacotado e embarcado com destino ao comprador.

Para fins de determinação da origem dos bens identificados como "feito na União Européia", estes serão elegíveis sem necessidade de identificar o correspondente país específico da União Européia.

A origem dos materiais, partes ou componentes dos bens ou a nacionalidade da empresa produtora, montadora, distribuidora ou vendedora dos bens não determina a origem dos mesmos.

C) Origem dos Serviços

O país de origem dos serviços é o mesmo do indivíduo ou empresa que presta os serviços conforme os critérios de nacionalidade acima estabelecidos. Este critério é aplicado aos serviços conexos ao fornecimento de bens (tais como transporte, seguro, instalação, montagem, etc.), aos serviços de construção e aos serviços de consultoria.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Anexo 4 Política do Banco sobre Práticas Proibidas

Práticas Proibidas

1.1 O Banco requer que todos os Mutuários (incluindo beneficiários de doações), Agências Executoras ou Agências Contratantes, bem como todas as empresas, entidades ou pessoas físicas que estejam apresentando propostas ou participando de atividades financiadas pelo Banco, incluindo, inter alia, solicitantes, concorrentes, fornecedores de bens, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias (incluindo seus respectivos funcionários, empregados e agentes, quer com atribuições expressas ou implícitas), observem os mais altos padrões éticos, e denunciem ao Banco todos os atos suspeitos de constituir uma Prática Proibida da qual tenha conhecimento ou seja informado, durante o processo de seleção e negociação ou na execução de um contrato. As Práticas Proibidas compreendem atos de: (a) práticas corruptas; (b) práticas fraudulentas; (c) práticas coercitivas; (d) práticas colusivas e (e) práticas obstrutivas. O Banco estabeleceu mecanismos para denúncia de suspeitas de Práticas Proibidas. Qualquer denúncia deverá ser apresentada ao Escritório de Integridade Institucional (EII) do Banco para que se realize a devida investigação. O Banco também estabeleceu procedimentos de sanção para a resolução de casos. Além disso, o Banco celebrou acordos com outras instituições financeiras internacionais (IFI) visando ao reconhecimento recíproco às sanções aplicadas pelos respectivos órgãos de sanção.

(a) Para fins de cumprimento dessa política, o Banco define os termos indicados a seguir:

(i) uma prática corrupta consiste em oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer coisa de valor para influenciar as ações de outra parte;

(ii) uma prática fraudulenta é qualquer ato ou omissão, incluindo uma declaração falsa que engane ou tente enganar uma parte para obter benefício financeiro ou de outra natureza ou para evitar uma obrigação;

(iii) uma prática coercitiva consiste em prejudicar ou causar dano ou na ameaça de prejudicar ou de causar dano, direta ou indiretamente, a qualquer parte ou propriedade da parte para influenciar indevidamente as ações de uma parte;

(iv) uma prática colusiva é um acordo entre duas ou mais partes efetuado com o intuito de alcançar um propósito impróprio, incluindo influenciar impropriamente as ações de outra parte; e

(v) uma prática obstrutiva consiste em:

(aa) destruir, falsificar, alterar ou ocultar deliberadamente uma evidência significativa para a investigação ou prestar declarações falsas aos investigadores com o fim de obstruir materialmente uma investigação do Grupo do Banco sobre denúncias de uma prática corrupta, fraudulenta, coercitiva ou colusiva; e/ou ameaçar, assediar ou intimidar qualquer parte para impedir a divulgação de seu conhecimento de assuntos que são importantes para a investigação ou a continuação da investigação,

(bb) ameaçar, assediar ou intimidar qualquer parte para impedir a divulgação de seu conhecimento de assuntos que são importantes para a investigação do Grupo BID ou a continuação da investigação; ou

(cc) todo ato que vise a impedir materialmente o exercício de inspeção do Grupo BID e dos direitos de auditoria previstos no parágrafo 1.1(f) a seguir; e

(vi) A "apropriação indevida" consiste no uso de fundos ou recursos do Grupo BID para um propósito indevido ou para um propósito não autorizado, cometido de forma intencional ou por negligência grave.



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

(b) Se, em conformidade com os procedimentos de sanções do Banco, for determinado que em qualquer estágio da aquisição ou da execução de um contrato qualquer empresa, entidade ou pessoa física atuando como licitante ou participando de uma atividade financiada pelo Banco, incluindo, entre outros, solicitantes, licitantes, fornecedores, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionárias, Mutuários (incluindo os Beneficiários de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos funcionários, empregados e agentes, quer sejam suas atribuições expressas ou implícitas), estiver envolvida em uma Prática Proibida em qualquer etapa da adjudicação ou execução de um contrato, o Banco poderá:

(i) não financiar nenhuma proposta de adjudicação de um contrato para obras, bens e serviços relacionados financiados pelo Banco;

(ii) suspender os desembolsos da operação se for determinado, em qualquer etapa, que um empregado, agente ou representante do Mutuário, do Órgão Executor ou da Agência Contratante estiver envolvido em uma Prática Proibida;

(iii) declarar uma aquisição viciada e cancelar e/ou declarar vencido antecipadamente o pagamento de parte de um empréstimo ou doação relacionada inequivocamente com um contrato, se houver evidências de que o representante do Mutuário ou Beneficiário de uma doação não tomou as medidas corretivas adequadas (incluindo, entre outras medidas, a notificação adequada ao Banco após tomar conhecimento da Prática Proibida) dentro de um período que o Banco considere razoável;

(iv) emitir advertência à empresa, entidade ou pessoa física com uma carta formal censurando sua conduta;

(v) declarar que uma empresa, entidade ou pessoa física é inelegível, permanentemente ou por um período determinado, para: (i) adjudicação de contratos ou participação em atividades financiadas pelo Banco; e (ii) designação como subconsultor, subempreiteiro ou fornecedor de bens ou serviços por outra empresa elegível a qual tenha sido adjudicado um contrato para executar atividades financiadas pelo Banco;

(vi) encaminhar o assunto às autoridades competentes encarregadas de fazer cumprir a lei; e/ou;

(vii) impor outras sanções que julgar apropriadas às circunstâncias do caso, inclusive multas que representem para o Banco um reembolso dos custos referentes às investigações e ao processo. Essas sanções podem ser impostas adicionalmente ou em substituição às sanções acima referidas.

(c) O disposto nos parágrafos 1.1 (b) (i) e (ii) se aplicará também nos casos em que as partes tenham sido temporariamente declaradas inelegíveis para a adjudicação de novos contratos, na pendência da adoção de uma decisão definitiva em um processo de sanção ou qualquer outra resolução.

(d) A imposição de qualquer medida que seja tomada pelo Banco conforme as disposições anteriormente referidas será de caráter público.

(e) Além disso, qualquer empresa, entidade ou pessoa física atuando como licitante ou participando de uma atividade financiada pelo Banco, incluindo, entre outros, solicitantes, licitantes, fornecedores de bens, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços, concessionárias, Mutuários (incluindo os Beneficiários de doações), Agências Executoras ou Agências Contratantes (incluindo seus respectivos funcionários, empregados e representantes, quer suas atribuições sejam expressas ou implícitas), poderá ser sujeita a sanções, em conformidade com o disposto nos acordos que o Banco tenha celebrado com outra instituição financeira internacional com respeito ao reconhecimento recíproco de decisões de inelegibilidade. Para fins do disposto neste parágrafo, o termo "sanção" refere-se a toda inelegibilidade permanente, imposição de condições para a participação em futuros contratos ou adoção pública de medidas em resposta a uma contravenção às regras vigentes de uma IFI aplicável à resolução de denúncias de Práticas Proibidas;

(f) O Banco exige que os solicitantes, concorrentes, fornecedores e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, prestadores de serviços e concessionárias permitam que o Banco revise quaisquer



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

contas, registros e outros documentos relativos à apresentação de propostas e a execução do contrato e os submeta a uma auditoria por auditores designados pelo Banco. Solicitantes, concorrentes, fornecedores de bens e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias deverão prestar plena assistência ao Banco em sua investigação. O Banco requer ainda que todos os solicitantes, concorrentes, fornecedores de bens e seus agentes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias: (i) mantenham todos os documentos e registros referentes às atividades financiadas pelo Banco por um período de sete (7) anos após a conclusão do trabalho contemplado no respectivo contrato; e (ii) forneçam qualquer documento necessário à investigação de denúncias de Práticas Proibidas e assegurem-se de que os empregados ou representantes dos solicitantes, concorrentes, fornecedores de bens e seus representantes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias que tenham conhecimento das atividades financiadas pelo Banco estejam disponíveis para responder às consultas relacionadas com a investigação provenientes de pessoal do Banco ou de qualquer investigador, agente, auditor ou consultor devidamente designado. Caso o solicitante, concorrente, fornecedor e seu agente, empreiteiro, consultor, pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionária se negue a cooperar ou descumpra o exigido pelo Banco, ou de qualquer outra forma crie obstáculos à investigação por parte do Banco, o Banco, a seu critério, poderá tomar medidas apropriadas contra o solicitante, concorrente, fornecedor e seu agente, empreiteiro, consultor, pessoal, subempreiteiro, subconsultor, prestador de serviços ou concessionária.

(g) Se um Mutuário fizer aquisições de bens, obras, serviços que forem ou não de consultoria diretamente de uma agência especializada, todas as disposições da Seção 8 relativas às sanções e Práticas Proibidas serão aplicadas integralmente aos solicitantes, concorrentes, fornecedores e seus representantes, empreiteiros, consultores, pessoal, subempreiteiros, subconsultores, prestadores de serviços e concessionárias (incluindo seus respectivos funcionários, empregados e representantes, quer suas atribuições sejam expressas ou implícitas), ou qualquer outra entidade que tenha firmado contratos com essa agência especializada para fornecer tais bens, obras, serviços que forem ou não de consultoria, em conformidade com as atividades financiadas pelo Banco. O Banco se reserva o direito de obrigar o Mutuário a lançar mão de recursos tais como a suspensão ou a rescisão. As agências especializadas deverão consultar a lista de empresas ou pessoas físicas declaradas temporária ou permanentemente inelegíveis pelo Banco. Caso alguma agência especializada celebre um contrato ou uma ordem de compra com uma empresa ou uma pessoa física declarada temporária ou permanentemente inelegível pelo Banco, o Banco não financiará os gastos correlatos e poderá tomar as demais medidas que considere convenientes.

1.2 Os Concorrentes ao apresentar uma proposta declaram e garantem que:

(i) leram e entenderam a proibição sobre atos de fraude e corrupção disposta pelo Banco e se obrigam a observar as normas pertinentes;

(ii) não incorreram em nenhuma Prática Proibida descrita neste documento;

(iii) não adulteraram nem ocultaram nenhum fato substancial durante os processos de seleção, negociação e execução do contrato;

(iv) nem eles nem os seus agentes, pessoal, subempreiteiros, subconsultores ou quaisquer de seus diretores, funcionários ou acionistas principais foram declarados inelegíveis pelo Banco ou outra Instituição Financeira Internacional (IFI) e sujeito às disposições dos acordos celebrados pelo Banco relativos ao reconhecimento mútuo de sanções à adjudicação de contratos financiados pelo Banco, nem foram declarados culpados de delitos vinculados a práticas proibidas;

(v) nenhum de seus diretores, funcionários ou acionistas principais tenha sido diretor, funcionário ou acionista principal de qualquer outra empresa ou entidade que tenha sido declarada inelegível pelo Banco ou outra Instituição Financeira Internacional (IFI) e sujeito às disposições dos acordos celebrados pelo Banco relativos ao reconhecimento mútuo de sanções à adjudicação de contratos financiados pelo Banco ou tenha sido declarado culpado de um delito envolvendo Práticas Proibidas;



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

(vi) declararam todas as comissões, honorários de representantes ou pagamentos para participar de atividades financiadas pelo Banco; e

(vii) reconhecem que o descumprimento de qualquer destas garantias constitui fundamento para a imposição pelo Banco de uma ou mais medidas descritas na Cláusula 1.1 (b).



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

Anexo 5 - Matriz de Risco

FASE 6 - PLANO DE TRATAMENTO DE RISCOS DE CADA CONTRATAÇÃO						
Nº DO RISCO	CONTROLES A SEREM IMPLANTADOS OU APERFEIÇOADOS	POR QUE SERÁ FEITO	COMO SERÁ REALIZADO	QUEM SERÁ O RESPONSÁVEL	ONDE SERÁ REALIZADO	QUANDO SERÁ REALIZADO
1	Cláusulas de Estabilidade de Preços	Para reduzir o impacto de reajustes não planejados e garantir previsibilidade de custos	Negociar cláusulas contratuais que limitem aumentos de preços, estabelecendo uma margem fixa ou indexada para ajustes com a inflação.	SGF/DTI	SEFAZ	Atividade contínua
1	Reserva Orçamentária	Para cobrir variações de custos e evitar interrupções no serviço por falta de orçamento	Criar e monitorar uma reserva orçamentária semestral, dedicada a cobrir aumentos de custos ao longo do contrato.	SGF/DTI/GSINF	SEFAZ	Durante a implantação
1	Análise de Custos Alternativos	Para avaliar opções economicamente viáveis caso ocorram aumentos inesperados	Revisar anualmente opções de renegociação de pacotes com fornecedores, incluindo novos acordos de preços fixos.	SGF/DTI/GSINF	SEFAZ	Durante a vigência do contrato
2	Plano de Capacitação Contínua	Para assegurar a familiaridade e eficácia da equipe no uso dos novos processos e ferramentas de segurança da informação	Realizar treinamentos práticos e teóricos periódicos sobre o processos, melhores práticas e ferramentas de segurança da informação.	SGF/DTI/GSINF	SEFAZ	Atividade contínua
2	Programa de Adaptação Gradual	Para minimizar a resistência à mudança e permitir uma transição tranquila para os novos processos e ferramentas de segurança da informação	Implementar os novos processos e ferramentas em fases, permitindo uma transição suave e acompanhando a adaptação da equipe em cada etapa.	SGF/DTI/GSINF	SEFAZ	Durante a implantação
2	Comunicação e Engajamento	Para conscientizar e engajar a equipe sobre os	Organizar workshops e manter canais de comunicação	SGF/DTI/GSINF	SEFAZ	Durante a vigência do contrato



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

FASE 6 - PLANO DE TRATAMENTO DE RISCOS DE CADA CONTRATAÇÃO						
Nº DO RISCO	CONTROLES A SEREM IMPLANTADOS OU APERFEIÇOADOS	POR QUE SERÁ FEITO	COMO SERÁ REALIZADO	QUEM SERÁ O RESPONSÁVEL	ONDE SERÁ REALIZADO	QUANDO SERÁ REALIZADO
		benefícios e uso dos novos processos e ferramentas de segurança da informação	abertos para responder dúvidas e comunicar as vantagens dos novos processos e ferramentas.			
3	Acordos de Nível de Serviço (SLAs)	Para garantir que o fornecedor ofereça tempos de resposta rápidos e qualidade no serviço	Estabelecer SLAs detalhados que definam tempos máximos de resposta e recuperação, com cláusulas de penalidade por descumprimento.	SGF/DTI/GSINF	SEFAZ	Durante a vigência do contrato
3	Plano de Contingência	Para reduzir o impacto de interrupções no serviço e garantir continuidade das operações de segurança da informação	Desenvolver um plano de contingência que inclua redundância e alternativas temporárias durante falhas do fornecedor do Centro de Operações de Segurança (SOC) ou das ferramentas de TI	SGF/DTI/GSINF	SEFAZ	Atividade contínua
3	Monitoramento Contínuo	Para identificar e corrigir interrupções de forma proativa e minimizar impactos nos usuários	Adotar ferramentas de monitoramento que alertem em tempo real sobre falhas, permitindo ações preventivas imediatas.	SGF/DTI/GSINF	SEFAZ	Atividade contínua
4	Políticas de Segurança e Auditoria	Para proteger dados sensíveis e garantir conformidade com a LGPD	Estabelecer auditorias de segurança regulares e implementar autenticação multifatorial e controle rigoroso de acessos.	SGF/DTI/GSINF	SEFAZ	Atividade contínua
4	Treinamento em Cibersegurança	Para conscientizar a equipe sobre práticas de segurança e	Realizar treinamentos frequentes sobre boas práticas de segurança e	SGF/DTI/GSINF	SEFAZ	Atividade contínua



ESTADO DA BAHIA
SECRETARIA DA FAZENDA

FASE 6 - PLANO DE TRATAMENTO DE RISCOS DE CADA CONTRATAÇÃO						
Nº DO RISCO	CONTROLES A SEREM IMPLANTADOS OU APERFEIÇOADOS	POR QUE SERÁ FEITO	COMO SERÁ REALIZADO	QUEM SERÁ O RESPONSÁVEL	ONDE SERÁ REALIZADO	QUANDO SERÁ REALIZADO
		reduzir o risco de ataques cibernéticos	proteção de dados sensíveis para toda a equipe de TI.			
4	Ferramentas de Monitoramento e Testes de Vulnerabilidade	Para prevenir vazamento de dados e fortalecer a segurança da solução SaaS	Implementar monitoramento de atividades suspeitas e realizar testes de vulnerabilidade periódicos para identificar e mitigar riscos.	SGF/DTI/GSINF	SEFAZ	Atividade contínua
5	Plano de Capacitação Contínua	Para assegurar a familiaridade e eficácia da equipe no uso dos novos processos e ferramentas de segurança da informação	Realizar treinamentos práticos e teóricos periódicos sobre o processos, melhores práticas e ferramentas de segurança da informação.	SGF/DTI/GSINF	SEFAZ	Atividade contínua
5	Programa de Adaptação Gradual	Para minimizar a resistência à mudança e permitir uma transição tranquila para os novos processos e ferramentas de segurança da informação	Implementar os novos processos e ferramentas em fases, permitindo uma transição suave e acompanhando a adaptação da equipe em cada etapa.	SGF/DTI/GSINF	SEFAZ	Durante a implantação
5	Comunicação e Engajamento	Para conscientizar e engajar a equipe sobre os benefícios e uso dos novos processos e ferramentas de segurança da informação	Organizar workshops e manter canais de comunicação abertos para responder dúvidas e comunicar as vantagens dos novos processos e ferramentas.	SGF/DTI/GSINF	SEFAZ	Durante a vigência do contrato