

TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO Nº /2026-DIAD

Processo Administrativo nº /2026

1 – OBJETO

Registro de preço para futura contratação de solução de detecção e resposta a incidentes, auditoria e proteção de dados, detecção e resposta a ameaças baseadas em dados, coleta de fluxos de metadados, e análise constante de dados e de seus repositórios de dados corporativos, plataforma de compartilhamento colaborativo, incluindo prestação de serviço de instalação e configuração, com garantia técnica de 12 (doze meses) meses, com treinamento para capacitação de técnicos da Companhia de Saneamento de Sergipe e serviço de operação assistida e apoio operacional.

Trata-se de demanda de contratação que tem por objeto a modernização da segurança cibernética da Companhia de Saneamento de Sergipe, cuja solução deve ser baseada em software de auditoria de dados, monitoramento, automação e controle em ambiente on-premise Microsoft e ambiente de colaboração em nuvem Google Drive, devendo compreender o serviço de instalação/configuração, transferência de conhecimento na forma de treinamento oficial, garantia da solução pelo tempo da contratação com atualização/suporte técnico e serviço de técnico operacional na modalidade de operação assistida. O objeto da contratação visa apoiar as equipes de segurança nas atividades de investigação e análise de alertas dos comportamentos suspeitos na Rede interna e ambiente de colaboração em nuvem.

2 – JUSTIFICATIVA

2.1 – DO OBJETO

O cenário de TI configura atualmente um processo acelerado de transformação digital, no qual as soluções tecnológicas que possibilitam o tratamento de dados se tornam

imprescindíveis para uma prestação jurisdicional mais efetiva. A efetividade do referido processo só ocorrerá com a devida e correspondente proteção de dados, informações e usuários.

Neste cenário, eventos recentes de ataques cibernéticos a alguns órgãos do poder público descortinam um horizonte de ameaças que põe em risco o aludido planejamento, cujos incidentes demonstram o poder desses atacantes e a necessidade cada vez maior de implementar ações preventivas, detectivas e corretivas, de forma estruturada, objetivando antecipar incidentes e mitigar os impactos de ataques cibernéticos.

Nestes termos, a atenção relativa à segurança deve ser dispensada não somente aos sistemas informatizados, mas também aos ativos que recebem, processam, armazenam, publicam e descartam informações. Na sociedade da informação vivida nos tempos atuais, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão estas sob constantes ameaças e necessitam ser adequadamente protegidas. Com isso, a Segurança da Informação tornou-se essencial ao funcionamento de empresas privadas e órgãos públicos, visando a continuidade da entrega de serviços, sobrevivência e credibilidade das instituições.

Por este motivo, além do risco de perda e vazamento de dados sensíveis durante ataques cibernéticos, existe a preocupação de que a sociedade perca a confiança nos serviços disponibilizados, entre outras inúmeras consequências à imagem da instituição. Para que seja alcançado o nível de segurança exigido atualmente, é necessário investir em processos, sistemas e conhecimento específicos contra ameaças avançadas.

Neste contexto, a Gerência de Tecnologia da Informação da DESO, entende ser necessária a contratação de serviços e soluções de tecnológicas de segurança da informação cuja eficiência na mitigação de ataques cibernéticos seja comprovada e que permitam o provimento eficiente da integração entre todos os recursos necessários à auditoria e mitigação dos riscos sistêmicos de segurança cibernética, contando com atividades contínuas e especializadas em alerta, tratamento e mitigação de eventos e incidentes de segurança.

A pretensa contratação tem como objetivo principal, transformar de forma positiva a maneira como a prevenção de ataques cibernéticos é gerenciada pelas unidades de defesa cibernética da GTIC, garantindo a complementação efetiva dos controles já utilizados, visando prover soluções de inspeção e proteção contra ameaçadas avançadas nos servidores

de Diretórios (AD), dispositivos de armazenamento local e em nuvem, bem como aprimorar a proteção e resiliência dos serviços tecnológicos ofertados pelo DESO.

A Ata de Registro de Preços decorrente deste certame poderá ser utilizada por órgãos ou entidades da Administração Pública que não participaram do procedimento inicial, mediante anuência da DESO, na condição de órgão gerenciador, e desde que devidamente justificada a vantagem da adesão. O limite para adesões por órgãos não participantes ("caronas") deverá observar o disposto no Regulamento Interno de Licitações e Contratos (RILC) da DESO, limitando-se o quantitativo total das adesões ao dobro do quantitativo de cada item registrado na ata para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos que aderirem. Tal previsão visa conferir maior celeridade e eficiência à Administração Pública, aproveitando as condições obtidas pela DESO neste processo licitatório, sempre em estrita observância à Lei nº 13.303/2016.

2.2. DA MODALIDADE

Considerando as transformações iminentes na empresa após o leilão de parte de suas operações, o número de usuários pode sofrer alterações que, no presente momento, são imprevisíveis. Diante dessa incerteza, optamos pela realização de um registro de preços com uma margem de 25% sobre o número máximo de usuários ativos atuais. Essa abordagem permitirá ajustar a contratação conforme a real necessidade futura, garantindo maior flexibilidade e eficiência no processo de aquisição, sem comprometer a adequação aos novos cenários que possam surgir.

2.3. DA METODOLOGIA DO PREÇO MÁXIMO

A metodologia utilizada para definição do preço máximo de referência foi o preço médio da pesquisa de mercado.

2.4. DO QUANTITATIVO

Foi levado em consideração a quantidade de contas ativas do Microsoft Active Directory para cada usuário da rede de computadores da DESO, bem como o número de contas da DESO no Google Workspace.

3 – QUANTIDADE E DESCRIÇÃO DOS SERVIÇOS

3.1 – LOTE ÚNICO

ITEM	DESCRIPTIVO	Unidade	Quantidade
1	Licença de uso de software de auditoria e controle de ameaças sobre dados não estruturados on-premise, com treinamento, instalação e suporte por 12 meses	usuários	1.000
2	Licença de uso de software de auditoria e controle de ameaças sobre dados não estruturados armazenados em serviço de nuvem, com treinamento, instalação e suporte por 12 meses.	usuários	1.000

4 – ESTIMATIVA DO VALOR DO OBJETO DA CONTRATAÇÃO

Na orçamentação do objeto foram realizadas consultas no mercado para compor os preços e buscar atender ao previsto no RILC da Companhia de Saneamento de Sergipe – DESO a partir de pesquisa junto as empresas representantes das soluções disponíveis no mercado.

5 – DA QUALIFICAÇÃO TÉCNICA

5.1 – A solução a ser CONTRATADA deve ainda atender a conformidade de normas ISO relacionadas à segurança da informação, e devem ser demonstradas juntamente a apresentação da proposta comercial, são elas:

5.1.1 – Por se tratar de software de proteção de dados sensíveis com análise comportamental de usuários para ambiente de nuvem, o fabricante ou a solução deverá ser certificada ISO/IEC 27017, que traça diretrizes para controles de segurança de serviços em nuvem.

5.1.2 – Por se tratar de software de proteção de dados sensíveis o fabricante ou a solução deverá ser certificada ISO/IEC 27018, que traça diretrizes para proteção de dados pessoais.

5.1.3 – Por se tratar de software de proteção de dados sensíveis o fabricante ou a solução

deverá ser certificada ISO/IEC 27701, que traça diretrizes para o gerenciamento da privacidade da informação dentro da organização.

5.1.4 – O fabricante deverá possuir certificação SOC 2 e SOC 3, para garantir segurança, confidencialidade, disponibilidade, privacidade e integridade das informações.

5.2 – A LICITANTE deverá apresentar pelo menos 01 (um) Atestado de Capacidade Técnica comprovando que executou, sem restrição, ao menos uma implantação da solução ofertada abrangendo no mínimo 50% do total das quantidades da tabela no item 3.1.

5.2.1 – Não serão aceitos atestados emitidos por empresas do mesmo grupo empresarial da proponente, nem pela própria;

5.2.2 – São consideradas como pertencentes ao mesmo grupo empresarial da proponente empresas por ela controladas ou empresas controladoras da proponente, ou empresas que tenham, no mínimo, uma mesma pessoa física ou jurídica que seja sócio da empresa emitente do atestado e da proponente;

5.3 – A CONTRATANTE se reserva o direito de conferir as informações prestadas pelas empresas emitentes dos atestados, através de consultas e visitas.

6 – ESPECIFICAÇÕES TÉCNICAS

6.1 – Considerações Gerais

6.1.1 – Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução de auditoria deverá ser de um único fabricante;

6.1.2 – A solução deve disponibilizar console web ou cliente que poderá ser acessada através do servidor de aplicação e estações de trabalho dos usuários com acesso autorizado;

6.1.3 – A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention) e SIEM.

6.1.4 – Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo não deve impactar na disponibilidade dos servidores ou serviços;

- 6.1.5 – O agente deve possuir um mecanismo de monitoramento de desempenho dos servidores onde atua, de modo a não permitir que o nível de consumo de recursos ultrapasse limites definidos e configuráveis;
 - 6.1.6 – A solução deve oferecer a possibilidade de configurações de diferentes níveis de segurança às suas funcionalidades, podendo, desta forma, ser utilizada por diferentes equipes com variadas demandas de atividades e com acesso restrito a diferentes funções;
 - 6.1.7 – Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia forense inclusive como provas judiciais, a solução deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares;
 - 6.1.8 – A solução deve suportar a utilização de servidores virtualizados para os componentes;
 - 6.1.9 – A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;
 - 6.1.10 – A solução deverá fazer recomendações de melhores práticas a serem aplicadas no ambiente;
 - 6.1.11 – A solução deverá ser entregue como serviço na nuvem, sendo toda infraestrutura disponibilizada pelo fabricante. Caso a solução necessite de uma probe/coletor de dados no ambiente local, deve ser compatível com o ambiente virtualizado do órgão;
 - 6.1.12 – Toda a infraestrutura da nuvem deve ser gerenciada pelo fabricante, incluindo, mas não se limitando a: Manutenção do ambiente, atualizações aplicadas de forma transparente, pacotes de correções e novas features aplicadas direto no produto e sem nenhum tipo de impacto;
 - 6.1.13 – O fabricante deverá disponibilizar um time de resposta a incidentes para auxiliar em caso de investigação de algum incidente ou alguma suspeita de um alerta crítico que possa ter sido gerado no ambiente;
- 6.2 – Estrutura LOCAL (on-premise)**
- 6.2.1 – A solução deverá monitorar múltiplos domínios do Active Directory e servidores de arquivos Windows e NAS (Network Attached Storage) e Linux do ambiente,

incluindo: Contas, estruturas de diretórios, permissões e eventos;

- 6.2.2 – A solução deverá suportar no mínimo, para servidores de arquivos, Windows server 2012 ou superior e Linux para no mínimo as seguintes distribuições: Red Hat Enterprise Linux em todas as suas versões ativas, SUSE Linux Enterprise Server Versão 15 SP2 LTSS e 15 SP3.
- 6.2.3 – A solução deve permitir uma pré-visualização das alterações de permissionamento pretendidas de maneira gráfica antes da aplicação em produção. Esta pré-visualização deve demonstrar os impactos nos grupos e usuários em relação a suas permissões nos diretórios monitorados;
- 6.2.4 – A solução deve fornecer a visibilidade sobre aplicações de alteração que estão pendentes e o histórico das alterações aplicadas através da console;
- 6.2.5 – Caso a solução necessite da instalação de agente para o monitoramento dos eventos do Active Directory e servidores de arquivos, os agentes não devem gerar nenhuma queda de performance nos servidores;
- 6.2.6 – O gerenciamento da solução deverá ser centralizado para todos os módulos;
- 6.2.7 – A solução deverá monitorar todos os domain controllers instalados em qualquer versão do Windows Server 2003 ou superior;
- 6.2.8 – A solução deverá monitorar todos os servidores de arquivos instalados em Windows Server 2012 ou superior;
- 6.2.9 – A solução deverá monitorar no mínimo, os seguintes eventos do Microsoft Active Directory:
 - 6.2.9.1 – Conta habilitada e desabilitada ;
 - 6.2.9.2 – Autenticação de conta (TGT) ;
 - 6.2.9.3 – Renovação de acesso (TGS) ;
 - 6.2.9.4 – Replicação de AD ;
 - 6.2.9.5 – Logon de conta no DC;
 - 6.2.9.6 – Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS;
 - 6.2.9.7 – Requisição de acesso NTLM;
 - 6.2.9.8 – Alteração de senha de usuário;
 - 6.2.9.9 – Conta de usuário bloqueada;
 - 6.2.9.10 – Conta de usuário desbloqueada;
 - 6.2.9.11 – Netlogon vulnerável;
 - 6.2.9.12 – Criação, deleção e modificação de GPO;

- 6.2.9.13 – Tentativa de reset de senha;
- 6.2.9.14 – Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC;
- 6.2.9.15 – Alteração de política de kerberos.
- 6.2.10 – A solução deverá monitorar no mínimo, os seguintes eventos do servidor de Arquivos Windows:
 - 6.2.10.1 – Arquivo criado;
 - 6.2.10.2 – Arquivo deletado;
 - 6.2.10.3 – Arquivo aberto;
 - 6.2.10.4 – Arquivo renomeado;
 - 6.2.10.5 – Arquivo modificado;
 - 6.2.10.6 – Mudança de proprietário do arquivo;
 - 6.2.10.7 – Permissões adicionadas no arquivo;
 - 6.2.10.8 – Permissões removidas no arquivo;
 - 6.2.10.9 – Proteção adicionado no arquivo;
 - 6.2.10.10 – Proteção removida no arquivo;
 - 6.2.10.11 – Pasta criada;
 - 6.2.10.12 – Pasta deletada;
 - 6.2.10.13 – Pasta renomeada;
 - 6.2.10.14 – Mudança de proprietário da pasta;
 - 6.2.10.15 – Permissões adicionadas na pasta;
 - 6.2.10.16 – Permissões removidas na pasta;
 - 6.2.10.17 – Proteção adicionada na pasta;
 - 6.2.10.18 – Proteção removida na pasta;
- 6.2.11 – Deverá ser possível definir os proprietários das pastas através da console;
- 6.2.12 – A solução deverá exibir uma lista com todas as contas de usuários monitoradas, indicando no mínimo, o tipo de conta (serviço, executiva ou administrativa) e grupos que fazem parte;
- 6.2.13 – A solução deverá exibir o repositório monitorado em formato hierarquico, expandindo as pastas e sub-pastas até o nível do arquivo, permitindo a visualização de quais usuários tem acesso a cada recurso e as permissões concedidas;
- 6.2.14 – A solução deverá possuir uma visão bi-direcional indicando através de uma visualização gráfica e interativa, todas as permissões dos usuários e grupos, e

quais as permissões aplicadas nos objetos (arquivos e pastas);

- 6.2.15 – A solução deverá disponibilizar a visibilidade de permissões, sejam elas NTFS ou share;
- 6.2.16 – A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;
- 6.2.17 – A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e expressão regular;
- 6.2.18 – A solução deverá indicar para qualquer arquivo e pasta no servidor monitorado, uma visualização gráfica contendo o nível de exposição e indicando se o arquivo é sensível ou não a partir da classificação realizada;
- 6.2.19 – A solução deverá fornecer filtros para visualizar apenas determinados objetos de dados em exibição gráfica interativa, incluindo pastas protegidas e pastas únicas;
- 6.2.20 – A solução deverá incluir informações de classificação de dados na tela das permissões, incluindo: nome da regra classificada, e quantidade de instâncias sensíveis encontradas no arquivo;
- 6.2.21 – A solução deverá fornecer para as permissões, tipos de exibição diferentes, incluindo exibições hierárquicas e de lista;
- 6.2.22 – A solução deverá realizar a classificação de imagens através de OCR ou tecnologia similar;
- 6.2.23 – A solução deverá possibilitar a criação de regras customizadas para que os administradores possam definir o que deve ser encontrado dentro do conteúdo do arquivo, de acordo com a necessidade organizacional;
- 6.2.24 – Deve ser possível exportar eventos e informações apenas referente aos dados classificados como sensíveis;
- 6.2.25 – Deve ser possível definir o escopo do ambiente que vai ser classificado, podendo definir: repositório, arquivo, pasta, tipo de arquivo, quantidade mínima de hits e outros;
- 6.2.26 – A solução deverá permitir a análise dos arquivos classificados, indicando dentro do conteúdo do arquivo exatamente o que foi encontrado de dado sensível e confidencial;
- 6.2.27 – A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF, RG, CNH e outros) são armazenados, quem tem acesso aos

dados e quais são as atividades em cima destes dados;

- 6.2.28 – A solução deverá escanear e classificar no mínimo os seguintes tipos de arquivos: doc, docx, dwg, rtf, ppt, xls, txt, csv, pdf, xml, log, eml, jpg, jpeg, gif, png, rar e zip;
- 6.2.29 – A solução deverá encontrar em arquivos com formato tabular, palavras-chave em cabeçalhos e colunas;
- 6.2.30 – A solução deverá indicar no painel de diretórios: o nome da regra, a quantidade de hits do termo sensível encontrado nos arquivos e pastas e a quantidade de hits incluindo sub-pastas;
- 6.2.31 – A solução deverá notificar os administradores através de alertas para qualquer tipo de atividade incomum e comportamentos suspeitos de usuários;
- 6.2.32 – Os alertas da solução deverão ser encaminhados via SMTP e SNMP;
- 6.2.33 – A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;
- 6.2.34 – A solução deverá realizar a análise comportamental dos usuários de forma automática, através de machine learning, entendendo o comportamento e rotina de todos os usuários, o que acessam, quando acessam e onde;
- 6.2.35 – A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor com mais de 150 modelos de alertas pré-configurados de eventos suspeitos tais como:
 - 6.2.35.1 – Ataques de sequestro de dados (ransomware);
 - 6.2.35.2 – Detecção de ferramentas nocivas ao ambiente;
 - 6.2.35.3 – Ações com acessos negados;
 - 6.2.35.4 – Ações de escalações de privilégios;
 - 6.2.35.5 – Excesso de tentativas de autenticação ou contas bloqueadas;
 - 6.2.35.6 – Atividades suspeitas em dados parados e/ou inativos;
 - 6.2.35.7 – Alterações anormais em GPO;
 - 6.2.35.8 – Ataques de golden ticket;
 - 6.2.35.9 – Ataques de injeção de códigos maliciosos;
 - 6.2.35.10 – Ataques de decoberta de contas com NTLM e Kerberos;
 - 6.2.35.11 – Ataques de força bruta.
- 6.2.36 – Os modelos de alertas devem ser atualizados de forma automática;
- 6.2.37 – A solução deverá detectar ameaças em todos os estágios de um ataque

cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalção de privilégio, movimento lateral, negação de serviço e exfiltração de dados;

- 6.2.38 – A solução deverá monitorar a atividade do usuário para construir perfis de comportamento e usar os modelos de ameaça baseados em comportamento para alertar quando uma atividade anormal no Active Directory é detectada;
- 6.2.39 – A solução deverá construir perfis de comportamento comparando as atividades dos usuários e entidades e identificando a relação entre eles;
- 6.2.40 – A solução deverá possuir um período de aprendizado, para que seja feito a coleta de eventos e identificação do comportamento dos usuários para a criação do perfil comportamental;
- 6.2.41 – A solução deverá realizar a descoberta de contas privilegiadas de forma automática, identificando contas executivas, contas de serviço e contas administrativas baseado no seu comportamento e nos grupos de segurança que a conta está inserida;
- 6.2.42 – A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;
- 6.2.43 – A solução deverá possuir política de automação para remediação de exposição de dados para toda a organização, removendo as permissões globais das pastas e arquivos;
- 6.2.44 – A solução deverá possuir política de automação para remediar permissões inconsistentes, garantindo que não exista permissão quebrada e aplicando as entradas de permissão corretamente para as sub-pastas e arquivos;
- 6.2.45 – As políticas de automação para remediação devem ser executadas de forma manual e automática;
- 6.2.46 – A solução deverá suportar na busca dos eventos a utilização de operadores relativos, auxiliando na investigação e nos resultados esperados;
- 6.2.47 – Deve ser possível salvar uma pesquisa customizada, agendando para que ela possa ser executada de forma automática e que os administradores recebam as informações necessárias de forma periódica;
- 6.2.48 – A solução deverá suportar a criação e utilização de flags para serem aplicadas as contas de usuários e aos recursos monitorados, essas flags podem ser utilizadas nos filtros e na aba de eventos;
- 6.2.49 – A solução deverá identificar dados que não foram acessados por um período de

tempo, podendo especificar a quantidade de dias desejado;

- 6.2.50 – A solução deverá disponibilizar dashboard das informações correlacionadas dos dados do Active Directory, com painéis, indicando no mínimo: Usuários com senha que nunca expira, contas de usuários obsoletas, contas executivas, contas desabilitadas e contas habilitadas com a senha expirada;
- 6.2.51 – A solução deverá disponibilizar dashboard com painéis dos dados correlacionados dos servidores de arquivos Windows, indicando no mínimo: Arquivos sensíveis expostos para toda organização, pastas expostas, permissões obsoletas, permissões direta nas pastas, pastas com permissões inconsistentes e pastas com dados obsoletos;
- 6.2.52 – Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;
- 6.2.53 – Os widgets devem ser configuráveis e customizáveis, podendo alterar o modo de visualização, para alguns tipos, como: widgets de métrica única, widgets de porcentagem e widgets com linha do tempo;
- 6.2.54 – A solução deverá possuir Widget de geolocalização com mapa indicando a origem da ação para os alertas gerados;
- 6.2.55 – A solução deverá possuir uma tela de visualização de eventos, podendo realizar pesquisas e filtros à cerca de todas as atividades e dados do ambiente.
- 6.2.56 – Todos os eventos podem ser filtrados e organizados no mínimo por: tipo de evento, ID do evento, operação, status e plataforma;
- 6.2.57 – Deve ser possível definir uma data e horário para busca dos eventos;
- 6.2.58 – A solução deverá possuir filtro para última atividade registrada do usuário, facilitando a busca de contas que estão atualmente inativas;
- 6.2.59 – A solução deverá fornecer relatório dos níveis de exposição das permissões, no contexto de dados sensíveis para qualquer pasta e arquivo;
- 6.2.60 – A solução deverá fornecer relatório das permissões, incluindo dados da classificação;
- 6.2.61 – A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;
- 6.2.62 – A solução deverá fornecer relatório dos resultados da classificação dos dados, incluindo o número de hit e regra classificada;
- 6.2.63 – A solução deverá fornecer relatório dos dados que estão com permissões de grupos globais e quem está utilizando estas permissões para acessar as

informações;

- 6.2.64 – A solução deverá fornecer relatório para SID não resolvido em ACLs;
- 6.2.65 – A solução deverá fornecer relatório sobre grupos de segurança não utilizados ou vazios;
- 6.2.66 – A solução deverá fornecer relatório para usuários desabilitados;
- 6.2.67 – Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV, Excel e PDF;
- 6.2.68 – Deverá ser possível realizar o agendamento de relatórios;
- 6.2.69 – Deverá ser possível encaminhar o relatório apenas para o proprietário do dado;

6.3 – Estrutura em NUVEM

- 6.3.1 – A solução deverá contemplar o monitoramento de repositórios em nuvem Google Workspace OU Microsoft Sharepoint Online e OneDrive, devendo a CONTRATANTE definir qual módulo irá adquirir no momento do pedido de entrega.
- 6.3.2 – Para ambientes Microsoft, a solução deverá suportar todas as funcionalidades descritas no item 2 para os repositórios de nuvem corporativa: Microsoft Sharepoint Online e OneDrive, correlacionando identidades com privilégios, atividades, reduzindo riscos e acelerando investigações;
- 6.3.3 – A solução deverá monitorar, no mínimo, os seguintes eventos do Entra ID:
 - 6.3.3.1 – Conta desativada;
 - 6.3.3.2 – Conta ativada;
 - 6.3.3.3 – Aplicativo adicionado;
 - 6.3.3.4 – Consentimento do aplicativo aprovado;
 - 6.3.3.5 – Consentimento do aplicativo removido;
 - 6.3.3.6 – Proprietário do aplicativo adicionado;
 - 6.3.3.7 – Proprietário do aplicativo removido;
 - 6.3.3.8 – Aplicativo removido;
 - 6.3.3.9 – Aplicativo atualizado;
 - 6.3.3.10 – Dispositivo adicionado;
 - 6.3.3.11 – Proprietário do dispositivo adicionado;
 - 6.3.3.12 – Proprietário do dispositivo removido;
 - 6.3.3.13 – Usuário registrado do dispositivo adicionado;
 - 6.3.3.14 – Usuário registrado do dispositivo removido;
 - 6.3.3.15 – Dispositivo removido;

- 6.3.3.16 – Dispositivo atualizado;
- 6.3.3.17 – Grupo adicionado;
- 6.3.3.18 – Grupo excluído;
- 6.3.3.19 – Conjunto de licenças de grupo;
- 6.3.3.20 – Membro do grupo adicionado;
- 6.3.3.21 – Membro do grupo removido;
- 6.3.3.22 – Proprietário do grupo adicionado;
- 6.3.3.23 – Proprietário do grupo removido;
- 6.3.3.24 – Grupo atualizado login;
- 6.3.3.25 – Função do membro adicionada;
- 6.3.3.26 – Função do membro removida;
- 6.3.3.27 – Usuário adicionado;
- 6.3.3.28 – Usuário excluído;
- 6.3.3.29 – Usuário convidado para a organização;
- 6.3.3.30 – Licença de usuário alterada;
- 6.3.3.31 – Usuário restaurado e Usuário atualizado;
- 6.3.4 – A solução deverá monitorar, no mínimo, os seguintes eventos do Sharepoint Online e OneDrive:
 - 6.3.4.1 – Malware detectado no arquivo;
 - 6.3.4.2 – Solicitação de acesso a arquivos aprovada;
 - 6.3.4.3 – Arquivo copiado;
 - 6.3.4.4 – Arquivo excluído;
 - 6.3.4.5 – Arquivo baixado para uma pasta local sincronizada;
 - 6.3.4.6 – Arquivo baixado;
 - 6.3.4.7 – Convite de arquivo aceito;
 - 6.3.4.8 – Convite de arquivo cancelado;
 - 6.3.4.9 – Convite de arquivo criado;
 - 6.3.4.10 – Convite de arquivo atualizado;
 - 6.3.4.11 – Arquivo modificado;
 - 6.3.4.12 – Arquivo movido;
 - 6.3.4.13 – Arquivo aberto;
 - 6.3.4.14 – Arquivo renomeado;
 - 6.3.4.15 – Arquivo restaurado;
 - 6.3.4.16 – Link compartilhado de arquivo criado;

- 6.3.4.17 – Link compartilhado do arquivo removido;
- 6.3.4.18 – Link compartilhado do arquivo atualizado;
- 6.3.4.19 – Link compartilhado do arquivo usado;
- 6.3.4.20 – Arquivo enviado;
- 6.3.4.21 – Arquivo enviado de uma pasta local sincronizada;
- 6.3.4.22 – Solicitação de acesso à pasta aprovada;
- 6.3.4.23 – Pasta copiada;
- 6.3.4.24 – Pasta criada;
- 6.3.4.25 – Pasta excluída;
- 6.3.4.26 – Convite de pasta aceito;
- 6.3.4.27 – Convite de pasta cancelado;
- 6.3.4.28 – Convite de pasta criado;
- 6.3.4.29 – Convite de pasta atualizado;
- 6.3.4.30 – Pasta movida;
- 6.3.4.31 – Pasta renomeada;
- 6.3.4.32 – Pasta restaurada;
- 6.3.4.33 – Link compartilhado da pasta criado;
- 6.3.4.34 – Link compartilhado da pasta removido;
- 6.3.4.35 – Link compartilhado da pasta atualizado;
- 6.3.4.36 – Link compartilhado da pasta usado;
- 6.3.4.37 – Grupo adicionado;
- 6.3.4.38 – Grupo excluído;
- 6.3.4.39 – Membro do grupo adicionado;
- 6.3.4.40 – Membro do grupo removido;
- 6.3.4.41 – Permissões adicionadas;
- 6.3.4.42 – Herança de permissão quebrada;
- 6.3.4.43 – Herança de permissão restaurada;
- 6.3.4.44 – Permissões removidas;
- 6.3.4.45 – Administrador do conjunto de sites adicionado;
- 6.3.4.46 – Administrador do conjunto de sites removido;
- 6.3.4.47 – Mudança geográfica do site agendada;
- 6.3.4.48 – Mudança geográfica do site concluída;
- 6.3.5 – A solução deverá possuir uma visão bidirecional das permissões dos repositórios de nuvem, podendo clicar em um recurso para ver quem tem acesso a ele ou

filtrar um usuário/grupo e validar todo o seu acesso de acordo com os repositórios monitorados;

- 6.3.6 – A solução deverá fornecer uma visão gráfica interativa dos níveis de exposição de permissões (interna, externa, convidado, em toda a organização, qualquer pessoa) no contexto com dados confidenciais para qualquer arquivo, pasta e site no SharePoint Online e OneDrive ou Google Workspace;
- 6.3.7 – A solução deverá monitorar e detectar quando um usuário realizar o login no M365 ou Google Workspace de um país novo ou país incomum;
- 6.3.8 – A solução deverá suportar a configuração de gatilhos pré-definidos para incidentes de segurança e alertas com base em políticas definidas para links de compartilhamento público e em toda a organização que expõe dados confidenciais;
- 6.3.9 – A solução deverá monitorar e normalizar a atividade do usuário, criando um perfil comportamental, baseado nas suas atividades, gerando alertas para acessos anormais à dados sensíveis e dados parados;
- 6.3.10 – A solução deverá monitorar a atividade do usuário para construir perfis de comportamento e usar os modelos de ameaça baseados em comportamento para alertar atividades em risco ou incomuns no M365 ou Google Workspace;
- 6.3.11 – A solução deverá fornecer alerta para links de compartilhamento público e em toda a organização que expõe dados sensíveis;
- 6.3.12 – A solução deverá fornecer alerta para atividades suspeita em pastas e arquivos;
- 6.3.13 – A solução deverá fornecer alerta para mudanças de membros em grupos privilegiados;
- 6.3.14 – A solução deverá detectar e alertar de forma automática, atividades que correspondem a possíveis ameaças cibernéticas e padrões de ataques comuns;
- 6.3.15 – A solução deverá fornecer alerta para acessos anormais a dados sensíveis baseado no comportamento do usuário;
- 6.3.16 – A solução deverá fornecer uma visão gráfica e interativa dos links de compartilhamento do Microsoft 365 ou Google Workspace em contexto com sensibilidade e desatualização;
- 6.3.17 – A solução deverá realizar a classificação dos arquivos hospedados nos repositórios de nuvem suportados;
- 6.3.18 – A solução deverá auxiliar na conformidade com a LGPD, identificando aonde os dados pessoais (CPF, RG, CNH e outros) são armazenados, quem tem acesso aos

dados e quais são as atividades em cima destes dados;

- 6.3.19 – A solução deverá permitir a configuração dos tipos de arquivos que serão escaneados e a definição do tamanho do arquivo;
- 6.3.20 – A varredura para classificação dos arquivos deve acontecer de forma contínua para qualquer tipo de dado armazenado nos repositórios monitorados na nuvem;
- 6.3.21 – A solução deverá permitir a análise dos arquivos classificados, indicando dentro do conteúdo do arquivo exatamente o que foi encontrado de dado sensível e confidencial;
- 6.3.22 – A solução deverá realizar a varredura de classificação de forma incremental, monitorando as atividades dos arquivos e executando a varredura apenas para os dados que foram atualizados ou tiveram alguma alteração;
- 6.3.23 – A solução deverá possibilitar a revisão das políticas de automação antes de serem aplicadas, com fluxo de aprovação, para que os usuários que tenham permissão, possam aprovar a execução da política;
- 6.3.24 – A solução deverá remediar de forma automatizada:
 - 6.3.24.1 – Links de colaboração que expõe dados sensíveis;
 - 6.3.24.2 – links de colaboração que expõe dados externamente ou publicamente;
 - 6.3.24.3 – links de colaboração que expõe dados para toda a organização;
 - 6.3.24.4 – links de colaboração obsoletos;
 - 6.3.24.5 – permissões diretas;
 - 6.3.24.6 – permissões diretas obsoletas.
- 6.3.25 – A solução deverá permitir a customização das políticas de remediação, podendo ser agendadas ou executadas de forma manual, baseado em sensibilidade, utilização, tipo de link e outros;
- 6.3.26 – A solução deverá disponibilizar dashboard de informações dos alertas verificados, com gráficos e painéis de usuários desatualizados com funções administrativas, associações desatualizadas em grupos, grupos públicos e muito mais;
- 6.3.27 – A solução deverá disponibilizar dashboard do SharePoint Online, com painéis para visualização de permissões obsoletas, exposição de sites, exposição de arquivos, exposição de pastas e membros de grupos obsoletos;
- 6.3.28 – A solução deverá disponibilizar dashboard do OneDrive, com painéis para visualizar arquivos expostos, arquivos sensíveis obsoletos, permissões obsoletas, links de colaboração;

- 6.3.29 – A solução deverá fornecer relatórios e painéis que mostram onde os dados confidenciais estão concentrados e expostos na nuvem, e onde você pode remover o acesso desnecessário para obter conformidade e manter os riscos baixos;
- 6.3.30 – A solução deverá fornecer relatório de permissões, incluindo informação da classificação dos arquivos;
- 6.3.31 – A solução deverá fornecer relatório referente aos níveis de exposição dos dados na nuvem, para qualquer tipo de site, pasta ou arquivo;
- 6.3.32 – A solução deverá fornecer relatório dos níveis de exposição das permissões, no contexto de dados sensíveis para qualquer pasta e arquivo;
- 6.3.33 – A solução deverá fornecer relatório das atividades de acesso dos usuários aos arquivos e pastas;
- 6.3.34 – A solução deverá fornecer relatório dos resultados da classificação dos dados, incluindo o número de hits e regra classificada;
- 6.3.35 – A solução deverá fornecer relatório de dados obsoletos, que não estão sendo acessados por um certo período de tempo;
- 6.3.36 – A solução deverá fornecer relatório para usuários desabilitados;
- 6.3.37 – Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV, Excel e PDF;
- 6.3.38 – Deverá ser possível realizar o agendamento de relatórios;
- 6.3.39 – Deverá ser possível encaminhar o relatório apenas para o proprietário do dado.

6.4 – Serviços incluídos de instalação, treinamento e suporte técnico

6.4.1 – Serviço de Instalação

- 6.4.1.1 – Os serviços de instalação lógica serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir:
 - 6.4.1.1.1 – Fase de abertura:
 - 6.4.1.1.1.1 – Validar e homologar o escopo, objetivos, requisitos, premissas, riscos e restrições do projeto;
 - 6.4.1.1.1.2 – Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica;
 - 6.4.1.1.1.3 – Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema;
 - 6.4.1.1.1.4 – Apresentar o estudo dos riscos envolvidos na migração para o novo

sistema a ser implantado.

6.4.1.1.2 – Fase de planejamento:

- 6.4.1.1.2.1 – Elaborar plano de projeto;
- 6.4.1.1.2.2 – Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;
- 6.4.1.1.2.3 – Reunir as equipes da CONTRATADA e CONTRATANTE;
- 6.4.1.1.2.4 – Definir os parâmetros de configuração básicos e avançados a serem implementados;
- 6.4.1.1.2.5 – Apresentar o Mapa de rede contendo a topologia a ser implementada;
- 6.4.1.1.2.6 – Apresentação do cronograma do projeto com os prazos e responsabilidades;
- 6.4.1.1.2.7 – Verificar os pré-requisitos do projeto;
- 6.4.1.1.2.8 – Apresentar plano do projeto para a homologação por parte da CONTRATANTE.

6.4.1.1.3 – Fase de execução:

- 6.4.1.1.3.1 – O serviço de instalação consiste na implantação, configuração da solução, objeto da contratação, de forma remota, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos, e entrega final da solução em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE;
- 6.4.1.1.3.2 – A CONTRATADA será inteiramente responsável pela implantação da solução adquirida, de forma a não comprometer o funcionamento da solução.
- 6.4.1.1.3.3 – A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante (recommended settings);
- 6.4.1.1.3.4 – Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração ou artigos técnicos;
- 6.4.1.1.3.5 – A solução, deverá ser entregue com todas as funcionalidades e recursos descritas neste termo de referência;
- 6.4.1.1.3.6 – A instalação da solução, incluindo todos os componentes e

- acessórios, será realizada pela CONTRATADA, com acompanhamento de uma equipe destacada pela CONTRATANTE;
- 6.4.1.1.3.7 – A CONTRATADA deverá providenciar um profissional certificado pelo fabricante na solução para garantir a conformidade da instalação e a configuração dos eventuais equipamentos e softwares que compõem a solução;
- 6.4.1.1.3.8 – A instalação, configuração e testes da solução deverá ser feita com o acompanhamento de técnicos da CONTRATANTE, visando o repasse de conhecimento e observados os padrões de gerenciamento de manutenção e segurança da CONTRATANTE;
- 6.4.1.1.3.9 – Deverá ser fornecida documentação de toda a implementação e configuração dos produtos adquiridos;
- 6.4.1.1.3.10 – Fica a critério do CONTRATANTE, definir o horário de instalação e configuração da solução, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno, se for o caso;
- 6.4.1.1.3.11 – Atividades associadas à implantação com a necessidade eventual de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do CONTRATANTE e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica da CONTRATANTE;
- 6.4.1.1.3.12 – A CONTRATADA deverá comunicar a CONTRATANTE à conclusão da instalação e entregar toda documentação técnica (As Built) em até 15 (quinze) dias corridos após a conclusão da instalação, bem como de cada ordem de serviço gerada dos serviços técnicos especializados;
- 6.4.1.1.3.13 – A documentação técnica (As Built), deverá ser aprovada pela equipe da CONTRATANTE, e caso necessário, os ajustes solicitados deverão ser realizados pela CONTRATADA em até 05 (cinco) dias após a análise da equipe da CONTRATANTE;
- 6.4.1.1.3.14 – O serviço de implantação da solução deverá ser concluído no prazo de, no máximo, 30 (trinta) dias, contados a partir da confirmação do recebimento da Ordem de Serviço;
- 6.4.1.1.3.15 – As atividades de instalação deverão ser acompanhadas pela equipe

técnica da CONTRATANTE, devendo a CONTRATADA efetuar o repasse técnico referente à instalação, implementação e operacionalização da solução, com transferência dos procedimentos básicos de configuração e operação utilizados;

6.4.1.1.3.16 – O repasse técnico, procedimentos e operacionalização deverá cobrir conhecimentos mínimos necessários para administração, configuração, otimização, resolução de problemas básicos e utilização da solução;

6.4.1.1.3.17 – A equipe técnica da CONTRATANTE deverá disponibilizar analistas ou técnicos, de forma presencial ou remota, para o acompanhamento das atividades definidas nos itens acima;

6.4.1.1.3.18 – As atividades de instalação, implementação e operacionalização da solução, que serão acompanhadas pela equipe técnica da CONTRATANTE, e realizadas pela CONTRATADA, deverão ser previstas no Plano de Projeto, e estas deverão ser distribuídas ou organizadas da melhor maneira possível durante as atividades e procedimentos previstos, para não impactar ou comprometer o prazo de entrega da solução;

6.4.1.1.3.19 – As atividades de instalação, implementação e operacionalização da solução, que serão acompanhadas pela equipe técnica da CONTRATANTE, e realizadas pela CONTRATADA, deverão ser realizadas por profissionais que sejam aptos a demonstrar na prática as principais funcionalidades da solução, particularmente, aquelas relacionadas à mudança de configuração e operação e monitoração da solução;

6.4.1.1.3.20 – O serviço de instalação, implantação, parametrização e operacionalização somente será considerado entregue após a aprovação da documentação técnica (As Built) pela equipe técnica da CONTRATANTE;

6.4.1.1.3.21 – A comprovação do pleno funcionamento da solução, conforme definido no Plano de Projeto estabelecido, dar-se-á após o de acordo da equipe técnica da CONTRATANTE.

6.4.2 – Treinamento Oficial (Reciclagem)

6.4.2.1 – O treinamento será na forma remota (online), com duração de 20 horas, para

até 10 participantes, com emissão de certificado de participação, sendo que, a critério do CONTRATANTE, poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de certificado de participação e material (limitando-se a 4 participantes adicionais do tipo “ouvintes”).

- 6.4.2.2 – Consiste em treinamento oficial do fabricante da solução, cobrindo conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que os colaboradores capacitados possam colocar a solução em produção, bem como planejar mudanças de configuração no ambiente;
- 6.4.2.3 – O CONTRATANTE solicitará a realização do treinamento à CONTRATADA mediante Abertura - ORDEM DE SERVIÇO de treinamento, sendo que este deverá ser iniciado em até 45 (quarenta e cinco) dias corridos após o recebimento da Abertura da ORDEM DE SERVIÇO pela CONTRATADA;
- 6.4.2.4 – A CONTRATADA deverá comprovar, previamente à realização do Treinamento, que o(s) INSTRUTOR(ES) selecionado(s) para ministrar o treinamento possuem qualificação condizente com o conteúdo programático a ser ministrado, incluindo certificados ou declaração do fabricante da solução;
- 6.4.2.5 – O CONTRATANTE poderá, a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a troca do instrutor. Caso a deficiência não possa ser sanada sem prejuízo para o andamento do curso, esse será suspenso, devendo a CONTRATADA agendar novo curso, sem ônus adicional ao CONTRATANTE.
- 6.4.2.6 – O treinamento deverá, ainda, respeitar o limite de 4 (quatro) horas por dia, possuir o conteúdo organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos com laboratórios para fixação, além de incluir apostilas e manuais dos eventuais equipamentos e softwares necessários para a prática dos exercícios propostos no material oficial do fabricante e serem fornecidos certificados de participação para cada participante (exceto para aqueles na condição de ouvintes).
- 6.4.2.7 – Todos os manuais, apostilas e demais documentos devem ser individuais, de primeiro uso e estar no idioma português (ou inglês, quando não disponíveis em português) e o treinamento deve ser ministrado em português.

- 6.4.2.8 – Após realização do curso será feita uma avaliação de satisfação junto aos participantes, cujo resultado deverá alcançar a média de, pelo menos, 70% (setenta por cento) de satisfação dentre os critérios avaliados, para validação e emissão do Termo de Aceite Definitivo. Caso não alcance o resultado esperado, o treinamento deverá ser ministrado novamente.
- 6.4.2.9 – As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA.
- 6.4.2.10 – O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante.
- 6.4.2.11 – A licitante proponente deverá entregar, na fase de habilitação, uma declaração afirmando que oferta o treinamento oficial do fabricante da solução e que a ementa e todo o material oferecido é aprovado pelo fabricante da solução, bem como, indicar na proposta o calendário contendo as datas de realização do Treinamento.
- 6.4.2.12 – A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o treinamento ofertado atende os requisitos indicados no item.
- 6.4.2.13 – O treinamento deverá ser ministrado por profissionais certificados pelo fabricante, cuja comprovação deverá ser encaminhada na assinatura do Contrato.
- 6.4.2.14 – A pedido da CONTRATANTE, o treinamento poderá ser gravado e disponibilizado;
- 6.4.2.15 – A CONTRATADA deverá aplicar o Formulário de Satisfação utilizando a escala de até 5 (cinco) pontos para cada quesito. No mínimo 70% dos participantes deverá atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso.
- 6.4.2.16 – O resultado da Avaliação de Instrutor/Tutor será utilizado como critério de aceitação do treinamento oficial do fabricante, devendo ser considerado pela amostra de participantes como “proveitoso” para no mínimo 6 (seis) dos 10 (dez) itens avaliados.
- 6.4.2.17 – Caso o resultado da Avaliação de Instrutor/Tutor seja considerado “não proveitoso”, o treinamento oficial do fabricante fornecido será considerado não aceito.

6.4.2.18 – Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento oficial do fabricante, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE.

6.4.2.19 – Na hipótese de o resultado do segundo treinamento oficial do fabricante ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

6.4.3 – Serviço de Suporte Técnico Assistido

6.4.3.1 – A CONTRATADA deverá prover o SERVIÇO DE APOIO OPERACIONAL, INVESTIGAÇÃO E ANÁLISE DE ALERTAS E COMPORTAMENTOS SUSPEITOS, com atendimento remoto para solução através profissional da CONTRATADA, em horário a ser definido pela CONTRATANTE, podendo ser no período matutino ou vespertino não excedendo 2 (duas) horas semanais.

6.4.3.2 – O serviço consiste no fornecimento de informações e esclarecimentos solicitados pela CONTRATANTE, em intervenções técnicas para solução de incidentes e problemas que estejam impactando a solução, em orientações técnicas sobre melhores práticas para uso da solução e em intervenções técnicas para parametrização e configuração da solução.

6.4.3.3 – O início do serviço ocorrerá no dia útil posterior à emissão e assinatura do Termo de Recebimento Definitivo (TRD) da solução pela CONTRATANTE.

6.4.3.4 – Este serviço não pode ser confundido com os serviços de suporte/garantia e manutenção, já contemplados na solução.

6.4.3.5 – A CONTRATANTE deverá utilizar Ordens de Serviço - OS, conforme modelo, que definirá as atividades mensais, para solicitar quando necessário os serviços específicos deste item.

6.4.3.6 – A CONTRATADA deverá prestar os serviços com duração de 2 (duas) horas semanais, compreendendo, mas não se limitando, ao seguinte escopo de atendimento da solução:

6.4.3.6.1 – Identificar quem tem acesso a uma pasta;

6.4.3.6.2 – Geração de relatório de conformidade técnica “health check”;

6.4.3.6.3 – Identificar que pasta determinado usuário tem permissão para acessar;

6.4.3.6.4 – Identificar quais pastas um grupo global tem acesso;

6.4.3.6.5 – Identificar permissões dos usuários de compartilhamento e NTFS nas pastas;

- 6.4.3.6.6 – Identificar pastas que contém dados sensíveis;
- 6.4.3.6.7 – Identificar arquivos que contém dados sensíveis;
- 6.4.3.6.8 – Identificar pastas com dados ociosos por mais de 90 dias;
- 6.4.3.6.9 – Identificar proprietário de determinada pasta;
- 6.4.3.6.10 – Visualizar eventos realizados dentro dos servidores de arquivos (Arquivos/Pastas abertos, modificados, criados, apagados e outros);
- 6.4.3.6.11 – Recomendações;
- 6.4.3.6.12 – Criar regras de classificação para dados sensíveis;
- 6.4.3.6.13 – Identificar quem são os membros do grupo do AD;
- 6.4.3.6.14 – Identificar que grupo determinado usuário pertence;
- 6.4.3.6.15 – Identificar contas sem política de senha;
- 6.4.3.6.16 – Identificar contas sem atividade de logon por mais de 90 dias;
- 6.4.3.6.17 – Identificar contas ativadas sem expiração de senha;
- 6.4.3.6.18 – Identificar contas desabilitadas;
- 6.4.3.6.19 – Visualizar eventos realizados dentro do AD;
- 6.4.3.6.20 – Remediação de contas de computador que são contas de administrador;
- 6.4.3.6.21 – Identificar quem tem acesso à uma caixa de email específica;
- 6.4.3.6.22 – Identificar quais caixas de e-mail determinado usuário tem acesso;
- 6.4.3.6.23 – Identificar quem tem acesso à uma pasta pública, e quais são essas pastas;
- 6.4.3.6.24 – Habilitar alertas importantes de segurança, como:
 - 6.4.3.6.24.1 – Comportamento anormal: acesso a uma quantidade incomum de dados confidenciais ociosos;
 - 6.4.3.6.24.2 – Atividade de criptografia detectada;
 - 6.4.3.6.24.3 – Ataque de downgrade de criptografia;
 - 6.4.3.6.24.4 – Criptografia de múltiplos arquivos;
 - 6.4.3.6.24.5 – Arquivo criptografado por ransomware;
 - 6.4.3.6.24.6 – Padrão imediato detectado: as ações do usuário se assemelham a ransomware;
 - 6.4.3.6.24.7 – Falha de operação em uma ferramenta de exploit;
 - 6.4.3.6.24.8 – Possível escalção de privilégio;
 - 6.4.3.6.24.9 – Suspeita de ataque de força bruta;
 - 6.4.3.6.24.10 – Possível replicação do AD;
 - 6.4.3.6.24.11 – Visualizar trilha de auditoria a partir do alerta;

- 6.4.3.7 – A CONTRATADA deverá disponibilizar profissional qualificado na solução para o atendimento, o qual será responsável pelo apoio operacional e deverá possuir certificação do fabricante para realização atendimento.
- 6.4.3.8 – O profissional da CONTRATADA deverá propor e tomar as ações necessárias para o ambiente do CONTRATANTE seguindo as melhores práticas do fabricante.
- 6.4.3.9 – O profissional deverá apoiar a equipe da CONTRATANTE com emissão de relatórios da solução, com intuito de melhoria contínua do ambiente.

7 – LOCAL E PRAZO DE ENTREGA

O objeto será fornecido de acordo com as quantidades solicitadas com base na Ordem de Serviço emitida, correndo eventuais fretes e tributos às expensas do fornecedor.

7.1 – LOCAL DE ENTREGA

Os itens licitados deverão ser entregues no seguinte endereço: **GTIC – Gerência de Tecnologia da Informação, localizada na Sede da DESO, Rua Campo Do Brito, No 331, Bairro Praia 13 de Julho, Aracaju/SE**, nos seguintes horários: 07h:00 às 12h:00 e das 14h:00 às 16h:00. Caso a entrega seja eletrônica, deverá ser utilizado o email corporativo infra-tic@deso-se.com.br;

7.2 – PRAZO DE ENTREGA

A CONTRATADA deve realizar a entrega da solução em até 30 (trinta) dias, contados da data de emissão da Ordem de Fornecimento.

8 – INSTALAÇÃO, GARANTIA E SUPORTE

8.1 – Implementação da solução ofertada deve seguir os critérios abaixo:

8.1.1 – O escopo dos serviços a serem contratados deve abranger a instalação da Solução, implantação, parametrização e operacionalização dos diversos componentes da Solução de Auditoria de Dados e E-mail, além de treinamento e transferência de conhecimento, e apoio

operacional para investigação e análise de alertas e comportamentos suspeitos no ambiente da CONTRATANTE.

8.1.2 – Todas as atividades relacionadas à implantação da Solução serão prestadas nas instalações da CONTRATANTE pela equipe da CONTRATADA, podendo ser de forma remota.

8.1.3 – Por instalação, customização, integração e ativação entendam-se todos os procedimentos relacionados à instalação e configuração, física e lógica, parametrização e testes de quaisquer componentes de software fornecidos no escopo do Edital, de modo a garantir o pleno funcionamento da solução.

8.1.4 – A CONTRATADA deverá criar e manter atualizada documentação das atividades, processos, testes, homologação, entrega e conferência, reuniões de trabalho, compromissos e prazos, incluindo planos de trabalho e atas de reunião, de modo a compor uma documentação final da implantação a ser entregue. Toda a documentação gerada no escopo do projeto deverá estar no idioma português.

8.1.5 – A CONTRATANTE se reserva o direito de redefinir, a qualquer momento da implantação, quaisquer fases, ações, prazos e recursos envolvidos, objetivando a garantia de atendimento dos parâmetros de qualidade, segurança, mitigação de riscos e atendimento de prazos, cabendo à CONTRATADA adequar-se às modificações propostas, refazendo atividades e documentação, caso necessário, desde que essas não extrapolem o escopo dos serviços definidos no objeto.

8.1.6 – A CONTRATADA será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados aos serviços de implantação dos componentes da Solução objeto do Edital. Caso o diagnóstico aponte para problemas não relacionados aos componentes da Solução, o CONTRATANTE deverá adotar as medidas necessárias para solucioná-los, desde que devidamente comprovados pela CONTRATADA, e sempre a critério da CONTRATANTE.

8.1.7 – Os serviços de instalação das soluções abrangem todas as soluções ofertadas em sua proposta comercial.

8.2 – A solução contratada deverá contar com garantia mínima de 12 (doze) meses, com o

objetivo de prover a continuidade das operações, e oferecer suporte técnico e manutenção durante todo o período contratual. A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da solução.

8.3 – A CONTRATANTE poderá abrir chamados de manutenção diretamente no FABRICANTE do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas;

8.4 – A abertura de chamados poderá ser realizada através de telefone do fabricante, através da página da WEB do fabricante ou através de endereço de e-mail do fabricante. Este será considerado o início para contagem dos prazos estabelecidos.

8.5 – Durante o período de suporte técnico, devem ser disponibilizados, sem ônus à CONTRATANTE, todas as atualizações de software para a solução implantada, quando for necessário;

8.6 – O serviço de suporte deve proporcionar a interação com a equipe técnica do fabricante, fornecendo apoio na resolução de incidentes que envolvam os componentes da oferta, garantindo seu pronto restabelecimento.

8.7 – Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, devendo a CONTRATADA zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados. a. Todas as informações, imagens, aplicativos e documentos providos pela CONTRATANTE ou oriundos das informações que forem propriedade da CONTRATANTE que forem manuseados e utilizados, são de propriedade da CONTRATANTE, não podendo ser repassadas, copiadas, alteradas ou absorvidas na relação de bens da CONTRATADA, bem como, de seus executores, sem expressa autorização da CONTRATANTE.

8.7 – A CONTRATADA deve executar o objeto do certame em estreita observância dos ditames estabelecidos pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de

Dados Pessoais – LGPD).

8.8 – A CONTRATADA não deve veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato sem prévia autorização da CONTRATANTE.

8.9 – A CONTRATADA não deve fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do contrato em questão, além de dever manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os eventuais equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

8.10 – A CONTRATADA deverá aceitar o Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA e Profissional responsável pela execução dos serviços.

8.11 – A prestação de serviços de que trata este Termo de Referência não gera vínculo empregatício entre os empregados da CONTRATADA e a CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

9 – DAS OBRIGAÇÕES DAS PARTES

9.1 – DA CONTRATADA

9.1.1 – Entregar os produtos e serviços cumprindo rigorosamente todas as especificações, prazos, obrigações e cláusulas estabelecidas neste edital e seus Anexos;

9.1.2 – Zelar pela perfeita execução do contrato;

9.1.3 – Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no ato convocatório;

9.1.4 – Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato, obrigando-se a liquidá-los nos respectivos vencimentos,

sabendo que:

9.1.4.1 – A inadimplência do contratado, com referência aos encargos trabalhistas, fiscais, previdenciários e comerciais não transfere à Administração Pública a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato; e

9.1.4.2 – Não existirá, em hipótese alguma, nenhum vínculo empregatício entre os empregados da CONTRATADA e a CONTRATANTE.

9.1.5 – Responsabilizar-se por quaisquer danos pessoais e/ou materiais, causados por seus empregados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pela CONTRATANTE;

9.1.6 – Responsabilizar-se por todos os encargos e obrigações previstos na legislação pertinente a acidentes de trabalho, quando forem vítimas os seus funcionários no desempenho dos serviços objeto desta licitação, mesmo que ocorrido nas dependências da CONTRATANTE, assim como pelos seguros e demais obrigações empregatícias vigentes e futuras;

9.1.7 – Responsabilizar-se pelas eventuais despesas para execução do serviço solicitado, qualquer que seja o valor.

9.1.8 – Não transferir a qualquer título, os serviços contratados;

9.1.9 – Independentemente de transcrição na proposta, sujeitar-se às demais obrigações estabelecidas neste Termo de Referência.

9.1.10 – Cumprir todas as especificações, obrigações e cláusulas estabelecidas no Edital e seus Anexos;

9.1.11 – Comunicar à CONTRATANTE, por escrito, qualquer anormalidade de caráter urgente e prestar, com a devida antecedência, os esclarecimentos necessários;

9.1.12 – Assumir inteira responsabilidade sobre o objeto contratado perante a DESO;

9.1.13 – Providenciar a imediata correção das deficiências, falhas ou irregularidades apontadas pela CONTRATANTE na execução do objeto, atendendo às solicitações do

executor do contrato, voltadas ao saneamento e correção da(s) irregularidade(s) verificada(s);

9.2 – DA DESO

9.2.1 – Proporcionar à CONTRATADA todas as facilidades para que possa desempenhar o objeto do Termo de Referência de forma satisfatória.

9.2.2 – Designar uma equipe técnica para fiscalizar e acompanhar a execução dos serviços prestados.

9.2.3 – Avaliar e aprovar a execução dos serviços, funcionalidades da solução e a qualidade do projeto, solicitando à CONTRATADA a correção das não conformidades, sem que haja ônus para a DESO.

9.2.4 – Prestar as informações e os esclarecimentos que venham a ser solicitados pelos responsáveis da CONTRATADA.

9.2.5 – Dar ciência à CONTRATADA de quaisquer modificações que venham a ocorrer.

9.2.6 – Atestar as notas fiscais/faturas, por unidade competente, emitidas pela CONTRATADA, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactuadas.

10 – DA GESTÃO E FISCALIZAÇÃO

10.1. Gestor do Contrato

10.1.1. É de responsabilidade do ocupante da função FG-5 da Gerência de Tecnologia da Informação e Comunicação – GTIC a gestão do contrato;

10.1.2. É de responsabilidade do gestor do contrato:

a) Aplicar sanções e glosas mediante indicação do fiscal do contrato;

b) Liberação de pagamento mediante autorização do fiscal do contrato, após conferência da entrega em conformidade do produto ao especificado neste termo;

10.2. Fiscal do Contrato

10.2.1. É de responsabilidade do ocupante da função FG-4 da Coordenação de Infraestrutura – CINF a fiscalização do contrato;

10.2.2. É de responsabilidade do fiscal do contrato:

- a) Avaliação da qualidade do produto;
- b) Identificação de não conformidade do produto entregue e notificação ao gestor do contrato;
- c) Autorização para faturamento mediante conferência da entrega em conformidade do produto ao especificado neste termo;

11 – DO PAGAMENTO

11.1. O pagamento deverá ser efetuado em parcelas anuais, 30 (trinta) dias após a emissão do Termo de Aceite assinado pelo fiscal do contrato e apresentação de Fatura e Nota Fiscal.

11.2. Caso se faça necessária a apresentação ou reapresentação de qualquer Nota Fiscal/Fatura ou documentação por culpa da CONTRATADA, o prazo de até 30 (trinta) dias reiniciar-se-á a contar da data da respectiva apresentação ou reapresentação.

12 – DAS DISPOSIÇÕES GERAIS

A DESO poderá realizar uma reunião de integração com o Fornecedor no momento da entrega do Contrato, caso julgue necessário.

A CONTRATADA deverá assumir todos os custos, ônus e taxas, decorrentes do fornecimento, devendo ser previamente verificados pela empresa em sua proposta comercial. Não serão aceitos custos adicionais sob qualquer pretexto, devendo a empresa dirimir previamente todas as dúvidas e assumir inteira responsabilidade pelo fornecimento do objeto.

O adequado transporte para eventual entrega dos produtos, no local indicado, data e

prazos de fornecimento são de integral responsabilidade da CONTRATADA.

O Termo de Aceite só será emitido pela DESO quando toda solução for instalada e assim forem constatadas todas as funcionalidades exigidas neste Termo de Referência.

13 – DISPOSIÇÕES ESPECÍFICAS

13.1 – OS RECURSOS ORÇAMENTÁRIOS:

Os recursos para o pagamento dos serviços objeto do Pregão Eletrônico, provêm da previsão de Recursos Próprios da DESO, constante do Orçamento para o exercício de 2026 e 2027.

13.2 – CLASSIFICAÇÃO ORÇAMENTÁRIA

As despesas decorrentes do objeto desta licitação obedecerão a classificação adiante discriminada, consignada no orçamento empresarial da DESO.

Conta: **300.05 – SERVIÇOS DE TERCEIROS**

13.3 – VALIDADE DA PROPOSTA

O prazo de validade da proposta não pode ser inferior a 90 (noventa) dias consecutivos, contados da data da sessão pública de abertura desta licitação.

13.4 – DA SUBCONTRATAÇÃO E ALTERAÇÃO SUBJETIVA

13.4.1 – Não será admitida a subcontratação do objeto licitatório.

13.5 – PRAZO DE VIGÊNCIA

O prazo de validade da Ata de Registro de Preços decorrente deste certame será de 12 (doze) meses, contados a partir da emissão da ordem de serviço, período no qual os preços registrados permanecerão disponíveis para futuras contratações pela DESO e órgãos

aderentes autorizados. O referido prazo de validade da Ata não se confunde e não invalida o prazo de vigência contratual da prestação dos serviços, o qual poderá ser de até 12(doze) meses, contados a partir da emissão da Ordem de Serviços, sendo este prazo prorrogável por até 60 (sessenta) meses, conforme o Regulamento Interno de Licitações e Contratos (RILC) da DESO e a Lei nº 13.303/2016.

13.6 – DO CRITÉRIO DE JULGAMENTO

O critério de julgamento será o de MENOR PREÇO DO LOTE

13.7 – DO REGIME DE EXECUÇÃO

O regime de execução será por PREÇO UNITÁRIO.

14 – DAS CONDIÇÕES DE PARTICIPAÇÃO

14.1 – Poderão participar do certame todos os interessados do ramo de atividade pertinente ao objeto da contratação.

14.2 – Não poderão participar os interessados que se encontrarem sob falência, concurso de credores, dissolução, liquidação, empresas estrangeiras que não funcionam no país, nem aqueles que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública, ou punidos com suspensão do direito de licitar e contratar com a Administração Pública Estadual.

14.3 – A participação neste certame implica aceitação de todas as condições estabelecidas neste instrumento.

15 – DAS SANÇÕES ADMINISTRATIVAS

15.1 – A CONTRATADA pelo inadimplemento de suas obrigações, garantida a prévia defesa da CONTRATADA no prazo de 10 (dias) dias úteis, ficará sujeita as seguintes sanções previstas no RILC e na Lei 13.303/2016:

15.1.1 – Advertência;

15.1.2 – Multa moratória;

15.1.3 – Multa compensatória;

15.1.4 – Suspensão do direito de participar de licitação e impedimento de contatar com a DESO, pelo prazo de até 02 (dois) anos;

15.1.5 – Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

15.2 – As sanções constantes no subitem 10.1 poderão ser aplicadas de forma cumulativa.

15.3 – Ficar impedida de licitar e de contratar com a Administração Pública Estadual, pelo prazo de até 05 (cinco) anos, garantido o direito prévio de defesa, o fornecedor que:

15.3.1 – Ensejar o retardamento da execução do objeto desta licitação;

15.3.2 – Não mantiver proposta, injustificadamente;

15.3.3 – Comportar-se de modo inidôneo;

15.3.4 – Fizer declaração falsa;

15.3.5 – Cometer fraude fiscal;

15.3.6 – Falhar ou fraudar no fornecimento do objeto.

15.4 – São consideradas condutas reprováveis e passíveis de sanções, dentre outras, as previstas no art. 186 do RILC.

15.5 – As multas estabelecidas serão entendidas como independentes e cumulativas e serão compensadas pela DESO com as importâncias em dinheiro, relativas às prestações a que corresponderem, ou da garantia do contrato, quando for o caso, cobradas judicialmente.

15.6 – A aplicação de sanção de advertência se efetiva com o registro da mesma junto ao cadastro de fornecedores e no sistema de gerenciamento de contatos da DESO, independentemente de tratar-se de pessoa cadastrada ao não.

15.7 – A multa poderá ser aplicada nos seguintes casos:

I – Em decorrência da interposição de recursos meramente procrastinatórios, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

II – Em decorrência da não regularização da documentação de habilitação, nos termos do artigo 43, § 1º da Lei Complementar nº 123/2006, a vista do subitem 15.3.6, poderá ser aplicada multa correspondente 3% do valor máximo estabelecido para a licitação em questão.

III – Pela recusa em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido por este edital, poderá ser aplicada multa correspondente a 5% do valor máximo estabelecido para a licitação em questão.

IV – No caso de atraso na entrega da garantia contratual, quando exigida, o instrumento convocatório deverá prever, mediante competente justificativa, a incidência de multa correspondente 3% do valor total do contrato;

V – No caso de inexecução parcial, incidirá multa na razão de 10% sobre o valor da parcela não executada;

VI – No caso de inexecução total, incidirá multa na razão de 25% sobre o saldo remanescente do contrato;

VII – nos demais casos de atraso, incidirá multa na razão de 5% sobre o valor da parcela em atraso.

15.8 – Caso não haja o recolhimento da multa no prazo estipulado, a DESO descontará a referida importância de eventuais créditos a vencer da empresa CONTRATADA. Na ausência de créditos disponíveis para quitação da importância da multa, a DESO executará a garantia quando exigida, e quando for o caso, será cobrada judicialmente.

15.9 – A DESO poderá quando do não pagamento da multa pela CONTRATADA, aplicar a sanção de suspensão do direito de participar de licitação e impedimento de contratar com a DESO, por até 02 (dois) anos;

15.10 – Cabe a sanção de suspensão em razão de ação ou omissão capaz de causar, ou que tenha causado dano à DESO, suas instalações, pessoas, imagem, meio ambiente ou a terceiros, aplicando a disposição do art. 189 e 190 do RILC em face da legislação previdenciária, social ou trabalhista.

16 – QUALIFICAÇÃO ECONÔMICA

16.1 – Não será exigida, em virtude da entrega integral do objeto de forma imediata.

17 – DA GARANTIA CONTRATUAL

17.1 – Não será exigida, em virtude da entrega integral do objeto de forma imediata.

18 – REAJUSTAMENTO DE PREÇOS

18.1 – A cada 12 (doze) meses, a partir da data de apresentação das Propostas de Preços, o Contrato será reajustado pelo IPCA, publicado pelo IBGE, com a aplicação da seguinte fórmula de reajuste:

$$R = V. \frac{I1 - I0}{I0}$$

Onde:

R = Reajuste

I1 = Índice no mês do fato gerador do evento do faturamento

I0 = Índice do mês de apresentação da proposta

V = Valor da fatura.

18.2 – Caso o valor do Índice não esteja disponível na data do cálculo do reajuste, utilizar-se-á o último Índice disponível e o cálculo do reajuste será complementado quando da publicação do Índice correspondente.

18.3 – Caberá à CONTRATADA a iniciativa e o encargo da apresentação da memória de cálculo do reajuste a ser pleiteado, cuja aprovação do percentual de reajuste deverá ser negociado e aprovado pela DESO, observando-se os valores praticados no mercado à época de sua concessão para serviços compatíveis com o objeto da contratação.

18.4 – Os reajustes serão formalizados por meio de apostilamento e não poderão alterar o

equilíbrio econômico-financeiro dos contratos.

18.5 – A omissão da CONTRATADA quanto ao seu direito de pleitear o reajuste, não será aceita como justificativa para o pedido de correção anual de preço com efeito retroativo à data a que legalmente faria jus, se não o fizer dentro do primeiro mês do aniversário deste instrumento, arcando esta, portanto, por sua própria inércia.

19 – CRITÉRIOS DE ACEITABILIDADE DOS PREÇOS

19.1 – Os preços unitários e global somente serão aceitos quando não superiores aos estimados no preço de referência da DESO;

19.2 – Em hipótese alguma será aceito aumento dos valores inicialmente propostos;

19.3 – Não havendo por parte do arrematante a revisão de sua proposta dentro do prazo estabelecido pelo pregoeiro, a mesma terá sua proposta desclassificada;

20 – DA PROPOSTA DE PREÇOS

20.1 – O licitante deverá estar ciente e levar em consideração, além das especificações e condições estabelecidas no Edital, o atendimento dos seguintes requisitos:

20.1.1 – Nos preços propostos deverão estar inclusos todos os custos necessários para o atendimento do objeto da licitação, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, deslocamentos de pessoal, treinamento, garantia, montagem, instalação, eventuais materiais e equipamentos, e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado constante da proposta;

20.1.2 – Os preços deverão ser cotados em moeda corrente nacional e neles deverão estar inclusas todas e quaisquer despesas, tais como: IPI e demais impostos, encargos sociais, seguros, taxas, tributos diretos e indiretos incidentes sobre o fornecimento dos materiais;

20.1.3 – A proposta entregue será considerada com prazo de validade de 90 dias, contados da data da sessão pública de abertura desta licitação;

20.2 – Deverá ser descrito as características reais dos produtos ofertados com modelo,

capacidade, etc, não sendo aceito a simples cópia do texto das especificações técnicas constantes nesse Termo de Referência.

20.3 – Deverá ser apresentado documentação oficial do fabricante que comprove o pleno atendimento dos produtos ofertados às especificações técnicas constantes neste Termo de referência. Serão aceitos catálogos oficiais do fabricante, documentos com links da internet do site oficial do fabricante ou declaração assinada pelo próprio fabricante.

20.4 – Serão desclassificadas as propostas:

- a) que não atendam às exigências do ato convocatório ou que apresentem dispositivos contrários à lei e à regulamentação vigente;
- b) que contiverem preços ou vantagens de qualquer natureza ou descontos não previstos neste Pregão, inclusive financiamentos subsidiados ou a fundo perdido;
- c) que forem omissas, vagas, apresentarem irregularidades ou defeitos capazes de dificultar o julgamento, bem como as que apresentarem preços ou vantagens baseadas nas ofertas de outros licitantes;
- d) que forem superiores ao valor orçado pela DESO.

20.5 – A proposta deverá limitar-se ao objeto desta licitação, sendo desconsideradas quaisquer alternativas de preço ou qualquer outra condição não prevista.

20.6 – Independentemente de declaração expressa, a simples apresentação das propostas implica submissão a todas as condições estipuladas no Edital e seus Anexos, sem prejuízo da estrita observância das normas contidas na legislação mencionada no preâmbulo do Edital.

20.7 – A Proposta de Preço será considerada completa e abrangerá todos os custos necessários ao objeto.

20.8 – Empresas que participarem deste processo, que praticarem, injustificadamente, ato ilegal tipificado no art. 7º da Lei 10.520/2002, a Administração instaurará processo administrativo para apurar as condutas das empresas (TCU – Acórdão nº 754/2015 – Plenário) concomitantemente com as Sanções Administrativas previstas no item 14 deste Termo de referência.

21 – EXIGÊNCIA DE AMOSTRA

21.1 – Após o aceite da proposta quanto ao valor e havendo dúvidas no tocante ao atendimento das especificações técnicas, o pregoeiro poderá solicitar, primeiramente, catálogo ou documento similar que comprove a conformidade do produto ofertado, devendo o licitante informar o site do fabricante;

21.2 – Inexistindo catálogo ou sendo este insuficiente para análise técnica das especificações do produto, o interessado classificado provisoriamente em primeiro lugar deverá apresentar amostra, na forma de prova de conceito, que terá data, local e horário de sua realização divulgados por mensagem no sistema, cuja presença será facultada a todos os interessados, incluindo os demais fornecedores interessados, mediante solicitação ao pregoeiro, para prévio agendamento com a unidade técnica.

LUCIANO COSTA

MACEDO:0032019

5562

Assinado de forma digital por
LUCIANO COSTA

MACEDO:00320195562

Dados: 2026.09.22 12:52:14
-03'00'

Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço <http://edocsergipe.se.gov.br/consultacodigo> e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: UBXN-QEID-UNQU-6X0N



O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 23/09/2026 é(são) :

Legenda: ● Aprovada ● Indeterminada ● Pendente

● LUCIANO COSTA MACEDO 22/09/2026 12:52:14 (Certificado Digital)