

TERMO DE REFERÊNCIA	DOD N° 27/2024
1. IDENTIFICAÇÃO DA CONTRATANTE	
<p>Razão Social: Agência de Fomento do Estado do Amazonas S.A. - AFEAM. CNPJ nº: 03.183.937/0001-38 Endereço: Avenida Constantino Nery, nº 5733, Flores, CEP 69058-795. Cidade: Manaus Estado: Amazonas</p> <p>Equipe de Planejamento da Contratação: José Alves Pereira Neto / GETI Jaderclei da Costa Nogueira / GETI Márcia Campelo da Silva / GEPEC Ívia Victória Monteiro Lima de Mattos /GEPEC</p>	
2. OBJETO	
2.1. Produto ou serviço a ser contratado:	
<p>2.1.1. Contratação de empresa especializada em fornecimento de Licenças de uso de software e garantia da solução de auditoria para os aplicativos ActiveDirectory, Microsoft Exchange Server, Windows File Server, SharePointOnline (One Drive), abrangendo centro de dados e endpoint, com fornecimento de instalação, treinamento e suporte técnico.</p>	
2.2. Característica do Objeto	
<p>2.2.1. O objeto, aquisição de soluções de segurança, gestão, monitoramento, é considerado comum</p>	
2.3. Subcontratação	
<p>2.3.1. Não será admitido a subcontratação do objeto.</p>	
3. JUSTIFICATIVA	
<p>3.1 Soluções de auditoria de dados estruturados e não estruturados endereçam requisitos de TI, bem como os requisitos das áreas de riscos e controle. A solução oferecerá funcionalidades para todos os casos de uso, descobrindo contas e dados em sistemas, dispositivos e aplicativos para gerenciamento subsequente, protegendo e isolando, monitorando, registrando e auditando sessões, comandos e ações de acesso. Além disso, delegação, controle e filtro de operações privilegiadas que um administrador pode executar e integração robusta de autenticação para garantir os níveis de confiança e reponsabilidade pelo acesso. Por fim, funcionalidades para serviços e aplicativos também são englobadas, como gerenciamento de dados, contas e sessões e gerenciamento de elevação e delegação de privilégios e permissionamento. Sendo assim, para atingir os objetivos estratégicos e de negócio e suprir as demandas, a TI tem que necessariamente estar apoiada em práticas, normas e ferramentas que propiciem a gestão dos permissionamentos e privilégios, pois de outra forma, seriam majorados os riscos de TI e consequentemente, os riscos</p>	

operacionais envolvidos nos processos de sustentação dos serviços. Neste sentido, a pretensa aquisição justifica-se para melhor controle dos acessos por contas, dados e permissionamento viabilizando a rastreabilidade dos autores responsáveis por atos praticados, inclusive, preservando as evidências e garantindo a audibilidade das ações.

3.2 A contratação vem atender ao planejamento estratégico da agência, conforme o DOD nº 27/2024, em seu item 1.5.1, a saber:

3.2.1 Metas Qualitativas – Ações Tecnológicas – Sistema de Monitoramento de Informações e prevenção contra de Dados.

3.2.2 Metas Qualitativas – Ações Tecnológicas – Sistema de Monitoramento de Informações e prevenção contra de Dados.

3.3 A contratação está alinhada com a política e normas administrativas da instituição. A realização da despesa dessa contratação está prevista no Planejamento Estratégico da AFEAM, Diretriz 02: Área Meio, Projeto nº 03: Sistema de Monitoramento de Informações e prevenção contra de Dados.

4. ESPECIFICAÇÕES TÉCNICAS DO OBJETO E DO QUANTITATIVO

4.1 Especificações e quantidades:

4.1.1 Os serviços serão licitados da seguinte forma:

Item	CATSER	Descrição do material ou serviço	Und. fornec	Qnt.
1	27502	Contratação de solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento dos serviços de auditoria para os aplicativos ActiveDirectory, Microsoft Exchange Server, Windows File Server, SharePointOnline (One Drive), abrangendo centro de dados e endpoint. A contratação inclui licenciamento, instalação, treinamento, garantia e suporte técnico para a solução pelo período de 12 meses.	LICENÇAS	250

4.1.2 Os licitantes deverão apresentar proposta de preços de acordo com tabela abaixo:

Item	Descrição	Qtd	Unidade Fornecimento	Valor Unitário	Valor Total
1	Licenças de uso de software e garantia da solução de auditoria para os aplicativos ActiveDirectory, Microsoft Exchange Server, Windows File Server, SharePointOnline (One Drive), e abrangendo centro de dados e endpoint,	250	LICENÇAS		

	com fornecimento de instalação, treinamento e suporte técnico.				
VALOR TOTAL					

4.1.3 Requisitos Gerais dos Serviços:

4.1.3.1 Os requisitos gerais definem os requisitos para todos os serviços que compõem o objeto SOLUÇÃO DE AUDITORIA DE DADOS NÃO ESTRUTURADOS, sempre que aplicáveis.

4.1.4 Considerações Gerais:

4.1.4.1 O não atendimento a qualquer um desses requisitos é fator impeditivo para a aceitação da proposta da licitante.

4.1.4.2 A solução deverá oferecer condições para gestão dos dados não estruturados de diretório de usuários, servidores de arquivos e serviços na plataforma Microsoft 365, de forma que a equipe de TI da AFEAM tenha condições de analisar, controlar e auditar os recursos e plataformas monitoradas.

4.1.4.3 A solução deverá fazer o monitoramento e auditoria dos usuários e seus acessos internos e externos ao diretório de usuários, pastas, arquivos e caixas de e-mail dos servidores monitorados.

4.1.4.4 Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo deverá ser executado de forma a diminuir o impacto sobre a disponibilidade dos serviços.

4.1.4.5 Devido à complexidade e à quantidade de servidores monitorados, todas as informações e plataformas monitoradas deverão ter seus acessos controlados por meio de autenticação baseada em usuários ou grupos do domínio da AFEAM.

4.1.4.6 Deve ser possível a configuração de diversos perfis com permissões e restrições de acesso dos usuários às funcionalidades da solução, de forma a segregar o acesso de analistas, equipe de suporte e usuários finais.

4.1.4.7 A solução deverá contemplar todas as licenças necessárias para o atendimento de todos os requisitos exigidos nesta especificação técnica;

4.1.4.8 A solução deverá ser instalada em máquina virtual com sistemas operacionais Windows Server 2012 R2 ou superior.

4.1.4.9 O padrão utilizado na AFEAM, no que se refere à tecnologia de bancos de dados, são as soluções Microsoft SQL Server e MySQL. Portanto, a solução ofertada deverá armazenar as informações de log de acessos nestes bancos de dados. Outras soluções não serão aceitas;

4.1.4.10 A solução deve permitir o acesso aos dados de auditoria capturados e armazenamento;

4.1.4.11 A solução deve suportar a utilização de servidores virtualizados para todos os seus componentes e deve ser compatível com o ambiente de virtualização Vmware ou Microsoft Hyper-V;

4.1.4.12 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 de as informações serem utilizadas para perícia, a solução deverá possuir relatórios que forneçam evidências para controles recomendados por certificações como a ISO/IEC 27.001 ou similares;

4.1.4.13 As soluções fornecidas pela contratada devem contemplar a auditoria de sistemas na última versão disponibilizada pelo fabricante;

4.1.4.14 A solução ofertada deve oferecer, com rotinas automatizadas, relatórios agendados e sob demanda, em diversos formatos de arquivos (Excel, PDF, CSV e XML), exportados no momento da geração, ou enviados por e-mail, ou armazenados em um compartilhamento de arquivos através de agendamentos customizáveis.

4.1.4.15 Deve ser possível, através da console, a criação de modelos de relatórios para posterior reutilização. Essa criação de modelos deve ser intuitiva e não deve necessitar da utilização de linguagem de programação ou outro software.

4.1.4.16 A documentação relativa às especificações técnicas da solução de TI deve ser fornecida em português. Alternativamente, poderá ser apresentada em Língua Inglesa.

4.1.4.17 A solução deve permitir o acesso de, pelo menos, 10 colaboradores a todas as suas funcionalidades administrativas. Para funcionalidades que eventualmente sejam disponibilizadas a todos os usuários da AFEAM, a solução deve permitir o acesso de todos os usuários.

4.1.4.18 A solução deve possuir interface nos idiomas português ou inglês.

4.1.4.19 Todos os itens apresentados nesta especificação são obrigatórios e deverão ser atendidos de forma nativa. Entende-se por itens atendidos de forma nativa, todos aqueles itens atendidos diretamente pelo software e seus módulos, sem a necessidade de alteração do código fonte em sua estrutura.

4.1.5 CARACTERÍSTICAS DE PERMISSIONAMENTO

4.1.5.1 A solução deverá apresentar, em sua interface, todos os usuários e grupos de segurança dos diferentes domínios monitorados, assim como os usuários e grupos de segurança locais de cada servidor ou plataforma monitorada.

4.1.5.2 A solução deve permitir a busca por uma pasta nos servidores monitorados e apresentar quais usuários e grupos de segurança têm permissões e quais permissões esses objetos têm na pasta.

4.1.5.3 A solução deverá consolidar as permissões NTFS e de compartilhamento de cada pasta e demonstrar a permissão efetiva dos usuários e grupos.

4.1.5.4 A solução deve utilizar os eventos coletados pela auditoria para realizar a análise comportamental dos usuários de maneira a fazer recomendações de revogação de acesso aos dados não estruturados dos servidores monitorados.

4.1.5.5 Além da visibilidade de permissões, usuários e grupos de segurança, deve ser possível realizar alterações de permissionamento dos usuários e grupos de segurança às pastas e diretórios dos servidores monitorados através da interface gráfica da solução.

4.1.5.6 A solução deve fornecer a visibilidade sobre aplicação de alterações e o histórico das alterações aplicadas através da console.

4.1.6 LOGS DE AUDITORIA MONITORADOS

4.1.6.1 A solução deve coletar de forma automática e contínua logs de acessos a diretórios, pastas e arquivos dos servidores de arquivos monitorados, acessos a objetos do Active Directory(AD), compartilhamento de arquivos e acessos aos recursos da solução Office 365.

4.1.6.2 Deve ser possível, na interface gráfica da solução, visualizar os logs de auditoria de acessos a diretórios, pastas e arquivos dos servidores monitorados, acessos a objetos do AD e acessos a objetos do Office 365 organizados e agrupados por recurso monitorado:

4.1.6.2.1 Pasta ou diretório: demonstrar todos os eventos para aquela pasta, subpastas e arquivos;

4.1.6.2.2 Unidade organizacional: demonstrar os eventos ocorridos em determinada OU;

4.1.6.2.3 Usuário ou grupo de segurança: demonstrar os eventos gerados ou sofridos por determinado usuário ou grupo.

4.1.6.3 Os eventos de auditoria coletados pela solução devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto acessado, caminho dos arquivos, pastas e objetos, identificação do domínio, arquivo, pasta ou objeto impactado e nome do usuário que realizou a ação.

4.1.6.4 As consultas aos logs através da console da solução poderão ser customizadas pela aplicação de filtros, de forma que seja simples e rápida a obtenção de dados necessários para auditoria sobre os arquivos, pastas, usuários, grupos de segurança e e-mails dos serviços monitorados.

4.1.6.5 Deve ser possível alterar também o conjunto de dados (colunas) retornados da consulta de auditoria de acordo com a necessidade da informação.

4.1.6.6 Todos os eventos dos diferentes servidores monitorados devem ser apresentados na mesma console gráfica da solução onde são também apresentadas as informações de permissionamento desses mesmos servidores monitorados.

4.1.6.7 A solução deve fornecer resumo das atividades auditadas, incluindo:

4.1.6.7.1 Quantidade de eventos por dia;

4.1.6.7.2 Visualização dos usuários mais e menos ativos nos servidores monitorados;

4.1.6.7.3 Visualização dos diretórios mais e menos acessados nos servidores monitorados;

4.1.6.7.4 Visualização dos diretórios e pastas acessadas por um usuário ou grupo de segurança;

4.1.7 IDENTIFICAÇÃO E CLASSIFICAÇÃO DE CONTEÚDOS SENSÍVEIS

4.1.7.1 As soluções requeridas deverão possuir possibilitar a inspeção o conteúdo dos arquivos sem escopo em busca de palavras, termos, expressões regulares, valores, e identificar informações sensíveis para o negócio;

4.1.7.2 A solução deve identificar dados sensíveis nas plataformas Windows;

4.1.7.3 A solução deve exibir na mesma interface gráfica as informações sobre os permissionamentos, ACL's, quantidade de informações sensíveis e qual tipo de informação sensível classificada, a fim de facilitar a identificação de potenciais repositórios e pastas superexpostos;

4.1.7.4 A solução deve gerar, em forma de relatórios, dados sobre a classificação das informações;

4.1.7.5 A solução deve ter a capacidade de incluir filtros relativos à classificação dos dados nas pesquisas dos logs;

4.1.7.6 A solução deve ter a capacidade de incluir filtros relativos à classificação dos dados nos relatórios de acesso;

4.1.7.7 Para cada arquivo marcado como sensível, as soluções devem possibilitar a visão, diretamente da ferramenta, das expressões regulares ou caracteres que fizeram com que esse arquivo fosse considerado como sensível;

4.1.7.8 A solução deve fornecer visibilidade de conteúdo crítico de negócio através da classificação da informação;

4.1.7.9 A ferramenta deve fornecer visibilidade dos locais que possuem dados sensíveis;

4.1.7.10 A solução deve possibilitar a instalação da funcionalidade de classificação de dados sensíveis nos mesmos servidores onde serão instaladas as funcionalidades de auditoria, sem a necessidade de servidores adicionais, diminuindo assim o esforço e custo da solução integrada;

4.1.7.11 A solução deve fornecer a funcionalidade de busca de arquivos através de palavras-chave, frases e expressões regulares;

4.1.7.12 A ferramenta deve permitir integração com ferramentas de DLP (Data Loss Prevention) de classificação de dados sensíveis e informar em relatório onde estes dados se encontram dentro do sistema de arquivos da solução;

4.1.7.13 Deve ser possível definir o agendamento da classificação com hora de início e fim, frequência em que a busca ocorrerá e data em que deve parar, para que não haja impacto no ambiente;

4.1.7.14 A solução deverá fazer a descoberta de dados sensíveis nos servidores de arquivos Windows on-premise monitorados e nos repositórios OneDrive e Sharepoint On-line na nuvem do Office 365.

4.1.8 SOLUÇÃO BASEADA EM SOFTWARE DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO PARA AUDITORIA E OUTRAS FUNCIONALIDADES DE SERVIÇO DE DIRETÓRIO (MICROSOFT ACTIVE DIRECTORY).

4.1.8.1 Requisitos Gerais

4.1.8.1.1 As funcionalidades descritas nas características gerais devem se aplicar à solução para os serviços de diretórios de usuários do Microsoft *Active Directory*.

4.1.8.1.2 A solução descrita neste item deve possuir as seguintes funcionalidades globais:

4.1.8.1.3 Auditar ações sobre objetos do Active Directory;

4.1.8.1.4 O software ofertado deve ter um compressor de dados para não onerar a banda;

4.1.8.1.5 O software ofertado deve ser capaz de coletar os dados de forma nativa para a fonte de dados auditada;

4.1.8.1.6 Reter as informações de histórico em banco de dados por um período de acordo com a necessidade do solicitante;

4.1.8.1.7 Ser capaz de rastrear as atividades dos usuários e administradores com informações detalhadas, incluindo quem, o que, quando, onde, qual estação de trabalho, para os eventos de alteração, além dos valores originais e atuais para todas as mudanças;

4.1.8.1.8 Gerar alerta com base nas informações auditadas;

4.1.8.1.9 Monitorar e analisar comportamentos suspeitos de usuários;

4.1.8.1.10 Possuir painel que consolide métricas e indicadores relevantes do ambiente para entender o impacto na segurança geral da TI;

4.1.8.1.11 Permitir agendamento de relatórios;

4.1.8.1.12 Permitir salvar ou exportar os relatórios nos formatos; Excel, PDF, HTML e CSV;

4.1.8.1.13 Permitir a filtragem dos relatórios de acordo com o objeto auditado;

4.1.8.1.14 Permitir a criação de relatórios personalizado com informações inerentes do próprio ambiente;

4.1.8.1.15 Permitir acesso para auditores poderem executar pesquisas e relatórios, sem fazer quaisquer alterações de configuração para a aplicação, sem necessidade de assistência e tempo dos administradores;

4.1.8.1.16 Permitir o agendamento para envio de relatórios por e-mail e em uma determinada

pasta do servidor sem a necessidade de customização adicional;

4.1.8.1.17 O envio dos relatórios por e-mail deve ser feito a partir da própria solução, sem a utilização de software de terceiros e deve suportar o protocolo SMTP;

4.1.8.1.18 Possibilitar relatórios customizáveis sob demanda e agendados;

4.1.8.1.19 Ser capaz de fornecer relatórios para auditoria e conformidade (compliance).

4.1.8.2 A solução deve oferecer a visibilidade gráfica da estrutura hierárquica de todos os domínios, OUs e objetos monitorados no AD da agência, apresentados na mesma console em que apresenta seus logs de auditoria.

4.1.8.3 A solução deverá suportar árvore funcional do Active Directory 2012 ou superior.

4.1.8.4 A solução deve suportar a demonstração gráfica e a auditoria de diferentes domínios.

4.1.8.5 Funcionalidade: auditar ações sobre objetos do Active Directory

4.1.8.5.1 A solução deverá fornecer informações detalhadas de auditoria para perícia em relação aos seguintes pontos:

4.1.8.5.1.1 Quem pode acessar e qual acesso pode fazer aos objetos do AD;

4.1.8.5.1.2 Quem faz alteração nos objetos (usuários, grupos, GPO) com a identificação do autor da criação, modificação e remoção de contas de usuário com data e hora dos eventos;

4.1.8.5.1.3 Permitir auditar a atividade de autenticação (autenticação interativa, interativa remota e logons de rede incluindo logons com sucesso e falhos realizados nos servidores monitorados;

4.1.8.5.1.4 Identificação de contas de usuário bloqueadas com data e hora dos eventos, incluindo endereços IP de origem e destino ou nome dos computadores de origem e destino;

4.1.8.5.1.5 Identificação da última autenticação de conta de usuário no Active Directory com data, hora e origem (IP ou nome computador) dos eventos;

4.1.8.5.1.6 Identificação de autenticações em computadores por conta de usuário com data e hora dos eventos, incluindo endereço IP ou nome computador;

4.1.8.5.1.7 Detalhes dos eventos sobre objetos;

4.1.8.5.1.8 Quem possui permissões sobre os objetos;

4.1.8.5.1.9 Quem deu ou revogou permissões de acesso e modificação.

4.1.8.5.1.10 A solução deverá ser capaz de rastrear quem fez alterações nos usuários, grupos, OUs e GPOs dos domínios monitorados do Active Directory, qual foi a alteração feita, quando foi feita, a máquina de origem da alteração e detalhes das propriedades tanto do objeto afetado quanto do objeto que gerou o evento.

4.1.8.5.1.11 A solução deverá indicar graficamente ou por relatório usuários ativos e inativos, usuários habilitados e desabilitados no AD.

4.1.8.5.1.12 A solução deve suportar a auditoria dos eventos do serviço de diretório, tais como:

4.1.8.5.1.13 Criação e deleção de todos os objetos;

4.1.8.5.1.14 Alteração de membros de grupos;

4.1.8.5.1.15 Alteração nas propriedades dos objetos do serviço de diretório;

4.1.8.5.1.16 Requisições de acesso;

4.1.8.5.1.17 Autenticação de conta;

4.1.8.5.1.18 Reconfiguração de senhas;

4.1.8.5.1.19 Bloqueio e desbloqueio de conta;

4.1.8.5.1.20 Criação e deleção de conta;

4.1.8.5.1.21 Habilitação e desativação de conta;

4.1.8.5.1.22 Eventos de permissão adicionada ou removida de objeto;

4.1.8.5.1.23 Proprietário alterado;

4.1.8.5.1.24 Identificação de autor de criação, modificação e remoção de objetos de unidades organizacionais com data e hora dos eventos;

4.1.8.5.1.25 A solução deve permitir realizar o Roll-back de alterações no servidor Active Directory sejam objetos ou configurações.

4.1.8.6 Funcionalidade: gerar alerta com base nas informações auditadas

4.1.8.6.1 A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail quando aquela ação específica ocorrer novamente.

a) A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

b) Atividades anômalas;

c) Grupos de segurança, GPO's e outros objetos de Active Directory modificados ou removidos;

d) Escalações de privilégios não autorizadas;

e) Detecção atividades que indiquem a utilização de ferramentas de intrusão ou malwares, como acesso e modificação de muitos arquivos em um pequeno espaço de tempo.

4.1.8.6.2 O sistema de alerta em tempo real deve ser capaz de alarmar atividades em Active Directory (elevação de privilégios, inclusão/exclusão de grupos e usuários).

4.1.8.6.3 A solução deve permitir a integração com sistemas de e-mail padrão de mercado para

envio de e-mails (alertas, notificações) de forma automática, ou manual.

4.1.8.7 Funcionalidade: monitorar e analisar os comportamentos suspeitos de usuários

4.1.8.7.1 Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.

4.1.8.7.2 A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas monitoradas.

4.1.8.7.3 Através da análise comportamental, solução deve realizar a descoberta automática de contas privilegiadas como usuários administrativos e contas de serviço.

4.1.8.7.4 Deve ser contemplada a assinatura de uma base de conhecimentos do fornecedor atualizada mensalmente de alertas pré-configurados de eventos suspeitos tais como:

- a) Detecção de ferramentas nocivas ao ambiente;
- b) Excessos de ações com acessos negados;
- c) Acessos indevidos dos administradores nos dados da empresa;
- d) Excessivas tentativas de elevação de privilégios;
- e) Excesso de tentativas de autenticação ou contas bloqueadas;
- f) Alterações excessivas e anormais em GPO;
- g) Excesso de ações em um curto espaço de tempo.

4.1.8.7.5 A solução deve entregar painel de controle (Dashboard) que permita análise dos comportamentos e eventos suspeitos listados:

- a) Quantidade de alertas e suas severidades em determinado período;
- b) Usuários se comportando de forma suspeita;
- c) Tipos de alertas mais disparados;

4.2.1.2. A página com lista dos eventos deve apresentar gráfico que demonstre o quantitativo dos eventos em determinado período, para que seja possível identificar o desvio do comportamento indicado pela solução.

4.1.8.7.6 A solução deve possuir relatórios com os principais indicadores de performance dos servidores e recursos monitorados (AD, File Servers e Office 365) com informações essenciais para a gestão, e a partir desses indicadores, deve ser possível abrir a lista de informações detalhadas, tais como:

4.1.8.7.6.1 Quantidade de usuários habilitados inativos, usuários desabilitados, usuários habilitados com senhas expiradas, usuários habilitados bloqueados, grupos vazios, grupos não-administrativos com usuários administradores;

4.1.8.7.6.2 Número total de grupos de segurança, contas de usuários e computadores;

4.1.8.8 Funcionalidade: relatórios:

4.1.8.8.1 A solução deve fornecer os seguintes relatórios:

- a) Auditoria de contas de usuário do Active Directory;
- b) Auditoria de grupos do Active Directory;
- c) Auditoria de GPOs (Objetos de Diretivas de Grupo) do Active Directory;
- d) Auditoria de contas de computadores do Active Directory;
- e) Auditoria de OU (Unidades Organizacionais) do Active Directory;
- f) Auditoria de autenticação de contas de usuário no Active Directory;
- g) Auditoria de autenticação de computadores no Active Directory;
- h) Indicativos de uso de dados para a gestão de usuários, grupos de segurança e objetos do AD;
- i) Relatórios de logon/logoff de usuários;
- j) Logs de acessos e modificações de objetos do AD, com detalhamento dos eventos e metadados dos objetos afetados;
- k) Alterações em grupos de segurança dos domínios monitorados;
- l) Alterações em contas de usuários e de computador;
- m) Alterações em descrição, membros (associação direta e indireta) de grupos;
- n) Alterações em grupos monitorados;
- o) Usuários inativos no domínio;
- p) Grupos de segurança vazios ou não utilizados;
- q) Usuários desabilitados que ainda fazem parte de grupos de segurança;
- r) Histórico de membros de grupos de segurança;
- s) Estatísticas de autenticação e falha de autenticação;
- t) Lista de usuários administradores em grupos não administrativos;
- u) Recomendações de revogação de permissões dos usuários calculadas pela análise comportamental;

- v) Informações sobre as alterações, versão alterada e quais foram as mudanças realizadas emGPOs dos domínios monitorados;
- w) Auditoria das alterações do AD por Controlador de Domínio;
- x) Auditoria de todas as alterações do Active Directory em grupo, tipo de objeto e usuário;
- y) Auditoria de alterações no site, em container de configuração e esquema do Active Directory;
- z) Auditoria de alterações na associação de grupos administrativos;
- aa) Auditoria de alterações na conta do computador;
- bb) Auditoria de alterações no grupo de distribuição;
- cc) Auditoria de alterações no controlador de domínio;
- dd) Auditoria de alterações de relação de confiança de domínio;
- ee) Auditoria em contas de usuários.

4.1.9 SOLUÇÃO BASEADA EM SOFTWARE DE SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO PARA AUDITORIA E OUTRAS FUNCIONALIDADES DE SERVIDORES DE ARQUIVOS.

4.1.9.1 Requisitos gerais

4.1.9.1.1 As funcionalidades descritas nas características gerais (item 4.2) devem se aplicar para a solução de servidores de arquivos Windows.

4.1.9.1.2 A solução descrita neste item deve possuir as seguintes funcionalidades globais:

- a) Auditar acesso, criação, modificação e remoção de pastas e arquivos em servidores de arquivos, com data e hora dos eventos;
- b) Possibilitar a identificação de conteúdo inserido e modificado;
- c) Executar ações com base na auditoria, inclusive para múltiplos objetos;
- d) Gerar alerta com base nas informações auditadas;
- e) Capacidade de fazer buscas, gerar relatórios e alertar mudanças ocorridas em um arquivo específico, pasta, pasta compartilhada ou drives monitorados;
- f) Gerar alerta com base nas informações auditadas e receber alertas em tempo real quando alguém tenta acessar algum arquivo ou pasta protegido de um servidor Windows;
- g) Rastrear eventos relacionados aos compartilhamentos e arquivos;
- h) Monitorar e analisar comportamentos suspeitos de usuários.

4.1.9.1.3 A solução deve suportar servidores virtuais de arquivos com a versão Windows

Server2016 ou superior.

4.1.9.1.4 A solução deve oferecer, a partir da console, as funcionalidades de visibilidade e alteração de permissionamento das pastas dos repositórios monitorados além de monitorar os usuários que possuem permissão de criação de pastas e permissões para que a gestão do repositório seja centralizada.

4.1.9.1.5 A interface gráfica da solução deverá permitir a busca por um usuário ou grupo de segurança e deverá apresentar suas permissões e pastas dos servidores monitorados. As informações apresentadas incluem:

- a) Identificação de herança de permissão ativada/desativada;
- b) Indicação de existência de compartilhamento;
- c) A fonte da permissão, ou seja, de que grupo o usuário está herdando a permissão.

4.1.9.2 Funcionalidade: gerar alerta com base nas informações auditadas

4.1.9.2.1 A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada para que seja disparado um e-mail, seja gerado syslog, eventlog, SNMP ou que seja executado um script quando aquela ação específica ocorrer novamente.

4.1.9.3 A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

- a) Atividades anômalas;
- b) Acesso a dados sensíveis;
- c) Arquivos sensíveis acessados ou excluídos;
- d) Escalações de privilégios não autorizadas;
- e) Modificação de permissões em diretórios sensíveis;
- f) Identificação de ações que indiquem o uso de ferramentas de intrusão ou malwares.

4.1.9.4 A solução de alerta em tempo real deve ser capaz de alarmar atividades em arquivos (deleção, abertura, movimentação, acessos negados, entre outras).

4.1.10 Funcionalidade: monitorar e analisar os comportamentos suspeitos de usuários

4.1.10.1 Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão dos recursos monitorados, para que desvios e anomalias nesses comportamentos sejam identificados automaticamente e alertados em tempo real.

4.1.10.2 A solução deve ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar eventos anormais que tenham ocorrido nas plataformas

monitoradas.

4.1.10.3 A solução deve oferecer relatório dos alertas de comportamento anômalo identificados nos arquivos, pastas e diretórios dos servidores monitorados.

4.1.10.4 O painel deve possuir página com os principais indicadores e métricas do serviço de compartilhamento de arquivos com informações essenciais para a gestão. Deve também apresentar a quantidade e tamanho total dos arquivos e pastas.

4.1.10.5 A solução deve atender todas as características comuns descritas nesta funcionalidade.

4.1.11 Funcionalidade: relatórios

4.1.11.1 A solução deve fornecer os seguintes relatórios:

- a) Indicativos de uso de dados para a gestão de arquivos e pastas;
- b) Logs de acessos e modificações de arquivos e pastas, com detalhamento dos eventos e metadados dos objetos afetados;
- c) Todas as modificações de permissionamento dos diretórios e pastas dos servidores monitorados feitas através da interface gráfica da solução ou feitas de forma manual diretamente nos servidores de arquivos;
- d) Pastas e diretórios dos servidores de arquivos monitorados onde há permissões concedidas a grupos de segurança globais (Everyone, Users ou Authenticated Users);
- e) Pasta ou de todas as pastas do servidor que tenham permissão direta aplicada a usuários;
- f) Dados inativos ou sem utilização no domínio;
- g) Histórico de permissões nas pastas e diretórios monitorados;
- h) Lista de pastas críticas com permissões excessivas nos servidores monitorados;
- i) Lista de permissões em pastas dos servidores monitorados de usuários desabilitados;
- j) Pastas dos servidores monitorados sem permissões de administradores;
- k) Recomendações de revogação de permissões dos usuários calculadas pela análise comportamental;
- l) Estatística de acesso às pastas, utilização por tipo de arquivo, eventos por usuário e distribuição por tipos de evento sobre os servidores monitorados;
- m) Auditoria de todas as atividades do servidor de arquivos por tipo de ação, servidor e usuário;
- n) Auditoria de arquivos e pastas criados, movidos, excluídos, renomeados e copiados;
- o) Listagem de arquivos duplicados e pastas vazias;

4.1.11.2 Os relatórios devem possibilitar a exportação pelo menos nos formatos CSV, PDF,

Excel, Arquivo XML;

4.1.12 Solução baseada em software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades em Microsoft 365 (Exchange Online, Teams, Sharepoint, OneDrive)

4.1.12.1 Requisitos gerais,

4.1.12.1.1 As funcionalidades descritas nas características gerais devem se aplicar às ferramentas do Microsoft 365 (Exchange Online, Teams, Sharepoint e OneDrive) e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados não estrutura dos monitorados.

4.1.12.1.2 solução descrita neste item deve possuir as seguintes funcionalidades globais:

- a) Auditar acesso, modificação e remoção de caixas postais e listas do ambiente de correio eletrônico;
- b) Auditar acesso e compartilhamento para usuários externos nos arquivos e pastas disponibilizadas no OneDrive;
- c) Auditar acesso e compartilhamentos de páginas do Sharepoint para usuários externos;
- d) Gerar alerta com base nas informações auditadas;
- e) Monitorar e analisar comportamentos suspeitos de usuários;
- f) Gerar relatórios sobre o ambiente do Office 365.

4.1.12.2 Funcionalidade: auditar acesso, modificação e remoção de objetos no Office 365

4.1.12.2.1 A solução deverá coletar os seguintes eventos no Exchange Online:

- a) Mailbox criada, aberta, deletada ou renomeada;
- b) Permissão em mailbox adicionada ou removida;
- c) Encaminhamento de mensagens adicionado ou removida para mailbox;
- d) Permissão em pasta de mailbox adicionada, removida ou alterada;
- e) Pasta de mailbox movida ou esvaziada;
- f) Mensagem enviada “em nome de” (on behalf of);
- g) Mensagem enviada “como” (“As”);
- h) Mensagem deletada ou movida;
- i) Informação de logon em mailbox;

4.1.12.2.2 A solução deverá coletar os seguintes eventos no Sharepoint:

- a) Criação ou remoção de páginas;
- b) Adição ou remoção de permissões em páginas;
- c) Adição ou remoção de donos de páginas.
- d) Adição ou remoção de arquivos/pastas/bibliotecas;
- e) Concessão ou remoção de permissões em arquivos/pastas/bibliotecas;
- f) Compartilhamento de arquivos/pastas/bibliotecas com usuários externos;
- g) Compartilhamento de arquivos/pastas/bibliotecas com permissão "Anônima".

4.1.12.2.3 A solução deverá coletar os seguintes eventos no OneDrive:

- a) Adição ou remoção de arquivos/pastas;
- b) Concessão ou remoção de permissões em arquivos/pastas/bibliotecas;
- c) Compartilhamento de arquivos/pastas/bibliotecas com usuários externos;
- d) Compartilhamento de arquivos/pastas/bibliotecas com permissão "Anônima".

4.1.12.3 Funcionalidade: gerar alerta com base nas informações auditadas e executar ações proativas, inclusive para múltiplos objetos

4.1.12.3.1 A solução deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitados para que seja disparado um e-mail, seja gerado syslog, eventlog, SNMP e que seja executado um script quando aquela ação específica ocorrer novamente.

4.1.12.3.2 A solução deve ser capaz de enviar alertas em tempo real dos seguintes tipos:

- a) Atividades anômalas;
- b) Acesso a dados sensíveis;
- c) Identificação de ações que indiquem o uso de ferramentas de intrusão ou malwares.
- d) O sistema de alerta em tempo real deve ser capaz de alarmar as atividades listadas no item 4.5.1 nas ferramentas Office 365.

4.1.12.4 Funcionalidade: relatórios

4.1.12.4.1 A solução deve fornecer os seguintes relatórios:

- a) Indicativos de uso de dados para a gestão de contas Office 365.
- b) Logs de acessos e modificações de contas, com detalhamento dos eventos e metadados dos objetos afetados.
- c) Modificações de permissionamento das contas feitas através da interface gráfica da solução

ou feitas de forma manual diretamente via powershell.

d) Estatística de acesso aos objetos da plataforma, eventos por usuário e distribuição por tipos de evento.

e) Modificações em contas e objetos monitorados.

4.1.12.5 Serviço de instalação e treinamento

4.1.12.5.1 A instalação e configuração inicial de todos os componentes da solução deverão ser feitas com o acompanhamento de equipe técnica designada pela AFEAM.

4.1.12.5.2 O treinamento será composto por todos os módulos que compõem a solução oferta da que deve consistir na oferta de cursos remotos, e com abordagem prática voltada a todos os requisitos funcionais da solução, devendo abordar de forma teórica e prática todas as funcionalidades solicitadas para as soluções contratadas.

4.1.12.5.3 As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência do Contrato.

4.1.12.5.4 Com objetivo de capacitar os servidores da área de TI da AFEAM, que atuam no suporte à solução, quanto aos procedimentos de instalação, atualização, configuração e operação das funcionalidades da solução a ser implantada na AFEAM, assim como quanto aos procedimentos de solução de problemas, é integrante desta contratação a prestação do serviço de treinamento prático(hands-on).

4.1.12.5.5 A CONTRATADA deverá obrigatoriamente estruturar duas modalidades de treinamento prático:

a) Treinamento prático de instalação e configuração (pré-instalação) – com vistas à capacitação dos profissionais da AFEAM sobre os procedimentos de instalação e configuração dos equipamentos e softwares, assim como os requisitos operacionais e de infraestrutura necessários para sua implantação. Desta forma, os profissionais da AFEAM terão condições de acompanhar, avaliar e validar os procedimentos e processos do plano de implantação da solução.

b) Treinamento prático de operação, gerenciamento e resolução de incidentes e problemas (pós-instalação) – com vistas à capacitação dos profissionais da AFEAM quanto aos procedimentos continuados de uso da solução, englobando todas as atividades de manutenção e atualização, procedimentos de salva e restauração (back-up), gerenciamento dos arquivos de registro da solução (logs), dentre outras aplicáveis para a operação diária do ambiente e na resolução de incidentes e problemas.

4.1.12.5.6 Os treinamentos deverão ser realizados no período da manhã, das 8:30h às 11:30h, ou no período da tarde, das 13:30h às 16:30h, a critério da AFEAM. Cada turma poderá ter até 10 participantes, a serem indicados pela AFEAM.

4.1.12.5.7 O ambiente de treinamento poderá ser composto pelos softwares que serão fornecidos pela CONTRATADA;

4.1.12.5.8 A modalidade do curso será de forma não-presencial (EAD - Ensino a Distância), desde que as condições de imersão e a qualidade de conexão e das ferramentas (lousa virtual, chat, gravação) disponibilizadas pela CONTRATADA sejam aprovadas pela AFEAM para a prestação do serviço.

4.1.12.5.9 Toda a infraestrutura de transmissão remota do treinamento, caso essa seja a opção, será de responsabilidade da CONTRATADA. A AFEAM e seus servidores serão responsáveis apenas pelas próprias conexões de internet e equipamentos em cada local.

4.1.12.5.10 A carga horária total de cada turma de treinamento é de até 20 horas, em datas acordadas com a AFEAM.

4.1.12.5.11 Serão demandadas duas turmas, sendo uma de pré-instalação e outra de pós-instalação, todas deverão ser ministradas antes da emissão do Termo de Recebimento Definitivo da Solução - TRD.

4.1.12.5.12 A CONTRATADA deverá fornecer material eletrônico com conteúdo programático orientado em procedimentos passo a passo e por telas das interfaces de administração e configuração do ambiente. Todo o material didático proposto deverá ser aprovado pela equipe de fiscalização e gestão do Contrato.

4.1.12.5.13 O material deverá ser fornecido em formato eletrônico editável para permitir futuras alterações e atualizações por parte da AFEAM.

4.1.12.5.14 Esse treinamento deverá ser ministrado por instrutor(es) devidamente qualificado(s), com comprovação documental de que possui(em) capacitação e competências para atuar(em) como instrutor(es) do treinamento prático da solução ofertada.

4.1.12.5.15 A capacitação poderá ser comprovada por meio de declarações ou certificações emitidas pelos fabricantes ou por meio de experiência profissional, mediante apresentação de atestados ou referências de treinamentos ministrados em outros clientes, que possam ser diligenciadas pela AFEAM.

4.1.12.5.16 A AFEAM, após o recebimento da agenda, material didático e demais comprovações, avaliará a documentação em até 10 (dez) dias corridos e, caso seja necessária alguma adequação no material/instrutores, a CONTRATADA terá até 3 (três) dias corridos, após ser comunicada, para realizar os ajustes e apresentar o novo material/instrutores. Esse processo de revisão pela AFEAM e ajuste pela CONTRATADA poderá ocorrer múltiplas vezes.

4.1.12.5.17 Após o término das interações entre a AFEAM e a CONTRATADA, será estabelecida, em acordo pelas partes, a data para início do treinamento.

4.1.12.5.18 Concluídas as atividades de treinamento, a CONTRATADA fornecerá a cada

participante que obteve, no mínimo, 80% de presença, um certificado de conclusão que contenha, expressamente, o nome da instituição organizadora, a carga horária do treinamento, o local, o período de realização e o nome completo do participante.

4.1.12.5.19 A AFEAM disponibilizará os recursos mencionados no subitem acima à CONTRATADA até 3 (três) dias úteis antes da data agendada para início do treinamento, de modo que seja possível, nesse prazo, preparar adequadamente o ambiente previamente à realização das aulas.

4.1.12.5.20 Todo o material de treinamento entregue, disponibilizado e utilizado pela CONTRATADA para a execução dos serviços de treinamento, incluindo o material de apoio, como apresentações, apostilas, manuais, vídeos de demonstração, dentre outros correlatos, serão concedidos com direito de uso e de reprodução à AFEAM, de forma irrestrita, para sua aplicação e uso em treinamentos internos para funcionários da AFEAM.

4.1.12.5.21 A CONTRATADA, caso demandado pela AFEAM, deverá providenciar a gravação das aulas em vídeo no formato digital.

4.1.12.5.22 A qualidade do treinamento deverá ser avaliada por seus participantes ao seu final e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a Autarquia.

4.1.12.5.23 A avaliação dos treinamentos deverá levar em consideração as questões listadas a seguir:

4.1.12.5.24 Avaliação do conteúdo:

- a) Adequação dos conteúdos aos objetivos propostos;
- b) Adequação das atividades desenvolvidas para alcance dos objetivos propostos;
- c) Adequação do tempo para o alcance dos objetivos propostos;
- d) Profundidade com que o conteúdo foi abordado, considerando os objetivos propostos;
- e) Integração entre teoria, pesquisa, prática e/ou aspectos da realidade;
- f) Qualidade dos exemplos utilizados;
- g) Aplicabilidade dos conhecimentos adquiridos no trabalho;
- h) Contribuição para melhoria do desempenho no trabalho;
- i) Qualidade do material instrucional (apostilas, gráficos etc.).

4.1.12.5.25 Avaliação do instrutor:

- a) Formas/métodos de apresentação dos conteúdos;
- b) Conhecimento dos temas tratados;

- c) Visão prática dos conteúdos tratados;
- d) Uso de estratégias para motivar os alunos em relação ao conteúdo;
- e) Incentivo à participação dos alunos em sala de aula;
- f) Incentivo à realização de atividades adicionais de aprofundamento do aprendizado.

4.1.12.5.26 Avaliação de ambiente e recursos

- a) Qualidade dos recursos tecnológicos utilizados pelo instrutor (áudio, vídeo, recursos para demonstração, etc);
- b) Qualidade do ambiente virtual disponibilizado para o curso.
- c) Qualidade da conexão disponibilizada pela contratada.

4.1.12.5.27 Cada participante deverá indicar uma nota de 1 a 10 para cada item e letra da avaliação.

4.1.12.5.28 A nota do treinamento será calculada pela média das respostas de todos os itens e letras, e de todos os participantes indicados pela AFEAM.

4.1.12.5.29 O treinamento será considerado com qualidade suficiente, caso atinja uma nota igual ou superior a 8.

4.1.12.5.30 Para comprovação da nota do treinamento, deverá ser encaminhado o detalhamento do cálculo realizado pela contratada, juntamente com uma cópia dos formulários preenchidos pelos participantes.

4.1.12.5.31 Caso alguns dos prazos previstos e acordados para a execução do treinamento não sejam cumpridos por responsabilidade da contratada, ela estará sujeita às sanções previstas no termo de referência.

4.1.13 SUPORTE TÉCNICO E GARANTIA

4.1.13.1 Deverá ser provido o serviço de suporte para atendimento, suporte, esclarecimento de dúvidas e resolução de falhas de software que não sejam cobertos pela garantia do fabricante nos termos dessa seção.

4.1.13.2 A prestação do serviço de suporte durante o prazo de vigência estabelecido no Termo de Referência e abrangerá todos os itens de softwares que foram fornecidos em atendimento ao objeto e deverá ser prestado nos prazos e tempo de resolução de acordo com níveis de serviços estabelecidos no presente termo.

4.1.13.3 Os serviços de suporte técnico e garantia abrangem:

4.1.13.3.1 Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

4.1.13.3.2 Transferência de conhecimento aos técnicos da AFEAM referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes;

4.1.13.3.3 Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante;

4.1.13.4 Toda despesa com seus técnicos deverá estar contemplada na proposta de preços;

4.1.13.5 Os serviços de suporte técnico e garantia abrangem todas as soluções fornecidas pela contratada no âmbito dessa contratação.

4.1.13.6 Os produtos adquiridos devem ser licenciados de forma que o suporte e a garantia permitam as atualizações dos sistemas e ferramentas durante a vigência do contrato. Deverão estar incluídas tanto as atualizações de segurança, quanto as atualizações para novas versões dos softwares licenciados, quando disponibilizadas, independente da política de comercialização do fabricante.

4.1.13.7 Todas os sistemas ou ferramentas que fazem parte da solução deverão ser disponibilizados na versão mais recente disponibilizada pelo fabricante.

4.1.13.8 A CONTRATADA deverá designar um profissional responsável pelo acompanhamento das solicitações de suporte abertas pela CONTRATANTE. Caberá a este profissional supervisionar os técnicos da CONTRATADA responsáveis pelo atendimento dos chamados abertos pela CONTRATANTE. Este profissional será o contato oficial da CONTRATANTE com a CONTRATADA para assuntos relativos aos serviços de suporte técnico. A comunicação da CONTRATANTE com esse profissional será realizada obrigatoriamente em português do Brasil;

4.1.13.9 O serviço de suporte técnico estará sujeito aos níveis de serviço especificados neste TR. - Garantia dos Bens e Serviços e Critérios de Aceitação - Níveis Mínimos de Serviço.

4.1.14 CANAIS DE COMUNICAÇÃO

4.1.14.1 Para abertura de solicitações a CONTRATADA deverá disponibilizar, no mínimo, dois tipos de canais de comunicação, a saber:

TABELA 1 - TIPOS DE CANAIS DE COMUNICAÇÃO

Tipo	Grupo de Tecnologia	Classificação
1	E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 1
2	Sistema de ITSM do inglês <i>Information Technology Service Management</i> (Gerenciamento de Serviços de TI).	Tipo 2

4.1.14.2 Independente do canal de comunicação utilizado pelo CONTRATANTE, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI). Ou

seja, caso a abertura de chamado se dê por via e-mail, este deve ser tratado na mesma ferramenta disponibilizada para a abertura direta.

4.1.14.3 A CONTRATADA deverá disponibilizar endereço de correio eletrônico (e-mail) e portal web para acionamento do serviço de suporte técnico, que deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

4.1.14.4 A CONTRATADA deverá disponibilizar acesso para a CONTRATANTE ao sistema de abertura e fechamento de tickets para que seja possível extrair relatórios gerenciais de tickets.

4.1.15 HORÁRIO DE ATENDIMENTO

4.1.15.1 O serviço de suporte técnico deverá estar disponível 8 (oito) horas por dia, 5 (cinco) dias da semana (dias úteis), e englobará todos os recursos e procedimentos necessários para que a solução implantada na AFEAM retorne ao seu estado normal de operação;

4.1.15.2 Dias úteis são aqueles ocorridos entre segunda e sexta-feira, exceto feriados nacionais;

4.1.16 ENTREGA DE SERVIÇOS

4.1.16.1 A CONTRATADA deve disponibilizar guias e procedimentos para aplicar as atualizações de versão e melhorias da solução no ambiente da AFEAM quando efetivamente for necessário em função de atualização crítica para o funcionamento da solução, ou para alguma parametrização necessária para atender ao negócio, contados do Termo de Recebimento Definitivo (TRD), e durante todo o prazo de vigência do contrato.

4.1.16.2 Todos os acessos e alterações no ambiente para a resolução de incidentes e problemas na infraestrutura da AFEAM poderão ser executados através de atendimento remoto;

4.1.16.3 A CONTRATADA deverá fornecer credencial de acesso à CONTRATANTE para os sistemas do fabricante que estejam relacionados a procedimentos de suporte, webinars e perguntas mais frequentes, caso seja disponibilizado este tipo de sistema por parte do fabricante e seja necessária credencial de acesso.

4.1.16.4 A CONTRATADA deve garantir que todas as personalizações e configurações realizadas, caso ocorram, sejam automaticamente portadas para novas versões em caso de atualização, reinstalação ou upgrade, dispensando a necessidade de migrações ostensivas e onerosas.

4.1.16.5 Considerar-se-á como tempo de resolução do chamado o período compreendido entre a abertura do chamado através de telefone ou e-mail junto à CONTRATADA e a resolução final do mesmo, que deverá ser aprovada pela AFEAM;

4.1.16.6 Ao final da abertura de cada atendimento de suporte, a CONTRATADA deverá emitir e informar um ticket do chamado técnico contendo, no mínimo:

- 4.1.16.6.1** Número do chamado;
- 4.1.16.6.2** Data e hora de abertura do chamado;
- 4.1.16.6.3** Previsão de conclusão do atendimento;
- 4.1.16.6.4** Severidade do erro;
- 4.1.16.6.5** Descrição da solicitação;
- 4.1.16.7** A CONTRATADA deverá disponibilizar relatórios de chamados por período, contendo, no mínimo, as seguintes informações:
 - 4.1.16.7.1** Número do chamado;
 - 4.1.16.7.2** Data e hora de abertura do chamado;
 - 4.1.16.7.3** Data e hora do início do tratamento do chamado;
 - 4.1.16.7.4** Data e hora de resolução do chamado;
 - 4.1.16.7.5** Prazo Total de Início do Tratamento do Chamado (ITC);
 - 4.1.16.7.6** Prazo Total de Resolução do Chamado (PRC)
 - 4.1.16.7.7** Início do Tratamento do Chamado (ITC) cumprido (Sim/Não);
 - 4.1.16.7.8** Prazo para Resolução do Chamado (PRC) cumprido (Sim/Não);
 - 4.1.16.7.9** Contato do técnico atendente;
 - 4.1.16.7.10** Responsável pelo registro do chamado;
 - 4.1.16.7.11** Severidade do chamado;
 - 4.1.16.7.12** Descrição da solicitação;
 - 4.1.16.7.13** Solução aplicada;
- 4.1.16.8** Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o fechamento deste. Caso a CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetiva mente solucionado pela CONTRATADA. Nesse caso, a CONTRATANTE fornecerá as pendências relativas ao chamado aberto.
- 4.1.17 MODALIDADE DE ATENDIMENTO**
 - 4.1.17.1** A modalidade principal de atendimento será do tipo remota, ou seja, a ser realizada por meio das dependências da CONTRATADA, obrigatoriamente obedecendo os critérios estabelecidos para sua execução, no presente termo de referência.
 - 4.1.17.2** O modelo de acesso remoto ao ambiente da AFEAM será acordado com a

CONTRATADA durante a vigência do contrato.

4.1.17.3 A CONTRATANTE poderá registrar um número ilimitado de chamados de suporte durante a vigência do Contrato.

4.1.17.4 Estima-se o registro de uma quantidade maior de solicitações de suporte durante os primeiros 8 meses de contrato e a diminuição do quantitativo de solicitações nos meses seguintes.

ACESSIBILIDADE E CONFIDENCIALIDADE

4.1.17.5 A CONTRATADA deve assinar e entregar ao CONTRATANTE na data de reunião de assinatura do contrato termo de confidencialidade e sigilo, que será disponibilizado pela AFEAM. Esse documento estabelecerá as condições para a prestação dos serviços acerca do sigilo das informações custodiadas, do acesso restrito das informações aos técnicos designados no projeto e da propriedade intelectual de todos os produtos e conhecimento advindos da execução.

4.1.17.6 Além disso, o termo de confidencialidade e sigilo deve ser reconhecido e assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato, sendo que o CONTRATANTE pode solicitar, a qualquer momento, a comprovação dessa obrigação. O respectivo termo deve ser entregue antes do início das atividades.

4.1.17.7 Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, empregadas na prestação de serviços ao CONTRATANTE, bem como solicitar a revogação destas ao CONTRATANTE, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

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

4.1.18 EXECUÇÃO DOS SERVIÇOS

4.1.18.1 A CONTRATADA deverá atender às seguintes condições gerais para início de prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de cronograma de execução, planejamento de atividades de instalação, customização de ambiente e ativação de serviços, sem ônus adicionais ao CONTRATANTE:

4.1.18.1.1 Serão de responsabilidade da CONTRATADA as atividades de instalação, integração, configuração e testes dos produtos ofertados, em conformidade com o cronograma de execução a ser elaborado e apresentado pela CONTRATADA para aprovação da AFEAM;

4.1.18.1.2 A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Cronograma de execução, e verificar eventuais requisitos

físicos a serem providos para a correta instalação e prestação dos serviços;

4.1.19 DA DOCUMENTAÇÃO SUPLEMENTAR

4.1.19.1 Deverá ser disponibilizado manuais do fabricante com o seguinte conteúdo mínimo:

- a) Fabricante: Nome do fabricante da licença;
- b) Modelo: código e nome das licenças;
- c) Fabricação: Versão e data do último release da licença; Suporte: Endereço na Internet (site) do fabricante onde seja possível a obtenção de literatura técnica (especificações detalhadas, consumíveis, FAQ e etc.) e drivers atualizados;

4.1.19.2 Os manuais do usuário (formato digital) deverão ser adaptados aos requisitos e à arquitetura tecnológica da AFEAM em língua portuguesa (Brasil) ou inglesa, com informações detalhadas e atualizadas sobre a instalação, configuração, operação e administração para cada componente da solução e que demonstrem o atendimento aos requisitos técnicos deste Termo.

4.1.19.3 Os manuais deverão estar disponíveis em site público na internet para consulta a qualquer momento. Caso não seja possível, deverá ser confirmada a veracidade das informações por meio de declaração fornecida pelo fabricante destinada ao AFEAM e com referência explícita a este processo de aquisição.

4.2 Informar necessidade de visita técnica:

4.2.1. Não há necessidade de visita técnica para este objeto.

5. FORMA DE CONTRATAÇÃO: MODALIDADE

5.1. Modalidade de licitação:

5.1.1 Será adotada o Procedimento na modalidade Similar ao Pregão Eletrônico.

5.2. Critério de julgamento das propostas:

5.2.1. O critério de julgamento será o de **MENOR PREÇO GLOBAL**.

5.3. Critério de adjudicação/ seleção do fornecedor

5.3.1. O critério de adjudicação será global.

5.4. Opção pela utilização ou não do Sistema de Registro de Preços

5.4.1. Não será utilizado o Sistema de Registro de Preços.

5.5. Permissão ou vedação quanto à participação de consórcios

5.5.1. Não será permitida a participação de consórcios.

5.6. Permissão ou vedação quanto à participação de cooperativas;

5.6.1. Será permitida a participação de cooperativas.

6. ACOMPANHAMENTO E RECEBIMENTO DO OBJETO

6.1. Pelas características do objeto, não haverá necessidade de recebimento provisório;

6.2. A gestão e a fiscalização do contrato consistirão na verificação da conformidade da sua esmerita execução e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento das obrigações pactuadas, devendo ser exercida pelo gestor do contrato designado pela CONTRATANTE, que poderá ser auxiliado pelo fiscal técnico e pelo fiscal administrativo, cabendo ao responsável legal ou preposto da CONTRATADA o acompanhamento dessas atividades;

6.3. O recebimento definitivo do objeto se dará através da análise e aprovação dos seguintes documentos:

I. Nota fiscal/Fatura correspondente aos Serviços prestados (objeto deste Termo de Referência), de forma continuada, referente ao período em que o serviço foi prestado, contendo, de forma física ou acesso virtual, demonstrativo dos valores referentes à prestação dos serviços no período de apuração, com indicação do número de todas as linhas habilitadas e consumo correspondente;

II. Recibo, que poderá ser substituído por comprovante de pagamento emitido pelo financeiro da AFEAM;

III. Prova de regularidade com o INSS, mediante a apresentação da Certidão Negativa de Débitos Relativos aos Tributos Federais e a Dívida Ativa da União, e do FGTS, mediante apresentação do Certificado de Regularidade do FGTS – CRF, ambos em validade.

7. VALOR ESTIMADO DA CONTRATAÇÃO

7.1. O valor estimado para esta licitação é sigiloso, na forma do art. 34 da Lei nº 13.303/2016.

8. FORMA DE PAGAMENTO

8.1. O pagamento será efetuado após cada fornecimento efetuado em até 10 (dez) dias úteis após a apresentação da Nota Fiscal e ateste do fiscal técnico do contrato, que se dará mediante a apresentação dos documentos elencados no item 6.3 deste Termo.

9. REAJUSTE

9.1 Os preços registrados poderão ser alterados, por reajuste, apenas depois de decorridos 12 (doze) meses, nos termos do artigo 190 e ss. c/c artigo 140 inciso VIII do RILC AFEAM.

9.2 O prazo mencionado no subitem 9.1 será contado a partir da data da proposta ou do orçamento a que ela se referir, nos casos de reajuste.

9.3 Os valores contratuais serão reajustados com base no Índice Nacional de Preços ao Consumidor Amplo (IPCA/IBGE).

9.4 Havendo necessidade de revisão por eventos imprevisíveis, caso fortuito ou força maior, com vistas a restabelecer o equilíbrio econômico-financeiro do contrato, após a devida comprovação e demonstração analítica dos fatos e dos novos custos pelas partes, a mesma poderá ser feita mediante aditamento contratual, obedecidos os procedimentos constantes do artigo 200 c/c artigo 140 inciso VIII do RILC AFEAM.

10. PRAZO DE EXECUÇÃO E DE VIGÊNCIA

10.1 O prazo de execução do serviço será o mesmo prazo de vigência contrato, de 12 (doze) meses, podendo ser prorrogado, mediante termo aditivo, até o limite de 5 (cinco) anos, de acordo com o artigo 71, da Lei nº 13.303, de 2016.

11. REGIME DE EXECUÇÃO

11.1. Os serviços serão executados sob o regime de empreitada por preço global.

12. AMOSTRAS

12.1. Não haverá exigência de amostras para a presente contratação.

13. OBRIGAÇÕES DA CONTRATADA

13.1. Cumprir fielmente o objeto do contrato;

13.2. Entregar os produtos de acordo com o pactuado;

13.4. Indicar nome e telefone para comunicação e notificação para atendimento das demandas, bem como esclarecimentos de dúvidas de qualquer natureza quanto aos produtos objeto do contrato;

13.5. Manter, durante a execução do contrato, em compatibilidade com as obrigações por ela assumidas, as condições de habilitação e qualificação exigidas no curso do procedimento licitatório;

13.6. Fornecer e colocar à disposição da CONTRATANTE todos os elementos e informações que se fizerem necessárias à consecução do objeto do contrato;

13.7. Guardar sigilo absoluto sobre dados e informações contidos nos arquivos, documentos ou em qualquer outro sistema de informações a que tiverem acesso;

13.8. Reparar, corrigir, no total ou em parte, o objeto deste contrato, em que se verificarem incorreções resultantes da execução;

13.9. Apresentar a licença ambiental ou dispensa, caso não seja obrigada pela atividade que exerce;

13.10. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do objeto pela CONTRATANTE, bem como por toda e qualquer alteração relativa a incidência de impostos, não cabendo à CONTRATANTE qualquer ônus ou ação judicial;

13.11. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo

representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

13.12. Pagar todos os tributos, contribuições fiscais, trabalhistas e previdenciárias que incidem ou venham a incidir, direta ou indiretamente, sobre o objeto do contrato.

14. OBRIGAÇÕES DA CONTRATANTE

14.1. Permitir à CONTRATADA executar o objeto do contrato;

14.2. Prestar as informações e os esclarecimentos solicitados pela CONTRATADA para a boa e fiel execução do objeto do contrato;

14.3. Acompanhar e fiscalizar a execução do objeto do contrato e efetuar os pagamentos nas condições e preços pactuados, dentro dos prazos preestabelecidos em contrato;

14.4. Receber o objeto fornecido pela contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

14.5. Nomear Fiscais Técnico e Administrativo, bem como seus substitutos do contrato para acompanhar e fiscalizar a execução dos contratos;

14.6. Rejeitar o objeto executado em desacordo com as obrigações assumidas pela CONTRATADA, exigindo imediata correção ou substituição do objeto do contrato em que se verificarem vícios, defeitos ou incorreções na execução, sob pena de aplicação das penalidades previstas em lei e no contrato, ressalvados os casos fortuitos ou de força maior, justificados e aceitos pela CONTRATANTE;

14.7. Comunicar à CONTRATADA toda e qualquer ocorrência relevante relacionada com o objeto do contrato;

14.8. Realizar as retenções legais e recolhê-las para os órgãos competentes.

15. EXIGÊNCIAS PARA CONTRATAÇÃO

15.1. Critérios de Habilitação Jurídica

15.1.2. A documentação relativa à habilitação jurídica, conforme o caso consistirá em:

I. pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

II. empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

III. 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>;

IV. sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social

no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

V. sociedade empresária 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, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

VI. sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

VII. 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;

VIII. os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

IX. Para representação por meio de instrumento de procuração, a empresa com proposta de menor preço deverá apresentar, além da documentação pessoal do procurador, o Instrumento Particular ou Público de Procuração, em validade, que deve outorgar ao representante, poderes gerais para a prática de todos os atos inerentes ao Procedimento Similar ao Pregão Eletrônico, especialmente para formular ofertas e lances de preços, em nome da empresa representada. No caso de Instrumento particular de procuração, deverá ficar comprovado que o subscritor da procuração tem poderes para tal delegação por meio de cópia autenticada do contrato social e ou outro documento constitutivo.

15.2. Critérios de Qualificação Técnica

15.2.1. Serão solicitadas as seguintes documentações para a comprovação de qualificação técnica:

I. 1 (um) ou mais atestado(s) de capacidade técnica fornecido(s) por pessoa jurídica de direito público ou privado informando que o licitante já executou objeto compatível e pertinente em características, quantidades e prazos com o objeto da licitação e deverão referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificadas no contrato social vigente do licitante;

a) com relação à quantidade dos atestados a que se refere o inciso I do subitem 15.2, deverá demonstrar que o licitante executa ou executou contratos em atividades pertinentes e compatíveis com o objeto da licitação, que correspondam a 50% (cinquenta por cento), do quantitativo total de itens;

b) para atendimento do critério de quantidade constante no parágrafo anterior, poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico operacional, a uma única contratação.

c) com relação ao prazo de execução dos serviços, deverá ser comprovado que o licitante já executou objeto em contratação semelhante, pelo mesmo prazo de vigência inicial do contrato estipulado em

instrumento convocatório, ininterruptos ou não, ou seja, 12 (doze) meses.

II. Como condição para atender os requisitos dos itens do presente lote, a licitante vencedora deverá apresentar até a assinatura do contrato, os documentos da qualificação técnico-operacional em processos de serviços de TI:

a) Declarar que possuir ou possuirá no mínimo 1 (um) profissional com certificação técnica do fabricante da solução de que fornecerá a este órgão no âmbito da presente contratação.

15.3. Critérios de Qualificação Econômico-Financeira

15.3.1. A documentação relativa à qualificação econômico-financeira limitar-se a:

I. apresentação de certidão negativa de feitos sobre falência, recuperação judicial ou recuperação extrajudicial, expedida pelo cartório distribuidor da sede do licitante.

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

15.3.2. A comprovação da boa situação financeira da empresa será feita por meio da apresentação dos índices abaixo, podendo ser apresentada por meio de Declaração de Capacidade Financeira:

- a) Índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um);
- b) Caso não atendido os índices na forma do item anterior, comprovar capital mínimo ou Patrimônio Líquido igual ou superior a 10% (dez por cento) do valor estimado da contratação.

15.4. Regularidade Fiscal

15.4.1. A documentação relativa à regularidade fiscal consistirá em:

I. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ, ou no Cadastro de Pessoas Físicas – CPF, conforme o caso;

II. Prova de regularidade com o INSS, mediante a apresentação da Certidão Negativa de Débitos relativos aos Tributos Federais e à Dívida Ativa da União; e,

III. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), mediante a apresentação do Certificado de Regularidade do FGTS (CRF).

16. CONTRATO

16.1. As cláusulas referentes à presente contratação estarão descritas na Minuta do Instrumento equivalente ao Contrato, anexo do Edital de Procedimento na Modalidade Similar ao Pregão Eletrônico.

17. CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

17.1. Não se aplica por não haver compatibilidade com o objeto.

18. PENALIDADES

18.1. Pelo atraso ou pela inexecução total ou parcial injustificados do objeto do contrato, a CONTRATANTE poderá, garantida a prévia defesa, aplicar à CONTRATADA as seguintes sanções:

I. advertência;

II. multa, na forma prevista neste Contrato; e

III. suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE, por até 2 (dois) anos.

18.2. As sanções previstas nos incisos I e III, do item 18.1, poderão ser aplicadas juntamente com a do inciso II.

18.3. A aplicação da sanção de advertência importa em sua comunicação à CONTRATADA, devendo ser informada no sistema cadastral correspondente ou no Sistema de Cadastramento Unificado de Fornecedores - SICAF, bem como ocorrer o seu registro junto aos documentos contratuais.

18.3.1. A reincidência da sanção de advertência, poderá ensejar a aplicação da penalidade de suspensão do direito de participar de licitação e impedimento de contratar com a AFEAM e/ou a aplicação de multa no valor de até 5% (cinco por cento) do valor do contrato, sem prejuízo da rescisão contratual.

18.4. No caso de inexecução parcial, incidência de multa de 10% (dez por cento) sobre o valor da parcela inadimplida ou do saldo remanescente do contrato, a depender do inadimplemento, conforme avaliação da AFEAM;

18.5. No caso de inexecução total, incidência de multa de 20% (vinte por cento) sobre o valor total do contrato, conforme avaliação da AFEAM;

18.6. A sanção de multa será aplicada na execução do contrato, quando a CONTRATADA cometer alguma das infrações constantes da “Tabela 1 - Grau de infrações”, respeitada a dosimetria atribuída a sua respectiva gravidade, assim como os percentuais de multa dos graus de infração, por tempo de incidência ou ocorrência, constantes na “Tabela 2 - Valor das Infrações por Grau”;

Tabela 1: Grau das Infrações

ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU
01	Permitir situação que crie a possibilidade de causar dano físico, lesão corporal ou consequências letais.	04
02	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, a entrega dos produtos e/ou serviços contratuais.	03
03	Manter empregado sem qualificação para executar os serviços contratados.	03
04	Recusar-se a executar serviço determinado pela fiscalização.	02

05	Deixar de zelar pelas instalações da CONTRATANTE utilizadas.	03
06	Utilizar as dependências da AFEAM para fins diversos do objeto do contrato.	03
07	Retirar das dependências da CONTRATANTE qualquer equipamento ou material que não seja de sua propriedade ou que esteja previsto em contrato, sem autorização prévia do gestor/fiscal do contrato.	03
08	Deixar de cumprir determinação formal ou instrução complementar da CONTRATANTE.	02
09	Deixar de atender às demandas e solicitações da CONTRATANTE nos prazos e horários estabelecidos em Comunicados, no Edital e seus Anexos.	02
10	Deixar de cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta tabela de multas.	01
11	Deixar de cumprir quaisquer dos itens do Edital e seus Anexos não previstos nesta Tabela de multas, após reincidência formalmente notificada pela CONTRATANTE.	02
12	Não entregar a amostra do equipamento ou produto, quando solicitado.	02
13	Não entregar os equipamentos, produtos e/ou prestar os serviços contratados na data avençada.	04
14	Paralisação da obra, serviço ou fornecimento sem justa causa e prévia comunicação à CONTRATANTE.	04
15	Reincidir em qualquer das infrações cometidas, após notificação da CONTRATANTE, por item e por ocorrência.	04

Tabela 2: Aplicação de multas para serviços comuns ou aquisições:

GRAU	CORRESPONDÊNCIA
01	0,1% por dia ou ocorrência, sobre o valor mensal do contrato
02	0,3% por dia ou ocorrência, sobre o valor mensal do contrato
03	0,6% por dia ou ocorrência, sobre o valor mensal do contrato
04	1,0% por dia ou ocorrência, sobre o valor mensal do contrato

18.7. A sanção de suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE será aplicada nos casos estabelecidos no artigo 245 do Regulamento Interno de Licitações e Contratos da AFEAM – RILC AFEAM, disponível no seguinte endereço eletrônico: <<http://www.afeam.am.gov.br/>>, na forma estabelecida nos artigos 252 a 256.

19. GARANTIA

19.1. A fim de garantir a fiel observância dos serviços prestados e dos termos do contrato, a CONTRATADA deverá apresentar, no prazo de 10 (dez) dias úteis contados da assinatura do contrato, garantia correspondente a 3% (três por cento) do valor contratado, representada por caução em dinheiro, seguro-garantia ou fiança bancária.

19.2. No caso de garantia em dinheiro, a CONTRATADA deverá depositar o valor referente na seguinte conta da CONTRATANTE: banco: 237 (Bradesco); agência 3734 (Parque Dez); conta corrente nº: 5050-4, enviando o comprovante para o correio eletrônico: nf@afeam.org.br.

19.3. Na hipótese de renovação contratual, a garantia deverá ser atualizada e apresentada à CONTRATANTE, no mesmo prazo e percentual estabelecido no caput deste artigo.

19.4. A CONTRATANTE estará autorizada a proceder com a retenção preventiva da garantia contratual em função da execução do contrato, quando assim se fizer necessário, para evitar prejuízo decorrente do inadimplemento contratual da CONTRATADA.

19.5. Se a garantia for utilizada em pagamento de qualquer obrigação, a CONTRATADA se obrigará a fazer a respectiva reposição, no prazo máximo de 48h (quarenta e oito horas), a contar da data em que for notificada pela CONTRATANTE.

19.6. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

19.6.1. Prejuízo advindo do não cumprimento do contrato, parcial ou total, e do não adimplemento das demais obrigações nele previstas;

19.6.2. Prejuízos causados à CONTRATANTE ou a terceiro decorrentes de culpa ou dolo durante a execução do contrato; e,

19.6.3. Sanções contratuais e legais de qualquer natureza, aplicadas pela CONTRATANTE à CONTRATADA.

19.7. A garantia prestada pela CONTRATADA será liberada ou restituída após a execução e expedição do termo de recebimento definitivo do objeto contratual e, quando em dinheiro, atualizada monetariamente com base na variação do índice da caderneta de poupança.

19.8. A devolução da garantia do contrato será feita mediante a apresentação dos seguintes documentos:

19.8.1. Atesto do fiscal do contrato na última parcela referente ao serviço prestado ou objeto adquirido pela CONTRATANTE, sem que o mesmo tenha identificado qualquer obrigação pendente por parte da CONTRATADA; e,

19.8.2. Quando a resolução do contrato ocorrer sem que haja culpa da CONTRATADA.

19.9. O não cumprimento ou atraso injustificado da exigência prevista nos subitens 19.1 e 19.4 ensejará a aplicação de sanções administrativas constantes neste contrato e no RILC da AFEAM.

19.10. Poderá ser entendido como não cumprimento da exigência prevista no subitem 19.1 o atraso injustificado na apresentação de garantia que perdure até o limite da multa estabelecida no subitem 18.4.1 deste Termo de Referência.



20. APROVAÇÃO

20.1. A Equipe de Planejamento da Contratação declara que este Termo de Referência está de acordo com a Lei nº 13.303/2016, bem como com o RILC-AFEAM.

Manaus, 23 de setembro de 2024.

Jaderclei da Costa Nogueira
Especialista de Fomento – GETI
Mat. 686

José Alves Pereira Neto
Gerente – GETI
Mat. 245

Márcia Campelo da Silva
Assessora/GEPEC
Mat. 596

Ívia Victória Monteiro Lima de Mattos
Especialista de Fomento/GEPEC
Mat. 784

De acordo,

Manaus, de de 2024.

Aprovação da Área Administrativa

JAQUES DOUGLAS MOTA GONÇALVES
Gerente da GERAD

APROVO,

Manaus, de de 2024.

Autoridade Competente

MARCOS VINICIUS CARDOSO DE CASTRO
Diretor-Presidente