TERMO DE REFERÊNCIA

PROCESSO DE GESTÃO ADMINISTRATIVO Nº 19.21.0016.0019441/2024-94

HISTÓRICO DE REVISÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
10/07/2024	1.0	Primeira versão do documento.	Marcos Maciel Martins Brito
26/08/2024	2.0	Versão com ajustes	Marcos Maciel Martins Brito
03/10/2024	3.0	Correções solicitadas pela CLC	Marcos Maciel Martins Brito
20/01/2025	4.0	Correções solicitadas pela ASSPROCLI	Marcos Maciel Martins Brito
28/01/2025	4.1	Correção no item 15	Marcos Maciel Martins Brito

1. OBJETO DA CONTRATAÇÃO

1.1. O objeto da presente licitação é o **registro de preço, pelo prazo def 12 (doze) meses**, para eventual contratação de empresa para fornecimento de solução de segurança da informação, visando a aquisição de uso de software de Gestão e Controle de Contas de Usuários Privilegiados (PAM - *Privileged Access Management*) e ferramenta de segurança, auditoria, e prevenção de ameaças à base de dados não estruturados, incluindo licenciamento através de subscrição por um período mínimo de 36 (trinta e seis) meses, instalação, configuração, manutenção, suporte técnico e treinamento, a fim de atender as necessidades do Ministério Público do Estado do Piauí, conforme requisitos técnicos, níveis de qualidade e quantidades descritas neste termo.

2. DESCRIÇÃO DA SOLUÇÃO DE TI

2.1. AUDITORIA DE DADOS NÃO ESTRUTURADOS

O alto volume de dados e arquivos armazenados nos repositórios de Tecnologia da Informação do MPPI e as novas exigências impostas pela legislação vigente (Lei de Acesso à Informação e Lei Geral de Proteção de Dados, por exemplo) exigem o aperfeiçoamento dos processos de controle, gestão e governança dos dados.

Atualmente essa classificação e controle é feita de forma manual, sem uma ferramenta que otimize esse processo e garanta a integridade e a privacidade dos dados. Ressalta-se que, quanto a classificação, é necessário um controle mais efetivo quanto ao acesso a estes dados, principalmente no comportamento do usuário que os consome/consulta e acessa arquivos armazenados no ambiente do MPPI.

Como descrito, esse controle manual afeta diretamente as boas práticas de gestão e governança, não permitindo sequer uma auditoria de dados adequada. A aquisição de uma ferramenta que permita melhorar o controle de acesso, a classificação e atue monitorando atividades suspeitas, alertando comportamentos estranhos por parte de usuários e objetos a que têm acesso a arquivos e dados armazenados no ambiente do MPPI, garante não só o uso de boas práticas de auditoria, controle, gestão e governança de dados como gera também uma camada extra de segurança da informação, auxiliando na prevenção de possíveis ataques que acarretam em prejuízos ao órgão.

2.2. GERENCIAMENTO DE ACESSO PRIVILEGIADO

As soluções de Gestão de Acesso Privilegiado (PAM - Privileged Access Management) permitem a gestão de credenciais de contas privilegiadas, protegendo-as em um repositório seguro (cofre de senhas), permitem também a gravação das sessões privilegiadas e a trilha de ações dos usuários com relatórios. Proativamente é possível mitigar ações que contém ameaças realizadas pelos usuários através de análise comportamental e proteção para sistemas críticos. Possuem a capacidade de gerência de acesso remotos seguros, troca de senhas, rotação de chaves criptográficas (SSH) e de credenciais/secrets embarcadas nas aplicações containerizadas e tradicionais. Além disso, implementam proteção para as estações de trabalho, controladores de domínios e servidores, com a possibilidade de elevação de privilégio para

determinados serviços e remoção de administração local para mitigar roubo de credencias (técnica de overpass-the-hash).

Para embasar a identificação das empresas que atendem as necessidades da solução, validando na prática o seu uso e suas funcionalidades foram realizadas duas Provas de Conceito (POC) com as soluções SenhaSegura e BeyondTrust. Verificou-se que os resultados das POC atenderam nossas espectativas, pois as soluções demonstraram atender as necessidades elencadas.

2.3. DA SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

A solução visa melhorar em diversos aspectos a segurança da informação no MPPI, visto que com o advento da Lei 13.709/2018 (Lei Geral de Proteção de Dados) houve a necessidade do órgão de buscar ainda mais soluções para colaborar com a proteção dos dados, bem como a sua governança e gestão, dessa forma conforme preconiza o art. 19, VI, da resolução CNMP nº 283/2024, a solução é composta por ferramenta de cofre de senhas (que visa manter as credenciais sensíveis que acessam dados em local seguro, estruturado, contando com auditoria e gestão) , bem como ferramenta de análise de dados estruturados, buscando realizar a governança dos dados dentre outras funcionalidades já mencionadas no item 2.1.

Entendemos que a solução possui ferramentas que se complementam, e irão preencher lacunas que atualmente possuímos ligadas a segurança da informação, incrementando as ferramentas já existentes e diminuindo as possibilidades ataques bem sucedidos a infraestrutura e usuários do MPPI, tanto através de proteção de credenciais quanto no monitoramento de dados da instituição.

Além disso , visando a plena qualificação da empresa fornecedora que prestará os serviços de instalação e configuração, bem como prestará os serviços de suporte durante a vigência do contrato de garantia dos equipamentos, a total compatibilidade entre os equipamentos solicitados, a redução de custos operacionais e de infraestrutura física, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total.

2.4. BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

GRUPO 1 - ITENS 1 A 6				
Item	**Descrição**	**CATSER**	**Unidade de fornecimento**	**Qtd**
1	Licença para visibilidade, análise de dados locais, comportamento e prevenção de ameaças por 36 meses	**24333**	Usuários	1600
2	Licença para visibilidade, análise de dados em nuvem, comportamento e prevenção de ameaças por 36 meses	**24333**	Usuários	1600
3	Licença para visibilidade, análise de dados em caixas postais, comportamento e prevenção de ameaças por 36 meses	**24333**	Usuários	1600
4	Serviço de instalação e configuração para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	**26972**	Serviço	2
5	Manutenção e Suporte Técnico para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	**26972**	Serviço	2
6	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	**3840**	Turma	2
GRUPO 2 - ITENS 7 A 17				

7	Cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses	**469726**	Unidade	2
8	Balanceador de carga para cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses	**469726**	Unidade	2
9	Subscrição para usuários com acesso privilegiado por 36 meses	**24333**	Usuários	40
10	Subscrição para servidores físicos e virtuais por 36 meses	**24333**	Servidores	400
11	Subscrição para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN por 36 meses	**24333**	Equipamentos	1000
12	Subscrição para aplicações não conteinerizadas com senha embutida (hard coded) por 36 meses	**24333**	Aplicações	80
13	Subscrição para acesso remoto seguro por 36 meses	**24333**	Unidade	60
14	Subscrição de gerenciamento de certificados digitais por 36 meses	**24333**	Unidade	2
15	Serviço de instalação e configuração para solução de controle de acesso de usuários privilegiados.	**26972**	Serviço	2
16	Manutenção e Suporte Técnico para solução de controle de acesso de usuários privilegiados.	**26972**	Serviço	2
17	Treinamento para solução de controle de acesso de usuários privilegiados.	**3840**	Turma	2

2.5. ESPECIFICAÇÃO TÉCNICA DO OBJETO

2.5.1. GRUPO 1

2.5.1.1. AUDITORIA DE DADOS NÃO ESTRUTURADOS

2.5.1.1.1. A solução deverá monitorar todos os domínios e servidores de arquivos Microsoft do ambiente, incluindo: Contas, estruturas de diretórios, permissões e eventos;

2.5.1.1.2. 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;

2.5.1.1.3. O gerenciamento da solução deverá ser centralizado para todos os módulos;

2.5.1.1.4. A solução deverá monitorar todos os domain controllers instalados em qualquer versão do Windows Server 2012 e superior;

2.5.1.1.5. A solução deverá monitorar todos os servidores de arquivos instalados em versões do Windows Server 2012 e superior;

2.5.1.1.6. A solução deverá monitorar no mínimo, os seguintes eventos do Microsoft Active Directory:

a) Conta habilitada e desabilitada;

b) Autenticação de conta (TGT);

c) Renovação de acesso (TGS);

d) Replicação de AD;

e) Logon de conta no DC;

f) Criação, deleção, renomeação, modificação, remoção e adição de membros no objeto do DS;

g) Requisição de acesso NTLM;

h) Alteração de senha de usuário;

i) Conta de usuário bloqueada;

j) Conta de usuário desbloqueada;

k) Netlogon vulnerável;

l) Criação, deleção e modificação de GPO;

m) Tentativa de reset de senha;

n) Criação, atualização, deleção, habilitação e desabilitação de tarefa agendada dentro do DC;

o) Alteração de política de kerberos;

2.5.1.1.7. A solução deverá monitorar no mínimo, os seguintes eventos do servidor de Arquivos Windows:

a) Arquivo criado;

b) Arquivo deletado;

c) Arquivo aberto;

d) Arquivo renomeado;

e) Arquivo modificado;

f) Mudança de proprietário do arquivo;

g) Permissões adicionadas no arquivo;

h) Permissões removidas no arquivo;

i) Proteção adicionado no arquivo;

j) Proteção removida no arquivo;

k) Pasta criada;

l) Pasta deletada;

m) Pasta renomeada;

n) Mudança de proprietário da pasta;

o) Permissões adicionadas na pasta;

p) Permissões removidas na pasta;

q) Proteção adicionada na pasta;

r) Proteção removida na pasta;

2.5.1.1.8. Deverá ser possível definir os proprietários das pastas através da console;

2.5.1.1.9. 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;

2.5.1.1.10. A solução deverá exibir o repositório monitorado em formato hierárquico, 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;

2.5.1.1.11. 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);

2.5.1.1.12. A solução deverá disponibilizar a visibilidade de permissões, sejam elas NTFS ou share;

2.5.1.1.13. A solução deverá realizar a classificação do conteúdo do arquivo, fornecendo visibilidade sobre onde residem os dados confidenciais e sensíveis no sistema de arquivos;

2.5.1.1.14. A solução deverá utilizar múltiplos fatores para realizar a classificação do conteúdo do arquivo, incluindo: Metadados, padrões, dicionários, palavras-chave e expressão regular;

2.5.1.1.15. 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;

2.5.1.1.16. A solução deverá fornecer filtros para visualizar apenas determinados objetos de dados em exibição gráfica interativa, incluindo pastas protegidas e pastas únicas;

2.5.1.1.17. 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;

2.5.1.1.18. A solução deverá fornecer para as permissões, tipos de exibição diferentes, incluindo exibições hierárquicas e de lista;

2.5.1.1.19. A solução deverá realizar a classificação de imagens através de OCR ou tecnologia similar;

2.5.1.1.20. 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;

2.5.1.1.21. Deve ser possível realizar o agendamento do escaneamento das regras de classificação, podendo especificar: horário, dia e tempo de duração;

2.5.1.1.22. Deve ser possível exportar eventos e informações apenas referente aos dados classificados como sensíveis;

2.5.1.1.23. 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;

2.5.1.1.24. 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;

2.5.1.1.25. A solução deverá encontrar em arquivos com formato tabular, palavras chaves em cabeçalhos e colunas;

2.5.1.1.26. 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;

2.5.1.1.27. A solução deverá possuir funcionalidade que exiba o conteúdo classificado como sensível na console, indicando os trechos do documento que correspondem à regra especificada;

2.5.1.1.28. A solução deverá notificar os administradores através de alertas para qualquer tipo de atividade incomum e comportamentos suspeitos de usuários;

2.5.1.1.29. 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;

2.5.1.1.30. 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:

a) Ataques de sequestro de dados (ransomware);

b) Detecção de ferramentas nocivas ao ambiente;

c) Ações com acessos negados;

d) Ações de escalações de privilégios;

e) Excesso de tentativas de autenticação ou contas bloqueadas;

f) Atividades suspeitas em dados parados e/ou inativos;

g) Alterações anormais em GPO;

h) Ataques de golden ticket;

i) Ataques de injeção de códigos maliciosos;

j) Ataques de decoberta de contas com NTLM e Kerkeros;

k) Ataques de força bruta;

2.5.1.1.31. Os modelos de alertas devem ser atualizados de forma automática;

2.5.1.1.32. A solução deverá suportar a configuração de respostas automáticas para os alertas gerados, possibilitando a execução automática de scripts ou comandos pré-configurados;

2.5.1.1.33. Os alertas da solução deverão ser encaminhados no mínimo, via SMTP e SNMP;

2.5.1.1.34. Deve ser possível exportar logs para ferramentas de SIEM através de Syslog;

2.5.1.1.35. A solução deverá auxiliar na conformidade com a LGDP, 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;

2.5.1.1.36. A solução deverá construir perfis de comportamento comparando as atividades dos usuários e entidades e identificando a relação entre eles;

2.5.1.1.37. 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;

2.5.1.1.38. A solução deverá detectar ameaças em todos os estágios de um ataque cibernético, incluindo dashboard que indica algumas categorias como: Reconhecimento, intrusão, exploração, escalação de privilégio, movimento lateral, negação de serviço e exfiltração de dados;

2.5.1.1.39. 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;

2.5.1.1.40. 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;

2.5.1.1.41. A solução deverá possuir dashboard de alertas indicando os usuários mais alertados, dispositivos e modelos de alertas gerados;

2.5.1.1.42. 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.

2.5.1.1.43. 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;

2.5.1.1.44. As políticas de automação para remediação devem ser executadas de forma manual e automática;

2.5.1.1.45. A solução deverá suportar na busca dos eventos a utilização de operadores relativos, auxiliando na investigação e nos resultados esperados;

2.5.1.1.46. 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;

2.5.1.1.47. 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;

2.5.1.1.48. A solução deverá identificar dados que não foram acessados por um período de tempo, podendo especificar a quantidade de dias desejado;

2.5.1.1.49. 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;

2.5.1.1.50. 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;

2.5.1.1.51. A solução deverá possuir dashboards com indicadores de riscos mais importantes do ambiente monitorado, e outras métricas através de widgets.

2.5.1.1.52. A solução deverá possuir dashboards com widgets referente aos repositórios monitorados, incluindo dashboard de alertas, compliance, servidores de arquivos e do serviço de diretórios;

2.5.1.1.53. Deve ser possível comparar os gráficos do dashboard através da console, indicando a diferença dos valores atuais com o período anterior;

2.5.1.1.54. Deve ser possível exportar os dashboards através da console incluindo a comparação do dashboard atual com outro de período anterior;

2.5.1.1.55. 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;

2.5.1.1.56. A solução deverá possuir Widget de geolocalização com mapa indicando a origem da ação para os alertas gerados;

2.5.1.1.57. Deverá ser possível fazer o drill-down a partir dos widgets até chegar no evento gerado;

2.5.1.1.58. Deverá ser possível realizar pesquisas em cima dos repositórios monitorados, incluíndo: Eventos, alertas, permissões, contas e recursos;

2.5.1.1.59. Através da pesquisa realizada deve ser possível criar um relatório com os dados apresentados no resultado;

2.5.1.1.60. 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.

2.5.1.1.61. Deve ser possível visualizar os eventos de todos os recursos monitorados;

2.5.1.1.62. Todos os eventos podem ser filtrados e organizados no mínimo por: tipo de evento, ID do evento, operação, status e plataforma;

2.5.1.1.63. Deve ser possível definir uma data e horário para busca dos eventos;

2.5.1.1.64. A solução deverá possuir filtro para última atividade registrada do usuário, facilitando a busca de contas que estão atualmente inativas;

2.5.1.1.65. Deve ser possível encaminhar os eventos gerados da pesquisa para e-mail externos a organização;

2.5.1.1.66. Deve ser possível exportar o relatório em no mínimo 3 tipos de formatos: CSV, Excel e PDF;

2.5.1.1.67. A solução deverá possuir tela para visualização para todos os eventos coletados, através de um período específico, em formato de tabela, com filtros e colunas customizáveis;

2.5.1.1.68. Deve possuir insights com os dados mais importantes de acordo com a pesquisa;

2.5.1.1.69. Deverá ser possível realizar o agendamento de relatórios;

2.5.1.1.70. Deverá ser possível encaminhar o relatório apenas para o proprietário do dado;

2.5.1.2. AUDITORIA DE DADOS NÃO ESTRUTURADOS PARA NUVEM

2.5.1.2.1. A solução deverá monitorar repositórios de nuvem como M365 (Entra ID, Sharepoint Online e OneDrive) e Google Drive, correlacionando identidades com privilégios, atividades, reduzindo riscos e acelerando investigações;

2.5.1.2.2. A solução deverá monitorar, no mínimo, os seguintes eventos do Entra ID:

a) Conta desativada e ativada;

b) Aplicativo adicionado;

c) Consentimento do aplicativo aprovado e removido;

d) Proprietário do aplicativo adicionado e removido;

e) Aplicativo removido e atualizado;

f) Dispositivo adicionado;

g) Proprietário do dispositivo adicionado e removido;

h) Usuário registrado do dispositivo adicionado;

i) Usuário registrado do dispositivo removido;

j) Dispositivo removido e atualizado;

k) Grupo adicionado e excluído;

l) Conjunto de licenças de grupo;

m) Membro do grupo adicionado e removido;

n) Proprietário do grupo adicionado e removido;

o) Grupo atualizado, login;

p) Função do membro adicionada e removida;

q) Usuário adicionado e excluído;

r) Usuário convidado para a organização;

s) Licença de usuário alterada;

t) Usuário restaurado e atualizado;

2.5.1.2.3. A solução deverá monitorar, no mínimo, os seguintes eventos do Sharepoint Online e One Drive:

a) Malware detectado no arquivo;

b) Solicitação de acesso a arquivos aprovada;

c) Arquivo copiado e excluído;

d) Arquivo baixado para uma pasta local sincronizada;

e) Arquivo baixado;

f) Convite de arquivo aceito, cancelado, criado, e atualizado;

g) Arquivo modificado, movido, aberto, renomeado, e restaurado;

h) Link compartilhado de arquivo criado, removido, atualizado e usado;

i) Arquivo enviado;

j) Arquivo enviado de uma pasta local sincronizada;

k) Solicitação de acesso à pasta aprovada;

l) Pasta copiada , criada, excluída;

m) Convite de pasta aceito, cancelado, criado e atualizado;

n) Pasta movida, renomeada, restaurada;

o) Link compartilhado da pasta criado, removido, atualizado, usado, excluído;

p) Membro do grupo adicionado e removido;

q) Permissões adicionadas;

r) Herança de permissão quebrada e restaurada;

s) Permissões removidas;

t) Administrador do conjunto de sites adicionado e removido;

v) Mudança geográfica do site agendada e concluída;

2.5.1.2.4. 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;

2.5.1.2.5. A solução deverá encaminhar uma notificação via e-mail para os usuários responsáveis pela aprovação das políticas de automação, um link para revisão e aprovação das políticas;

2.5.1.2.2. Deve ser possível exportar logs para ferramentas de SIEM através de Syslog;

2.5.1.2.7. A solução deverá monitorar e detectar quando um usuário realizar o login no M365 e Google Workspace de um país novo ou país incomum;

2.5.1.2.8. 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;

2.5.1.2.9. 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;

2.5.1.2.10. 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 e Google Workspace;

2.5.1.2.11. A solução deverá disponibilizar dashboard de informações do Entra ID com gráficos e painéis de usuários desatualizados com funções administrativas, associações desatualizadas em grupos, grupos públicos e muito mais;

2.5.1.2.12. 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;

2.5.1.2.13. A solução deverá disponibilizar dashboard do OneDrive, com painéis para visualizar arquivos expostos, arquivos sensíveis obsoletos, permissões obsoletas, links de colaboração;

2.5.1.2.14. A solução deve 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;

2.5.1.2.15. 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 e Google Drive;

2.5.1.2.16. A solução deverá fornecer uma visão gráfica e interativa dos links de compartilhamento do Microsoft 365 e Google Drive em contexto com sensibilidade e desatualização;

2.5.1.2.17. A solução deverá fornecer relatório de permissões, incluindo informação da classificação dos arquivos;

2.5.1.2.18. A solução deverá fornecer relatório das atividades de acesso dos usuários;

2.5.1.2.19. A solução deverá detectar de forma automática, atividades que correspondem a possíveis ameaças cibernéticas e padrões de ataques comuns;

2.5.1.2.20. A solução deverá realizar a classificação dos arquivos hospedados nos repositórios da nuvem;

2.5.1.2.21. A solução deverá permitir a configuração dos tipos de arquivos que serão escaneados e a definição do tamanho do arquivo;

2.5.1.2.22. A solução deverá permitir o escaneamento em tempo real dos arquivos, possibilitando a aplicação de rótulos de classificação, utilizando regras integradas e outros padrões;

2.5.1.2.23. 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.

2.5.1.2.24. A solução deverá fornecer relatório referente aos níveis de exposição dos dados no SharePoint Online e OneDrive e Google Drive, para qualquer tipo de site, pasta ou arquivo;

2.5.1.2.25. A varredura para classificação dos arquivos deve acontecer de forma contínua para qualquer

tipo de dado armazenado nos repositórios monitorados na nuvem ou local;

2.5.1.2.26. 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;

2.5.1.2.27. 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;

2.5.1.2.28. A solução deverá remediar de forma automática: Links de colaboração que expõe dados sensíveis, links de colaboração que expõe dados externamente ou publicamente, links de colaboração que expõe dados para qualquer um na internet, links de colaboração que expõe dados para toda a organização, links de colaboração que expõe dados para pessoas específicas, links de colaboração que expõe dados para pessoas externas específicas, links de colaboração que estão inativos, permissões obsoletas, permissões diretas;

2.5.1.2.29. 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;

2.5.1.2.30. A solução deverá possuir políticas de remediação automatizadas para proteção do ambiente de nuvem, como:

2.5.1.2.31. Remoção de permissão direta de grupos dinâmicos, públicos, usuários de fora da organização, e usuários de toda a organização;

2.5.1.2.32. Remoção de links de colaboração para qualquer um na organização;

2.5.1.2.33. Remoção de links de colaboração para qualquer um na internet;

2.5.1.2.34. Remoção de links de colaboração inativos;

2.5.1.2.35. Remoção de permissões direta inativas;

2.5.1.3. AUDITORIA PARA CAIXAS POSTAIS

2.5.1.3.1. As funcionalidades descritas devem se aplicar às caixas postais e pastas públicas dos servidores de correio eletrônico Microsoft Exchange Online, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados não estruturados monitorados.

2.5.1.3.2. A 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) Gerar alerta com base nas informações auditadas;

c) Monitorar e analisar comportamentos suspeitos de usuários;

d) Gerar relatórios sobre o ambiente de correio eletrônico.

2.5.1.3.3. A solução deverá monitorar os eventos das caixas postais dos usuários e as pastas públicas do Exchange Online;

2.5.1.3.4. A solução deverá monitorar, no mínimo, os seguintes eventos do Exchange Online:

a) Pasta Exchange criada e excluída;

b) Pasta do Exchange movida e aberta;

c) Permissões de pasta do Exchange adicionadas e alteradas;

d) Pasta do Exchange renomeada;

e) Regra de encaminhamento criada e atualizada;

f) Logon na caixa de correio;

g) Permissão de caixa de correio adicionada (inclui Enviado como, Enviado em nome de X e Acesso total);

h) Permissão de caixa de correio removida (inclui Enviado como, Enviado em nome de X e Acesso total);

i) Mensagem criada, apagada, enviada, editada, movida, enviada como, enviada em nome;

j) Permissão administrativa de pasta pública adicionada;

k) Regra de transporte criada, desativada, ativada, removida e atualizada;

2.5.1.3.5. 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.

2.5.1.3.6. 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.

2.5.1.3.7. O painel web deve possibilitar a visualização: de todos os alertas e seus eventos em determinado período; Usuários se comportando de forma suspeita que dispararam alertas; Tipos de alertas mais disparados; Dispositivos mais alertados;

2.5.1.3.8. Deve ser possível, a partir de selecionado evento alertado, fazer filtragem e correlacionamento com outros eventos como, por exemplo, o comportamento dos usuários do mesmo departamento do usuário alertado ou acessos ao mesmo tipo de informação sensível identificado pela solução;

2.5.1.3.9. A solução deverá apresentar a razão para um alerta ter sido disparado;

2.5.1.3.10. A solução deverá apresentar detalhes dos alertas gerados como usuário envolvido, dispositivo envolvido, dados envolvidos e período do comportamento suspeito;

2.5.1.3.11. A solução deverá realizar a classificação dos dados localizados nas caixas de e-mail do exchange, em anexos e eventos do calendário;

2.5.1.3.12. Deve ser possível identificar quem tem acesso as caixas de e-mail compartilhadas e caixas de usuário, incluindo permissões delegadas;

2.5.1.3.13. Um dashboard do exchange online deve ser disponibilizado indicando no mínimo: quantidade de caixas de e-mail de usuário, caixas compartilhadas, caixas de e-mail que contém dados sensíveis, quantidade de mensagens sensíveis;

2.5.2. GRUPO 2

2.5.2.1. GERENCIAMENTO DE ACESSO PRIVILEGIADO

2.5.2.1.1. Gerenciar todo o ambiente sem a necessidade de instalação de agentes ou qualquer software nos sistemas-alvos ou dispositivos de rede;

2.5.2.1.2. Gerar vídeos ou logs de textos das sessões realizadas através da solução, armazenados em repositório seguro, criptografado e protegido contra qualquer alteração que comprometa a integridade dessas evidências;

2.5.2.1.3. Geração automática de senhas de alta complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;

2.5.2.1.4.Tanto appliances quanto sistemas operacionais que compõe a solução devem seguir padrões de “hardening” atualizados constantemente pelo fabricante da solução;

2.5.2.1.5.O Banco de Dados deverá ser fornecido como parte integrante da solução.

2.5.2.1.6.Utilizar um banco de dados com as melhores práticas de segurança, deve estar em ambiente “hardenizado”, com mecanismo de blindagem e criptografia do sistema operacional e documentação que comprove a contemplação destes requisitos;

2.5.2.1.7. Possibilitar a utilização de criptografia do banco de dados utilizado pela solução, para armazenar as senhas das credenciais gerenciadas por ela, devendo ainda ser compatível com pelo menos um dos seguintes métodos e padrões de criptografia:

a) AES com chaves de 256 bits;

b) FIPS 140-2;

c) Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo fabricante para a solução ofertada.

d) Para geração de hash, deve permitir a utilização do algoritmo SHA-256 ou variações superiores da família SHA-2.

2.5.2.1.8. A solução deverá prover mecanismos de criptografia de usuário e senha para conexão com base de dados.

2.5.2.1.9. A solução não deverá trafegar dados sensíveis em texto claro.

2.5.2.1.10. A solução deverá prover mecanismos de criptografia para informações sensíveis armazenadas em banco de dados compatível com o padrão AES com chaves de 256 bits.

2.5.2.1.11. A interface da solução, no acesso via navegador web, deverá utilizar o protocolo HTTPS.

2.5.2.1.12. O backup/restore de todos os dados e configurações da solução deve estar incluso e deve permitir ao administrador agendar backups para determinada data e hora e exportá-los para um servidor remoto.

2.5.2.1.13. A solução deverá manter a persistência de todos os relatórios e arquivos históricos, incluindo gravações de sessão, sem necessidade de resta1ração de backup, por pelo menos 90 (noventa) dias.

2.5.2.1.14. A solução deverá permitir retenção em backup de relatórios e logs da aplicação por pelo menos 2 (dois) anos.

2.5.2.1.15. A solução deve permitir retenção em backup das gravações de sessão por pelo menos 1 (um)

ano.

2.5.2.1.16. O arquivo de backup não deverá conter nenhuma informação de conta e senha em texto claro.

2.5.2.1.17. No backup da chave mestra, ela deve poder ser dividida pelo sistema por uma quantidade parametrizada de partes, de modo que não permita a visualização do todo por uma única pessoa, mas apenas a parte devida a cada uma delas.

2.5.2.1.18. A solução deverá possibilitar a replicação em outros Data Centers.

2.5.2.1.19. No caso de falha de um dos servidores do cluster de cofre de senhas de alta disponibilidade local, cada um dos servidores deve tratar todas as requisições de acesso, sem nenhum prejuízo no desempenho ou nas funcionalidades;

2.5.2.1.20. Alterações realizadas no cluster de cofre de senhas de alta disponibilidade local deve ser automaticamente replicadas para os outros servidores de redundância, de forma sincrona e com delay máximo de 50ms;

2.5.2.1.21. Utilizar tecnologia de restrição e autenticação que inclua Assinatura Digital (Hash), e endereço IP do host ou conjunto de hosts a serem acessados pela solução;

2.5.2.1.22. A solução deve permitir compatibilidade com, no mínimo, os seguintes padrões: ISO 27001, PCI, SOX, GDPR, PQO BM&F, para implementação de controles de acesso a credenciais privilegiadas;

2.5.2.1.23. Possibilidade de comunicação com os serviços de diretório via protocolo LDAPS;

2.5.2.1.24. Suportar sincronização do relógio interno via protocolo NTP

2.5.2.1.25. A solução deve possuir interface única, na mesma solução, para o gerenciamento de senhas e sessões.

2.5.2.1.26. A solução deve oferecer o provisionamento e gerenciamento de todas as contas privilegiadas, incluindo contas para a administração de aplicações de negócio, bancos de dados e dispositivos de redes, não se limitando apenas às contas de sistemas operacionais de servidores.

2.5.2.1.27. A solução deverá realizar sincronismo de data e relógio via protocolo NTP (Network Time Protocol) ou por meio do serviço de data e hora do sistema operacional.

2.5.2.1.28. A solução deverá prover mecanismos de atualização de segurança.

2.5.2.1.29. Ter uma console de configuração unificada para gerenciamento de contas e ativos agregados ao cofre de senhas;

2.5.2.1.30. Permitir o backup e o recovery de seu banco de dados, bem como das configurações de software estabelecidas, com as seguintes capacidades:

2.5.2.1.31. Permitir a execução de tarefas de backup e criptografia sem a necessidade de agentes de terceiro, provendo assim o maior nível possível de segurança e integridades dos dados a serem copiados;

2.5.2.1.32. Permitir a execução de backups automatizados através da programação/agendamento.

2.5.2.1.33. Permitir, através de interface gráfica, que administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.

2.5.2.1.34. Extrair backups do sistema, logs e vídeos além das credenciais para um servidor localizado em Data Centers remotos caso seja necessário para restaurar todas as configurações e os dados da solução de cofre de senhas;

2.5.2.1.35. A solução deve permitir que você finalize todas as sessões em andamento, bloqueie o acesso a dispositivos predefinidos ou bloqueie todo o acesso a ele por um período definido.

2.5.2.1.36. Gerenciamento de senhas:

a) A solução deve permitir parametrização de políticas de segurança e força de senha pelo administrador do sistema, dentre as quais: conjunto de caracteres alfanuméricos, numéricos e caracteres especiais, podendo ser escolhidos também quais caracteres especiais serão permitidos, com possibilidade de não possibilitar caracteres repetidos, gerando senhas aleatórias.

b) Gerenciar chaves SSH e fazer Scan de servidores Linux e identificação e publicação de chaves SSH

c) Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;

d) Consolidação periódica de senhas para identificar senhas que foram alterados em sistema gerenciados;

e) Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;

f) Oferecer interface com visão personalizada exclusiva para Auditorias e Órgãos Reguladores, contendo

os dispositivos e credenciais gerenciadas pela solução;

g) Fornecer uma área de transferência segura, para que o solicitante possa visualizar ou copiar a senha na tela de login do sistema de destino;

h) Prover área de transferência segura, de forma que o solicitante possa visualizar a senha ou copiá-la para a tela de login do sistema-alvo;

i) Liberação ou revogação de todos os acessos de uma determinada credencial de maneira automatizada e imediata;

j) Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;

k) Permitir o monitoramento on-line do uso das contas e desligamento da sessão;

2.5.2.1.37. Apresentar o recurso "break glass" para acesso de emergência às contas, ou seja, permitirá acesso a ativos protegidos de forma emergencial, sem a necessidade de aprovação prévia em contas no qual o usuário não teria acesso, sem perda de rastreabilidade;

2.5.2.1.38. Oferecer a funcionalidade de "Discovery" para realizar busca de novos servidores, elementos de rede e bancos de dados, sendo capaz de levantar automaticamente as contas criadas nesses novos dispositivos incluindo a possibilidade de descobrir certificados SSL utilizado nos dispositivos gerenciados;

2.5.2.1.39. A ferramenta deverá cuidar do ciclo de vida completo de um certificado, possuindo as seguintes funcionalidades: Criação de uma requisição, assinatura, renovação e revogação de certificados.

2.5.2.1.40. A solução deverá possuir fluxos de aprovação, incluindo aprovação multinível para as seguintes funcionalidades: Assinatura de um .csr, renovação e instalação.

2.5.2.1.41. A solução deverá realizar o deploy de certificados no mínimo nos seguintes ambientes: Apache, IBM Websphere, F5 BigIP, IIS, Nginx, Tomcat

2.5.2.1.42. A solução deve possibilitar a revogação de um certificado, não permitindo nenhuma interação com o certificado quando estiver revogado, apenas a renovação.

2.5.2.1.43. A solução deverá possuir relatórios e dashboards gerenciais que mostrem toda a base de certificados, centralizando as informações mais críticas de um certificado, como por exemplo certificados que estão próximos a vencer.

2.5.2.1.44. A solução deverá possibilitar a configuração de notificações multi-níveis como por exemplo, um certificado a 90 dias para vencer irá notificar o analista, 60 dias para vencer irá notificar o gestor, e 30 irá notificar o gerente.

2.5.2.1.45. A solução deverá possibilitar a criação e importação de requisições de certificados (.csr).

2.5.2.1.46. A solução deverá se integrar com no mínimo as seguintes autoridades certificadoras: DigiCert, Godaddy, Microsoft CA, Comodo, GlobalSign e Let's Encrypt

2.5.2.1.47. A solução deve possibilitar o saque de senha de um certificado baseado nas permissões que foram atribuídas para cada usuário. Todos os saques deverão ser auditados, e também deve ser possível passar por um processo de fluxo de aprovação com break the glass e aprovação multiníveis.

2.5.2.1.48. A solução deverá possibilitar a criação de organizações gerenciais de certificados dentro do sistema.

2.5.2.1.49. A solução deverá permitir a importação manual de um certificado, independentemente de qual formato ele seja.

2.5.2.1.50. Deve ser possível o envio de certificados por e-mail nos principais formatos, sendo no mínimo: der, pem, pfx, p7b.

2.5.2.1.51. Deve ser possível o download de certificados nos principais formatos, sendo no mínimo: der, pem, pfx, p7b.

2.5.2.1.52. A solução deve permitir o gerenciamento de certificados independentemente de qual formato ele é. Essa informação deverá ser transparente ao administrador.

2.5.2.1.53. A solução deverá ter uma funcionalidade para delegar um responsável, que será notificado em relação a qualquer acontecimento relacionado a aquele certificado.

2.5.2.1.54. A solução deve possuir dashboards gerenciáveis que mostre todos os certificados ativos gerenciados, separando por diversos tipos de regras de negócio, como vencimento, nível de segurança e a localização dos certificados.

2.5.2.1.55. A solução deve possibilitar a renovação de certificados, podendo também alterar informações de um certificado e gerar um histórico para que seja um possível regaste de informações.

2.5.2.1.56. A solução deve permitir a instalação programada de um certificado, podendo ser selecionado dia, hora e data que será instalada, e também em quais dispositivos aquele certificado será instalado.

2.5.2.1.57. A solução deve possuir uma funcionalidade para renovar automaticamente certificados quando o certificado estiver: X dias antes do vencimento, na data do vencimento, e X dias após o vencimento.

2.5.2.1.58. A solução deve possuir uma inteligência para fazer a avaliação de segurança de um certificado, levando em consideração pelo menos 5 critérios de segurança.

2.5.2.1.59. A solução deve gerenciar os certificados de uma maneira que não considere o formato dos certificados, ou seja, na requisição, assinatura, renovação e instalação dos certificados, o administrador não deve saber quais são os formatos necessários, isso deve estar embutido na inteligência da aplicação.

2.5.2.1.60. Possibilidade de bloqueio de comandos específicos, com opção de interromper a sessão caso o usuário execute um comando indevido;

2.5.2.1.61. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;

2.5.2.1.62. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;

2.5.2.1.63. Possibilidade de geração de relatórios baseados nos logs e exportá-los para arquivos em formato ".csv";

2.5.2.1.64. A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo, no mínimo, RPC,WinRM, SSH, API REST HTTP/HTTPS;

2.5.2.1.65. As senhas geradas automaticamente pela solução de cofre de senhas devem seguir os seguintes requisitos:

a) Poder determinar a quantidade de caracteres;

b) Ser composta por números, letras maiúsculas, letras minúsculas e por caracteres especiais;

c) Poder ser pré-definidas quais caracteres especiais poderão ser utilizados;

d) Aleatórias de modo que dentro do histórico de uma conta seja improvável encontrar duas senhas iguais;

e) Não seja baseada em palavra de dicionário.

2.5.2.1.66. A solução deve permitir a criação de políticas de senhas de forma hierárquica ou em níveis de segurança, possibilitando a criação de senhas diferenciadas para grupos de ativos de diferentes plataformas ou criticidades.

2.5.2.1.67. Possuir mecanismo para exportar arquivo com as últimas senhas para repositório remoto, de forma criptografada e protegida por senha de dupla custódia para recuperações de senhas no caso de falha total da solução;

2.5.2.1.68. A solução deve possibilitar políticas de senha que impeça visualização simultânea de credenciais, sessões, bem como também configurar o tempo de expiração das senhas baseadas por visualização e data de expiração. Também deve ser possível escolher dias específicos da semana e horários que as credenciais poderão expirar.

2.5.2.1.69. A solução deve gerenciar senhas privilegiadas de aplicações, de modo a evitar situação de senhas embutidas em códigos-fonte.

2.5.2.1.70. A solução deve ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas ou domínios distintos;

2.5.2.1.71. A solução não deverá depender da instalação de agentes para realizar a troca de senhas.

2.5.2.1.72. Checkout/CheckIn de credencial: A solução deve redefinir a credencial (senha) no ambiente para os casos de visualização da senha pelo solicitante nos processos de checkout de credencial.

2.5.2.1.73. A solução deve ter a capacidade de realizar a reconciliação de credenciais automaticamente.

2.5.2.1.74. Rotação de senhas:

a) Troca automática de senhas para Servidores (Unix, Linux, Windows), Bancos de Dados (MS SQL, ORACLE, MYSQL, PostgreSQL), Aplicações Web, Dispositivos de Rede, Mainframe;

c) A solução deverá realizar a troca automática da senha da ligação entre servidores MS SQL server com Linked Servers;

d) Geração automática de senhas de força/complexidade de acordo com as regras de cada tecnologia e Política de Segurança da empresa;

e) Flexibilidade para configuração de força de senha gerada;

f) Realizar a troca automática das senhas, em horário programado, após terem sido liberadas para uso ou por vencimento de prazo;

g) Possibilidade de gerenciar senhas privilegiadas em aplicações e integração com sistemas legado;

h) Possibilidade de executar trocas de senhas por meio de automações que interagem com páginas web, tanto para sistemas externos e conhecidos, como para sistemas internos desenvolvidos por equipes internas.

i) Armazenamento de histórico de senhas por equipamento;

j) Registro de troca executadas;

k) Relatório de acompanhamento de trocas;

l) Relatório de erros de trocas;

m) Alertas de falha ou sucesso de trocas;

n) Possibilidade de reconfiguração/customização de scripts ou plugin de troca de senhas para configuração de casos que exijam parâmetros específicos para rotação de senhas;

o) Configuração de políticas de trocas de senhas com agendamento programado ou por ocorrências de eventos com especificação de parâmetros de prazo para a troca;

p) Disponibilizar os Templates de troca de senha de forma que possam ser abertos, editáveis e auditáveis;

q) Templates com linguagem acessível e fácil interpretação;

r) Rastreabilidade de Alteração de Template;

s) Troca de senhas em aplicações HTTP/HTTPS com templates

2.5.2.1.75. Controle de Acesso:

a) A solução deve ser capaz de limitar a execução de comandos críticos pelos usuários cadastrados.

b) A solução deve ser capaz de prover acesso externo sem a necessidade de instalação de Agent ou utilização de VPN

c) A solução deve permitir o controle de execução de comandos críticos por, pelo menos, “whitelist” e “blacklist”.

d) A solução deve permitir o início e a condução de sessões dentro do próprio navegador, dispensando o uso de clients externos como o mstsc.exe e o putty.exe.

e) A solução deve possuir tempo de expiração de sessão configurável pelo administrador do sistema.

f) A solução deve suportar a desconexão da sessão por atividade/uso indevido de comandos pré-cadastrados no sistema.

g) A solução deve permitir a criação de grupos de usuários.

h) Bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução - Baseado em blacklist;

i) Bloqueio ou alerta de comandos com alertas, interrupção de sessão ou apenas o registro de execução - Baseado em whitelist;

2.5.2.1.76. Possibilidade de bloqueio e auditoria de comandos específicos;

2.5.2.1.77. Buscar por comandos específicos executados pelo usuário através de linha de comando em logs ou sessões gravadas;

2.5.2.1.78. Configuração de alertas imediatos quando realizados determinados comandos por usuários privilegiado;

2.5.2.1.79. Marcação de pontuação de comandos de acordo com nível de risco de cada comando.

2.5.2.1.80. A solução deve permitir a atribuição de privilégios a grupos de usuários, associados a um ou mais alvos gerenciados.

2.5.2.1.81. A Solução deve permitir integração com ferramentas de gestão de incidentes (ITSM) para validar tickets abertos durante processo de aprovação de acesso

2.5.2.1.82. A solução deve permitir acesso simultâneo ao cofre de senhas e as contas privilegiadas por dois ou mais usuários.

2.5.2.1.83. A solução deve viabilizar a segregação de funções entre usuários de uma mesma aplicação gerenciada.

2.5.2.1.84. A solução deve fornecer funcionalidade para revogar imediatamente todas as sessões remotas para um usuário conectado.

2.5.2.1.85. A solução deve permitir acesso simultâneo à credenciais privilegiadas por dois ou mais usuários.

2.5.2.1.86. Acessos simultâneos a credenciais, senhas e dispositivos não devem possuir

comprometimento da rastreabilidade.

2.5.2.1.87. Possibilitar via script, a criação de novos conectores baseado em acessos SSH e RDP, para que seja possível suportar novas interfaces de autenticação de ativos.

2.5.2.1.88. A solução deverá permitir o gerenciamento e monitoramento de sessões do Microsoft Azure.

2.5.2.1.89. Ser compatível com sistemas operacionais: Windows Server 2008 ou superior, Red Hat Enterprise, Debian, CentOS, IBM zOS, Solaris, Ubuntu Server.

2.5.2.1.90. Ser compatível com aplicações windows: contas de serviço e pools de aplicações do IIS

2.5.2.1.91. Ser compatível com sistemas gerenciadores de bancos de dados: Oracle, Oracle RAC, MSSQL, MySQL, Sybase ASE e IQ, MongoDB, PostgreSQL;

2.5.2.1.92. Ser compatível com appliances de segurança: Cisco, IBM, SourceFire;

2.5.2.1.93. Ser compatível com dispositivos de rede: Cisco, D-Link, HP, 3com, Alcatel, Foundry, Brocade, ARUBA, Huawei.

2.5.2.1.94. Ser compatível com aplicações: WebLogic, JBOSS, Tomcat, Peoplesoft, Oracle Application Server, Apache e IIS.

2.5.2.1.95. Ser compatível com serviços de Diretórios: AD, LDAP

2.5.2.1.96. Ser compatível com ambientes virtuais: VMware e Openstack;

2.5.2.1.97. Ser compatível com storages: Hitachi, Isilon, EMC, Huawei, Netapp, Pure Storage e IBM;

2.5.2.1.98. "Ser disponibilizado um SDK (Software Development Kit) ou API (Application Programming Interface) que pode ser configurado para permitir que aplicações clientes possam:

2.5.2.1.99. Solicitar credenciais e dispositivos;

2.5.2.1.100. Cadastro e alteração credenciais e dispositivos;

2.5.2.1.101. Solicitar chaves SSH;

2.5.2.1.102. Cadastro e alteração de chaves SSH."

2.5.2.1.103. Ser compativel com aplicações em nuvem como Rackspace, IBM SmartCloud, Microsoft Azure, Hyper-V, Google Cloud Platform, GoGrid, Vmware vCenter Server, Amazon AWS.

Cadastro de Ativos:

a) Cadastro de equipamentos parametrizado manualmente;

b) Atributos como Marca, Modelo, Fabricante, Localidade, Grupo abertos para configuração do administrador da ferramenta independente do fabricante.A solução deve armazenar senhas para aplicações e serviços online;

2.5.2.1.104. A solução deve armazenar documentos e arquivos;

2.5.2.1.105. A solução deve armazenar notas;

2.5.2.1.106. A solução deve possuir registro de acesso a informações privilegiadas;

2.5.2.1.107. A solução deve ter a possibilidade de compartilhar informações com outros usuários;

2.5.2.1.108. A solução deve possuir APIs para gerenciar itens do cofre;

2.5.2.1.109. A solução deve guardar diferentes versões de um segredo que possam ser restauradas

2.5.2.1.110. A solução deve oferecer importação em lote de senhas, notas, documentos e arquivos

2.5.2.1.111. A solução deve oferecer migração das informações do LastPass

2.5.2.1.112. A solução deve possuir um dashboard administrativo com opções de ambiente

2.5.2.1.113. A solução deve possuir uma extensão de navegador para Google Chrome

2.5.2.1.114. Utilizando a extensão deve ser possível salvar senhas diretamente do website acessado

2.5.2.1.115. A solução deverá ser flexivel no processo de aprovação para o acesso a contas privilegiadas (acessos pré-aprovados, acessos com aprovação única e e acessos com aprovações multiníveis).

2.5.2.1.116. A solução deverá permitir a configuração de fluxos de aprovação diferenciados por criticidade e características da conta, como contras privilegiadas e contas de uso por terceiros.

2.5.2.1.117. A solução deverá permitir a alteração, por parte do aprovador, do periodo de acesso solicitado por um usuário.

2.5.2.1.118. Caso uma solicitação de acesso seja aprovada, a sessão e o privilégio concedido deverão expirar automaticamente ao final do período autorizado.

2.5.2.1.119. O acesso ao fluxo de solicitação e aprovação deve ser possível de ser realizado de forma remota e segura.

2.5.2.1.120. A solução deve possuir função para revogar todos os acessos de uma pessoa de maneira imediata.

2.5.2.1.121. A solução deve oferecer um campo para que seja inserido um número identificador de demanda ou mudança ao qual o acesso estará associado.

2.5.2.1.122. A solução deve oferecer interface para usuários e auditores, provendo mecanismos de controle de acesso flexíveis para criar visões/grupos personalizados de dispositivos gerenciados e contas privilegiadas.

2.5.2.1.123. A solução deverá prover mecanismo de acesso emergencial a saque de senhas cadastradas na solução.

2.5.2.1.124. O acionamento do acesso emergencial deve notificar os aprovadores via e-mail ou pela interface da ferramenta.

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. CONTEXTUALIZAÇÃO E JUSTIFICATIVA DA CONTRATAÇÃO

3.1.1. Conforme verificado durante o estudo técnico preliminar, o alto volume de dados e arquivos armazenados nos repositórios de Tecnologia da Informação do MPPI e as novas exigências impostas pela legislação vigente (Lei de Acesso à Informação e Lei Geral de Proteção de Dados, por exemplo) exigem o aperfeiçoamento dos processos de controle, gestão e governança dos dados.

3.1.2. Atualmente a classificação e controle dos dados são feitos de forma manual, sem uma ferramenta que otimize esse processo e garanta a integridade e a privacidade dos dados. Ressalta-se que, quanto a classificação, é necessário um controle mais efetivo quanto ao acesso a estes dados, principalmente no comportamento do usuário que os consome/consulta e acessa arquivos armazenados no ambiente do MPPI.

3.1.3. Como descrito, esse controle manual afeta diretamente as boas práticas de gestão e governança, não permitindo sequer uma auditoria de dados adequada. A aquisição de uma ferramenta que permita melhorar o controle de acesso, a classificação e atue monitorando atividades suspeitas, alertando comportamentos estranhos por parte de usuários e objetos a que têm acesso a arquivos e dados armazenados no ambiente do MPPI, garante não só o uso de boas práticas de auditoria, controle, gestão e governança de dados como gera também uma camada extra de segurança da informação, auxiliando na prevenção de possíveis ataques que acarretam em prejuízos ao órgão.

3.1.4. Além disso, buscando a constante melhoria e a celeridade no cumprimento de seu papel está modernizando infraestrutura física e tecnológica, a Coordenação de Tecnologia da Informação (CTI) necessita adquirir soluções alinhadas com os objetivos estratégicos e de negócio da organização, e para atingir os objetivos estratégicos e de negócio e suprir as demandas, a CTI tem que necessariamente estar apoiada em práticas, normas e ferramentas que propiciem a Gestão das contas Privilegiadas, pois de outra forma, seriam majorados os riscos de TI e consequentemente, os riscos operacionais envolvidos nos processos de sustentação dos serviços.

3.1.5. Neste sentido, a aquisição de uma solução de controle dos acessos por contas privilegiadas e genéricas, viabilizando a rastreabilidade dos autores responsáveis por atos praticados com estas credenciais, inclusive o tempo em que a conta estará em posse de um usuário, o fornecimento de senhas temporárias e o registro de tudo o que foi feito durante a posse da conta, preservando as evidências e garantindo a audibilidade das ações.

3.1.6. Alcance de maior eficiência não só no âmbito da funcionalidade da solução, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, a resolução de conflitos entre fornecedores distintos. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado, não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, o suporte técnico e o treinamento serão executados por um único fornecedor representante do fabricante, respeitando a divisão de grupos que foi definida. Dessa forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores.

Assim, entende-se que é fundamental para a pretensa contratação, e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que todos os itens ora propostos sejam adquiridos/contratados de forma agrupada, conforme proposta na tabela do item 2.1 do tópico anterior.

3.1.7. Na situação em apreço, é imperativo destacar o que dispõe o Princípio da Padronização, insculpido no inciso I do art. 47 da Lei no 14.133/2021, pelo qual se estabelece que a Administração, sempre que

possível, tem o objetivo de compatibilizar especificações técnicas e de desempenho, segundo transcrição a seguir, in verbis:

“Lei no 14.133/2021

Art. 47. As licitações de serviços atenderão aos princípios:

I - da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;

3.1.8. Tal princípio, disposto no art. 47 , Inciso I, da Lei 14.133/2021, visa a propiciar à Administração uma consecução mais econômica e vantajosa de seus fins; e serve, pois, como instrumento de racionalização da atividade administrativa, por meio da redução de custos financeiros, tecnológicos, operacionais, gerenciais, técnico-administrativos e da otimização da aplicação de recursos. Isto é, fatores que se coadunam e se verificam na contratação ora pretendida. Significa, portanto, que, nesse caso, a padronização elimina variações tanto no tocante à seleção de equipamentos, componentes e produtos no momento da aquisição/contratação, como também na sua utilização, conservação, segurança e manutenção.

3.1.9. Dividir o objeto, nessa situação, ocasionará prejuízos técnicos, como também riscos de danos tecnológicos, visto que a manutenção, a garantia, o suporte técnico e o treinamento, se realizados por vários fornecedores, exigiriam um tempo excessivo em dirimir divergências entre possíveis incompatibilidades e causariam um potencial risco de operacionalização e funcionamento, pela adoção de procedimentos variados ou divergentes.

3.1.10. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes da solução, melhor gerenciamento do contrato e obtenção dos serviços de suporte e treinamento padronizados.

3.1.11. Conforme Acórdão no 861/2013 - TCU - Plenário -, é lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Além disso, a solução de TI, objeto da contratação em tela, possui uma natural indivisibilidade, o que também inviabiliza a contratação de seus serviços por item de forma separada.

3.1.12. Segundo o Acórdão no 5.260/2011 – TCU – 1a câmara, de 06/07/2011, “Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si”. O lote proposto nesse documento agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à competitividade.

3.1.13. O agrupamento também encontra amparo na jurisprudência do Tribunal de Contas da União, conforme se observa na Súmula 247 - TCU/2007.

"É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade."

3.14. Em suma, a opção pelo fornecimento e consequente adjudicação por grupo leva em conta a modalidade de contratação pretendida e os benefícios associados. O agrupamento de vários itens num mesmo objeto não compromete a competitividade do certame, uma vez que várias empresas, que atuam no mercado, apresentam condições para cotar todos os itens.

3.15. Resultados esperados com a aquisição da solução:

- Gestão e governança dos dados não estruturados do MPPI;
- Classificação e controle de forma automatizada de dados;
- Incremento da segurança e auditoria no acesso aos dados;
- Manter as contas privilegiadas em um único repositório seguro;
- Implementar regras para autorização do uso das contas privilegiadas;
- Geração automática da senha no momento da retirada;
- Entrega de sessão autenticada, sem que o usuário tenha contato com a senha;
- Definir o tempo em que o usuário autorizado poderá usufruir da conta privilegiada;
- Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);
- Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional;

- Obter o monitoramento das ações de funcionários e terceiros com o uso de credenciais privilegiadas;
- Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;
- Melhorar qualidade na prestação de informações aos órgãos de controle;
- Rastrear o uso de contas privilegiadas no ambiente computacional

3.16. Esta contratação está alinhada com objetivo estratégico 3.5 do Plano Estratégico Institucional, que é prover soluções tecnológicas integradas e inovadoras e alinhado com a perspectiva de Aprendizado e Crescimento, que diz:

> "13 – Prover soluções tecnológicas integradas e inovadoras, através da governança de TI; definição de papéis e responsabilidades, gerenciamento de competências técnicas de TI e desenvolvimento de conhecimentos e habilidades dos servidores de TI, além de suporte dos processos de negócio e provimento de soluções tecnológicas integrados, por meio da inovação."

3.2. ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTO INSTITUCIONAIS

3.2.1. O objeto da contratação também está alinhado ao Plano Estratégico do MPPI.

Nr/ID	Objetivos Estratégicos
O.E -13	Prover soluções tecnológicas integradas e inovadoras.
O.E -09	Assegurar a disponibilidade e a aplicação eficiente dos recursos orçamentários.

3.2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2025, conforme detalhamento a seguir:

ID	Item	Descrição
CTI - 9 - Nova Contratação	Solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturadas (Licenciamento, implantação, treinamento e suporte)	Viabilizar a rastreabilidade dos autores responsáveis por atos praticados com estas credenciais, inclusive o tempo em que a conta estará em posse de um usuário, o fornecimento de senhas temporárias e o registro de tudo o que foi feito durante a posse da conta, preservando as evidências e garantindo a audibilidade das ações
CTI - 10 - Nova Contração	COFRE DE SENHAS (Licenciamento, implantação, treinamento e suporte)	Controle dos acessos por contas privilegiadas e genéricas, viabilizando a rastreabilidade dos autores responsáveis por atos praticados com estas credenciais, inclusive o tempo em que a conta estará em posse de um usuário, o fornecimento de senhas temporárias e o registro de tudo o que foi feito durante a posse da conta, preservando as evidências e garantindo a audibilidade das ações

3.3. ESTIMATIVA DE DEMANDA

GRUPO 1 - ITENS 1 A 6			
Item	**Descrição**	**Unidade**	**Quantidade**
1	Licença para visibilidade, análise de dados locais, comportamento e prevenção de ameaças por 36 meses - **CATSER: 24333**	Usuários	1600
2	Licença para visibilidade, análise de dados em nuvem, comportamento e prevenção de ameaças por 36 meses - **CATSER: 24333**	Usuários	1600
3	Licença para visibilidade, análise de dados em caixas postais, comportamento e prevenção de ameaças por 36 meses - **CATSER: 24333**	Usuários	1600
4	Serviço de instalação e configuração para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. - **CATSER: 26972**	Serviço	2

5	Manutenção e Suporte Técnico para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. - **CATSER: 26972**	Serviço	2
6	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. - **CATSER: 3840**	Turma	2
GRUPO 2 - ITENS 7 A 17			
7	Cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses **- CATSER: 469726**	Unidade	2
8	Balanceador de carga para cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses**- CATSER: 469726**	Unidade	2
9	Subscrição para usuários com acesso privilegiado por 36 meses **- CATSER: 24333**	Usuários	40
10	Subscrição para servidores físicos e virtuais por 36 meses **- CATSER: 24333**	Servidores	400
11	Subscrição para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN por 36 meses **- CATSER: 24333**	Equipamentos	1000
12	Subscrição para aplicações não conteinerizadas com senha embutida (hard coded) por 36 meses **- CATSER: 24333**	Aplicações	80
13	Subscrição para acesso remoto seguro por 36 meses - **CATSER: 24333**	Unidade	60
14	Subscrição de gerenciamento de certificados digitais por 36 meses **- CATSER: 24333**	Unidade	2
15	Serviço de instalação e configuração para solução de controle de acesso de usuários privilegiados. - **CATSER: 26972**	Serviço	2
16	Manutenção e Suporte Técnico para solução de controle de acesso de usuários privilegiados. - **CATSER: 26972**	Serviço	2
17	Treinamento para solução de controle de acesso de usuários privilegiados. - **CATSER: 3840**	Turma	2

3.4. PARCELAMENTO DA SOLUÇÃO DE TI

3.4.1. A orientação do TCU no Acórdão nº 861/2013 - Plenário: "São lícitos os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si", admite a possibilidade do agrupamento de itens em lote único nos pregões eletrônicos.

3.4.2. Trata-se de prestação de serviço específico e comum, com objetivo de integrar os serviços e tecnologias e manter a alta disponibilidade do ambiente de forma segura e auditável. A rápida interação entre os profissionais envolvidos é fundamental para garantir pleno funcionamento dos serviços contratados.

3.4.3. Considerando que os itens licitados são intrinsicamente dependentes, uma maior divisão da contratação poderia acarretar riscos de não integração entre as partes, gerando alto tempo de resposta a incidentes e prejuízos ao MPPI.

3.4.4. Além disso, corroborando essa necessidade de adjudicação conjunta, através de LOTES, percebe-se que o mais conveniente para a CONTRATANTE é que todos os serviços previstos sejam realizados por

uma única empresa, de forma a se evitar a multiplicidade de contratos, possibilitando uma melhor fiscalização e controle, para cada lote definido.

3.4.5. Dessa forma, a licitação será dividida em itens, dispostos em LOTES, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos lotes forem de seu interesse.

3.5. RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS

a) Gestão e governança dos dados não estruturados do MPPI;

b) Classificação e controle de forma automatizada de dados;

c) Incremento da segurança e auditoria no acesso aos dados;

d) Manter as contas privilegiadas em um único repositório seguro;

e) Implementar regras para autorização do uso das contas privilegiadas;

f) Geração automática da senha no momento da retirada;

g) Entrega de sessão autenticada, sem que o usuário tenha contato com a senha;

h) Definir o tempo em que o usuário autorizado poderá usufruir da conta privilegiada;

i) Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);

j) Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional;

k) Obter o monitoramento das ações de funcionários e terceiros com o uso de credenciais privilegiadas;

l) Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;

m) Melhorar qualidade na prestação de informações aos órgãos de controle;

n) Rastrear o uso de contas privilegiadas no ambiente computacional

3.5.1. Esta contratação está alinhada com objetivo estratégico 3.5 do Plano Estratégico Institucional, que é prover soluções tecnológicas integradas e inovadoras e alinhado com a perspectiva de Aprendizado e Crescimento, que diz:

> "13 – Prover soluções tecnológicas integradas e inovadoras, através da governança de TI; definição de papéis e responsabilidades, gerenciamento de competências técnicas de TI e desenvolvimento de conhecimentos e habilidades dos servidores de TI, além de suporte dos processos de negócio e provimento de soluções tecnológicas integrados, por meio da inovação."

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. REQUISITOS DO NEGÓCIO

AUDITORIA DE DADOS NÃO ESTRUTURADOS:

- Aperfeiçoar os processos de controle, gestão e governança de dados. **Funcionalidades**:

a) Controle de acesso e classificação de dados;

b) Monitoramento das atividades suspeitas, alerta de comportamentos estranhos por parte de usuários e objetos a que têm acesso a arquivos e dados;

c) Boas práticas de auditoria, controle, gestão e governança de dados além de camada extra de segurança da informação, com auxilio na prevenção de possíveis ataques que acarretam em prejuízos ao MPPI;

GERENCIAMENTO DE ACESSO PRIVILEGIADO:

- Gestão de contas privilegiadas. **Funcionalidades**:

a) Manter as contas privilegiadas em um único repositório seguro;

b) Implementar regras para autorização do uso das contas privilegiadas;

c) Geração automática da senha no momento da retirada;

d) Entrega de sessão autenticada, sem que o usuário tenha contato com a senha;

e) Definir o tempo em que o usuário autorizado poderá usufruir da conta privilegiada;

f) Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);

g) Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional;

h) Obter o monitoramento das ações de funcionários e terceiros com o uso de credenciais privilegiadas;

i) Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;

j) Melhorar qualidade na prestação de informações aos órgãos de controle;

k) Rastrear o uso de contas privilegiadas no ambiente computacional

4.2. NECESSIDADE DO REQUISITANTE

4.2.1. Conforme as necessidades do MPPI, a Coordenadoria de Tecnologia da Informação deve apresentar soluções que atendam os requisitos do negócio e otimizem o trabalho, dessa forma, alinhados as necessidades de aprimoramento da segurança da informação e *compliance* com a Lei Geral de Proteção de Dados (LGPD);

4.2.2. Consoante tal necessidade, vemos que é necessário adquirir ferramentas para auxiliar o trabalho da coordenadoria na melhoria dos processos de controle, gestão e governança dos dados, bem como uma solução de controle dos acessos por contas privilegiadas e genéricas, viabilizando a rastreabilidade dos autores responsáveis por atos praticados com estas credenciais, inclusive o tempo em que a conta estará em posse de um usuário, o fornecimento de senhas temporárias e o registro de tudo o que foi feito durante a posse da conta, preservando as evidências e garantindo a audibilidade das ações.

4.3. REQUISITOS DE CAPACITAÇÃO

4.3.1. TREINAMENTO PARA O GRUPO 1

4.3.1.1. Deverá ser fornecido o treinamento do respectivo grupo 1, solução de segurança, auditoria, e prevenção de ameaças à base de dados não estruturados, conforme os seguintes requisitos:

a) O treinamento deverá contemplar todos os *softwares* que compõem a solução.

b) O treinamento poderá ser realizado remotamente.

c) Caberá à CONTRATADA oferecer os recursos ferramentais para a viabilização do treinamento.

d) O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

e) O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

f) A carga horária mínima exigida para este treinamento é de 20 horas.

g) A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 4 (quatro) horas de instrução diária.

h) Deverá ser ministrada uma turma de treinamento que terá até 15 participantes.

i) Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento. No caso de material impresso, os custos para impressão e lógica para envio para cada participante são de responsabilidade da CONTRATADA.

j) 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 período de realização e o nome completo do participante.

k) O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

l) As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência da garantia.

m) O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

n) 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 CONTRATANTE.

o) Para ser considerado adequado, o treinamento deverá ser aprovado por pelo menos 70% dos participantes das turmas.

4.3.1.2. A avaliação dos treinamentos levará em consideração as questões listadas a seguir:

a) Avaliação do conteúdo:

I)Adequação dos conteúdos aos objetivos propostos;

II) Adequação das atividades desenvolvidas para alcance dos objetivos propostos;

III) Adequação do tempo para o alcance dos objetivos propostos;

IV) Profundidade com que o conteúdo foi abordado, considerando os objetivos propostos;

V) Integração entre teoria, pesquisa, prática e/ou aspectos da realidade;

VI) Qualidade dos exemplos utilizados;

VII) Aplicabilidade dos conhecimentos adquiridos no trabalho;

VIII) Contribuição para melhoria do desempenho no trabalho;

IX) Qualidade do material instrucional (apostilas, gráficos. etc.).

b) Avaliação do instrutor:

I) Formas/métodos de apresentação dos conteúdos;

II) Conhecimento dos temas tratados;

III) Visão prática dos conteúdos tratados;

IV) Uso de estratégias para motivar os alunos em relação ao conteúdo;

VI) Incentivo à participação dos alunos em sala de aula;

VII) Incentivo à realização de atividades adicionais de aprofundamento do aprendizado.

c) Avaliação de ambiente e recursos

I) Qualidade dos recursos tecnológicos utilizados pelo instrutor (áudio, vídeo, recursos para demonstração etc.);

II) Qualidade do ambiente virtual disponibilizado para o curso;

III) Qualidade da conexão disponibilizada pela CONTRATADA.

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

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

VI) O treinamento será considerado com qualidade suficiente, caso tinja uma nota igual ou superior a 7,5.

VII) 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.

VIII) 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 neste termo de referência.

4.3.1.3. **Cronograma do Treinamento**

Evento	**Descrição**	**Prazo**	**Responsável**
01	Confirmação do recebimento da Ordem de Serviço de Treinamento	Durante a vigência do Contrato	MPPI
02	Entrega do Cronograma de Treinamento	Até 7 dias úteis após o evento 01.	CONTRATADA
03	Avaliação do Cronograma de Treinamento	Até 7 dias úteis após o evento 02.	MPPI
04	Ajustes no Cronograma de Treinamento	Até 7 dias úteis após o evento 03.	CONTRATADA
05	Execução dos Treinamentos	Até 30 dias úteis após o evento 04.	CONTRATADA
06	Emissão do Termo de Recebimento Definitivo do Treinamento	Até 10 dias úteis após o evento 05.	MPPI

4.3.2. TREINAMENTO PARA O GRUPO 2

4.3.2.1. Deverá ser fornecido o treinamento do respectivo grupo 2, Gestão e Controle de Contas de Usuários Privilegiados (PAM - *Privileged Access Management*), conforme os seguintes requisitos:

a) O treinamento deverá ser precedido de reunião de planejamento com a equipe da CONTRATANTE.

b) O treinamento contemplará todos os softwares e hardwares que compõem a solução.

c) O treinamento deverá ser realizado remotamente.

d) Caberá à CONTRATADA oferecer os recursos ferramentais para a viabilização do treinamento.

e) O treinamento deverá abordar de forma teórica e prática todas as funcionalidades solicitadas, com o objetivo de formar multiplicadores e profissionais capacitados na utilização das funcionalidades.

f) O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida pela CONTRATANTE, inclusive quanto à versão dos sistemas;

g) A carga horária mínima exigida para este treinamento é de 20 horas.

h) A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 4 (quatro) horas de instrução diária.

i) Deverá ser ministrada uma turma de treinamento que terá até 15 participantes.

j) Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento. No caso de material impresso, os custos para impressão e lógica para envio para cada participante são de responsabilidade da CONTRATADA.

k) 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 período de realização e o nome completo do participante.

l) O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.

m) As datas para a realização das atividades de treinamento e capacitação serão definidas previamente pela CONTRATANTE, respeitados os prazos de vigência da garantia.

n) O público-alvo deste treinamento são os analistas responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução. Os participantes serão indicados pela CONTRATANTE.

o) 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 CONTRATANTE.

p) Para ser considerado adequado, o treinamento deverá ser aprovado por pelo menos 70% dos participantes das turmas.

4.3.2.2. A avaliação dos treinamentos levará em consideração as questões listadas a seguir:

a) Avaliação do conteúdo:

I) Adequação dos conteúdos aos objetivos propostos;

II) Adequação das atividades desenvolvidas para alcance dos objetivos propostos;

III) Adequação do tempo para o alcance dos objetivos propostos;

IV) Profundidade com que o conteúdo foi abordado, considerando os objetivos propostos;

V) Integração entre teoria, pesquisa, prática e/ou aspectos da realidade;

VI) Qualidade dos exemplos utilizados;

VII) Aplicabilidade dos conhecimentos adquiridos no trabalho;

VIII) Contribuição para melhoria do desempenho no trabalho;

IX) Qualidade do material instrucional (apostilas, gráficos, etc.).

b) Avaliação do instrutor:

I) Formas/métodos de apresentação dos conteúdos;

II) Conhecimento dos temas tratados;

III) Visão prática dos conteúdos tratados;

IV) Uso de estratégias para motivar os alunos em relação ao conteúdo;

V) Incentivo à participação dos alunos em sala de aula;

VI) Incentivo à realização de atividades adicionais de aprofundamento do aprendizado.

c) Avaliação de ambiente e recursos:

I) Qualidade dos recursos tecnológicos utilizados pelo instrutor (áudio, vídeo, recursos para demonstração etc.);

II) Qualidade do ambiente virtual disponibilizado para o curso;

III) Qualidade da conexão disponibilizada pela CONTRATADA.

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

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

VII) O treinamento será considerado com qualidade suficiente, caso atinja uma nota igual ou superior a 7,5.

VIII) 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.

IX) 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 neste termo de referência.

4.3.2.3. **Cronograma do Treinamento**

Evento	Descrição	Prazo	Responsável
01	Confirmação do recebimento da Ordem de Serviço de Treinamento	Durante a vigência do Contrato	MPPI
02	Entrega do Cronograma de Treinamento	Até 7 dias úteis após o evento 01.	CONTRATADA
03	Avaliação do Cronograma de Treinamento	Até 7 dias úteis após o evento 02.	MPPI
04	Ajustes no Cronograma de Treinamento	Até 7 dias úteis após o evento 03.	CONTRATADA
05	Execução dos Treinamentos	Até 30 dias úteis após o evento 04.	CONTRATADA
06	Emissão do Termo de Recebimento Definitivo do Treinamento	Até 10 dias úteis após o evento 05.	MPPI

4.4. REQUISITOS LEGAIS

a) Lei Complementar n° 123/2006: Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e dá outras providências;

b) Lei Federal nº 14.133/2021: Estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;

c) Lei Federal nº 13.709/2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

d) Decreto nº 7.845/2012: Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

e) IN SGD/ME nº 94/2022: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. Instrução Normativa utilizada por falta de regulamentação local ou Estadual vigente e atualizada.

f) Resolução CNMP nº 283/2024: Disciplina, no âmbito do Ministério Público, os procedimentos relativos à contratação de Soluções de Tecnologia da Informação.

g) Nota Técnica nº 03/2020, que orienta o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades sujeitos à jurisdição do TCE-PI;

h) Lei nº 8.078/1990, que dispõe sobre a proteção do consumidor e dá outras providências;

i) Instrução Normativa SEGES nº 58/2022 (Dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP, para a aquisição de bens e a contratação de serviços e obras, no âmbito da administração pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital.), especialmente no que dispõe seu art. 12, considerando a análise dos estudos feitos pelo Tribunal de Justiça do Piauí, ao enfrentar semelhante necessidade, disponíveis no seu Portal da Transparência ((https://transparencia.tjpi.jus.br/licitacoes/702).

4.5. REQUISITOS DE MANUTENÇÃO

4.5.1. Requisitos de manutenção serão tratados no item 4.12, Manutenção e Assistência Técnica.

4.6. REQUISITOS TEMPORAIS

4.6.1. A solução deverá ser entregue, instalada e implantada conforme eventos abaixo:

Evento	Descrição	Prazo	Responsável
01	Confirmação do recebimento da Ordem de Serviço	Durante a vigência do Contrato	MPPI
02	Reunião Inicial e Apresentação do Projeto Executivo	Em até 10 (dez) dias úteis, contados a partir do evento 01	MPPI e CONTRATADA
03	Avaliação do Projeto Executivo	Em até 5 (cinco) dias úteis, contados a partir do evento 02	MPPI
04	Entrega dos produtos, equipamentos, softwares e licenças	Em até 45 (quarenta e cinco) dias úteis, contados a partir do evento 01	CONTRATADA
05	Emissão do Termo de Recebimento Provisório de Entrega de Equipamentos e Softwares	Em até 1 (dia) dia útil, contados a partir do evento 04	MPPI
06	Emissão do Termo de Recebimento Definitivo de Entrega de Equipamentos e Softwares	Em até 20 (vinte) dias úteis, contados a partir do evento 05	MPPI
07	Instalação, configuração e operacionalização dos produtos, equipamentos e softwares, além da entrega do *As Built* e repasse de conhecimento	Em até 30 (trinta) dias úteis, contados a partir do evento 04 e em caso de aprovação do evento 03	CONTRATADA

4.6.2. Para os itens relativos a treinamento, deverá ocorrer conforme eventos abaixo:

Evento	Descrição	Prazo	Responsável
01	Confirmação do recebimento da Ordem de Serviço de Treinamento	Durante a vigência do Contrato	MPPI
02	Entrega do Cronograma de Treinamento	Até 7 dias úteis após o evento 01.	CONTRATADA
03	Avaliação do Cronograma de Treinamento	Até 7 dias úteis após o evento 02.	MPPI
04	Ajustes no Cronograma de Treinamento	Até 7 dias úteis após o evento 03.	CONTRATADA

05	Execução dos Treinamentos	Até 30 dias úteis após o evento 04.	CONTRATADA
06	Emissão do Termo de Recebimento Definitivo do Treinamento	Até 10 dias úteis após o evento 05.	MPPI

4.7. REQUISITOS DE SEGURANÇA E PRIVACIDADE

4.7.1. Os serviços obedecerão, especialmente, às disposições legais da ABNT NBR 11515:2007 - Guia de práticas para segurança física, relativas ao armazenamento de dados.

4.7.2. A Contratada deverá exigir dos seus empregados, quando em serviço nas dependências do Contratante, o uso obrigatório de uniformes e crachás de identificação.

4.7.3. A Contratada não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado às informações de propriedade do MPPI.

4.7.4. A solução e os profissionais envolvidos na sua operacionalização deverão atender plenamente às seguintes condições:

a) Requisitos de segurança e procedimentos definidos para o acesso às dependências do MPPI, bem como requisitos de segurança da informação e de vedação de acesso e divulgação, conforme se aplique, a informações classificadas e privadas, e ainda a informações privilegiadas, isto é, aquelas que por qualquer motivo possam vir a representar vantagem mercantil competitiva;

b) Sigilo sobre iniciativas, projetos, decisões, dados e qualquer outro tipo de informação sensível de que venham a ter conhecimento durante a execução dos serviços, não podendo divulgá-las ou utilizá-las, durante a execução dos serviços e mesmo após seu encerramento, sem a expressa autorização do Ministério;

c) Deverão ser observados os requisitos de Segurança da Informação e Privacidade (SIP) de dados pessoais.

Observar conformidade com o seguinte arcabouço legislativo:

Decreto nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação.
Observar as recomendações das normas ABNT aplicáveis à Segurança da Informação (SI):

ABNT NBR ISO 22301:2013 - Sistemas de gestão de continuidade de negócios;
ABNT NBR ISO 22313:2015 - Orientações para uso da NBR 22301, no que tange à segurança e resiliência;
ABNT NBR ISO 27031:2015 - Diretrizes para a prontidão e continuidade dos negócios de tecnologia da informação;
ABNT NBR ISO 23081-1:2019 - Metadados para documentos de arquivo;
ABNT NBR ISO/IEC 27037:2012 - Diretrizes para identificação, coleta, aquisição e preservação de evidência digital;
ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;
ABNT NBR ISO/IEC 27014:2013 - Governança de segurança da informação;
ABNT NBR 16167:2013 - Diretrizes para classificação, rotulação e tratamento da informação;
ABNT NBR ISO/IEC 27017:2016 - Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002, para serviços em nuvem;
Obedecer à Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais, considerando, principalmente:
[...]

art. 7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

[...]

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

[...]

art. 26 - O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

[...]

IV - quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos.

[...]

§ 2º Os contratos e convênios de que trata o § 1º deste artigo deverão ser comunicados à autoridade nacional.

4.7.5. A solução deverá obedecer, integralmente, às políticas de Segurança da Informação do MPPI, com assinatura de Termo de Confidencialidade pelos funcionários alocados na prestação de serviços.

4.7.6. A Contratada deverá comunicar imediatamente ao CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do objeto, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.

4.8. REQUISITOS SOCIAIS, AMBIENTAIS, CULTURAIS E DE SUSTENTABILIDADE

4.8.1. Durante a execução de tarefas no ambiente do MPPI ou das demais instituições públicas envolvidas e durante reuniões de trabalho, sejam presenciais ou remotas, os profissionais envolvidos na sua operacionalização deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público.

4.8.2. Os relatórios gerenciais e técnicos elaborados pela CONTRATADA deverão ser produzidos no idioma "Português do Brasil", em linguagem formal.

4.8.3. A solução deverá providenciar a logística reversa de produtos e equipamentos sob sua responsabilidade, observando as normas específicas vigentes para a destinação final, inclusive para descarte de peças defeituosas e embalagens dos produtos utilizados, inclusive:

a) Lei nº 12.305, de 2 de agosto de 2010 - Política Nacional de Resíduos Sólidos;

b) Decreto nº 10.936, de 12 de janeiro de 2022 - Regulamenta a Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos;

c) Decreto nº 7.746, de 5 de junho de 2012; e

d) Instrução Normativa (IN) SLTI/MP nº 1, de 19 de janeiro de 2010.

4.8.4. Considerando o Decreto nº 7.746, de 5 de junho de 2012, que regulamentou o art. 3º, “caput”, da Lei nº 8.666, de 21 de junho de 1993, a Lei nº 12.305, de 2 de agosto de 2010 e a Instrução Normativa nº 01, de 19 de janeiro de 2010, para a presente contratação, aplicar-se-ão os seguintes critérios de sustentabilidade ambiental:

4.8.5. Utilização de tecnologias de virtualização, as quais podem ser definidas como soluções computacionais que permitem a execução de vários sistemas operacionais e seus respectivos softwares a partir de uma única máquina física ou mesmo maior utilização de um equipamento físico em sua divisão lógica virtual em várias unidades. Como benefícios da virtualização podem ser citados o melhor aproveitamento da infraestrutura existente, a redução no consumo de energia elétrica,diminuição na geração de lixo eletrônico e menor emissão de carbono;

4.8.6. Adotar processos administrativos na sua forma eletrônica, utilizando softwares aplicativos. Os documentos deverão ser gerados e mantidos em sua forma digital e, com o objetivo de garantir a integridade dos mesmos, nestes deverão ser utilizados recursos tecnológicos de segurança da informação. O objetivo da referida adoção é reduzir o número de cópias e impressões em papel;

4.8.7. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE.

4.8.8. A CONTRATADA deverá instruir e sensibilizar os seus empregados quanto à necessidade de racionalização de recursos no desempenho de suas atribuições, bem como das diretrizes de responsabilidade ambiental adotadas pelo CONTRATANTE.

4.8.9. As trocas de informações administrativas e de faturamento ocorrerão por meio do Sistema Eletrônico de Informações (SEI) do MPPI ou outro software de Gestão Eletrônica de Documentos (GED) que possa vir a substituir o SEI futuramente.

4.8.10. A solução deverá atender aos critérios de sustentabilidade ambiental, seguindo, no que couber, as diretrizes da Instrução Normativa SLTI/MPOG nº 01, de 19/01/2010, quanto ao uso de materiais, observando que esses sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme Normas ABNT NBR – 15448-1 e 15448-2.

4.8.11. Deverão ser observados os requisitos ambientais para a obtenção de certificação do Instituto

Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares.

4.8.12. Os equipamentos utilizados não poderão conter substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs) em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances).

4.9. REQUISITOS DE ARQUITETURA TECNOLÓGICA

4.9.1. Os requisitos de arquitetura tecnológica serão tratados em tópico próprio no item 2.5.

4.10. REQUISITOS DE PROJETO, IMPLEMENTAÇÃO E IMPLANTAÇÃO

4.10.1. A CONTRATADA deverá realizar a instalação de toda solução adquirida pelo prazo máximo de 75 (setenta e cinco) dias úteis, após a confirmação do recebimento da Ordem de Serviço;

4.10.2. Todos os componentes de hardware e software requeridos para atender as funcionalidades exigidas, mesmo que não estejam especificados e cotados na proposta, serão considerados como parte integrante da solução e deverão ser fornecidos devidamente licenciados pela Contratada, de acordo com definição do MPPI.

4.10.3. A CONTRATADA deverá criar e manter atualizada documentação das atividades, dos processos, testes, homologação, entrega e conferência, encontros de trabalho, compromissos e prazos, incluindo planos de trabalho, cronogramas, atas de reuniões, de modo a compor documentação (“as built”) a ser entregue à MPPI no final da implantação.

4.10.4. A CONTRATADA será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados aos serviços de implantação dos componentes das suas soluções objeto do Edital. Caso o diagnóstico aponte para problemas não relacionados aos componentes da solução, a MPPI deverá executar os procedimentos necessários, desde que devidamente comprovado pela CONTRATADA, a critério da MPPI.

4.10.5. 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 aqui descritos.

4.10.6. Será reservado o direito de propor modificações nesse documento à CONTRATANTE, no sentido de melhor atender ao bom andamento dos trabalhos ou à própria conveniência da instituição. Caberá à CONTRATADA acolher as demandas com relação aos pedidos de modificação nesse documento, que poderão ocorrer a qualquer tempo ao longo da execução da implantação, sem, em nenhuma hipótese, acrescentar qualquer custo adicional para o MPPI com respeito à solução proposta.

4.10.7. A CONTRATADA deverá apresentar ao setor técnico do MPPI em reunião própria e no prazo de até 10 (dez) dias úteis após a confirmação do recebimento da Ordem de Serviço, documento que balizará o acompanhamento de todo o projeto de implantação. Este documento deverá detalhar todas as fases, atividades, ações, recursos envolvidos (humanos e materiais) e prazos.

4.10.8. A implantação dos serviços contratados somente poderá ser iniciada após a aprovação por parte da equipe técnica do MPPI.

4.10.9. A implementação deverá ser iniciada de forma presencial, por pelo menos um prazo de 1 (uma) semana. Após este prazo as configurações poderão ser feitas de forma remota.

4.10.10. Deverá ser fornecido Relatórios de Pré-Requisitos de Instalação e Operação dos Produtos, contendo, por produto, informação de todos os seus pré-requisitos de instalação e operação, a citar: todas conexões físicas e lógicas, e configuração do appliance necessárias para interligação da solução com o ambiente proposto pela CONTRATADA com apoio da CONTRATANTE referente as especificidades da sua infraestrutura;

4.10.11. Deverá ser efetuado levantamento de requisitos, coletando-se informações do ambiente computacional do CONTRATANTE, por meio de reuniões e verificações in loco, com o objetivo de documentar e analisar informações quanto aos componentes de infraestrutura bem como estabelecer os parâmetros necessários à configuração e integração da solução;

4.10.12. A CONTRATADA deverá prestar consultoria para implantar toda a solução de acordo com as melhores práticas da indústria de TI, alocando profissionais devidamente capacitados e dentro dos níveis dos serviços contratados pelo órgão;

4.10.13. Para finalizar fase de instalação e ter início a fase de configuração, a CONTRATADA deverá apresentar os seguintes documentos:

I - Plano de Configuração:

a) Configuração da solução;

II - Plano de Execução:

a) Cronograma de atividades;

b) Responsáveis técnicos pelas atividades;

III - Plano de Testes.

4.10.14.Após instalação física da solução, deverão ser realizadas as configurações avançadas, que irão efetivamente integrar a nova solução ao ambiente computacional do CONTRATANTE;

4.10.15.A configuração deverá ser agendada junto à equipe técnica do CONTRATANTE com antecedência mínima de 48 (quarenta e oito) horas e respeitar o cronograma entregue;

4.10.16.As atividades de instalação dos equipamentos deverão ocorrer, preferencialmente, em dias úteis, no período das 08h às 15h, horário do local da instalação;

4.10.17.Caso a configuração possa provocar indisponibilidade nos serviços, a instalação poderá ocorrer em horário noturno e/ou fim de semana, a critério do CONTRATANTE;

4.10.18.Os procedimentos envolvidos nos processos de configuração deverão ser previamente aprovados pelo CONTRATANTE;

4.10.19.Após a configurações deverá ser agendado a execução do plano de testes para demonstrar efetividade das configurações realizadas e funcionamento de cada característica da Solução adquirida.

4.11. REQUISITOS DE GARANTIA TECNOLÓGICA

4.11.1. Os itens adquiridos nesse processo deverão possuir garantia do fabricante ou autorizada no Brasil com validade mínima de 36 meses, contados a partir do recebimento definitivo da solução.

4.11.2. A solução deverá atender às disposições do artigo nº. 31 da Lei Federal nº. 8.078 de 11/09/1990 (Código de Defesa do Consumidor) que diz: “A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores”.

4.12. MANUTENÇÃO E ASSISTÊNCIA TÉCNICA

4.12.1. Considera-se como requisitos a manutenção contínua e suporte técnico ao longo de todo o contrato, incluindo período de garantia dos serviços e equipamentos:

4.12.1.1. Os serviços poderão ser prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pelo fabricante da solução, sem prejuízo a responsabilidade integral da CONTRATADA quanto aos atendimentos dos níveis de serviço;

4.12.1.2. Entende-se por “Suporte” ou “Manutenção”, doravante denominada unicamente como “Suporte”, toda atividade do tipo “corretiva” não periódica que variavelmente poderá ocorrer, durante todo o período de garantia. A mesma possui suas causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos mesmos. Este “Suporte” inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

4.12.1.3. Do hardware: desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados

4.12.1.4. Do software: desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados;

4.12.1.5. Quanto às atualizações pertinentes aos softwares: Entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service packs”, novas “releases”, “versions”, “builds”, “upgrades”, englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia do contrato.

4.12.1.6. A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de software (bugs) ou falhas comprovadas de

segurança em software ou firmware dos aparelhos que integrem o objeto do contrato.

4.12.1.7. O atendimento deste requisito está condicionado a liberação pelo Fabricante dos pacotes de correção e/ou novas versões de software.

4.12.1.8. É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de “Suporte” do tipo “preventiva” que pela sua natureza reduza a incidência de problemas que possam gerar “Suporte” do tipo “corretiva”. As manutenções do tipo “preventiva” não podem gerar custos a CONTRATANTE.

4.12.1.9. A manutenção técnica do tipo “corretiva” será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone (com número do tipo “0800”) ou Internet ou e-mail ou fac-símile ou outra forma de contato;

4.12.1.10. Os serviços de “Suporte” incluem:

a) Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação e desenvolvimento;

b) Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;

c) Esclarecimento de dúvidas sobre o funcionamento e operação da solução;

d) Instalação de novas versões ou atualizações e patches, quando disponibilizados pelo Fabricante;

4.12.1.11. A CONTRATADA deve disponibilizar a central atendimento 24 horas por dia, 7 dias da semana (incluindo feriados) e equipe com conhecimentos sólidos no funcionamento e operação da solução de gestão.

4.12.1.12. O serviço de “Suporte” deve disponibilizar os seguintes tipos de atendimento:

a) Nível I - Atendimento Help Desk: chamados abertos através de ferramenta ITSM (Information Technology Service Management), telefônica ou e-mail ou outra forma de contato, em regime de 24x7: 24 horas por dia, 7 dias da semana (incluindo feriados). Esse serviço deve atender demandas dos usuários referentes ao funcionamento da solução, que decorram de problemas de funcionamento.

b) Nível II - Atendimento Remoto: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pela CONTRATANTE, mediante prévia autorização e seguindo os padrões de segurança da CONTRATANTE, objetivando análise e solução remota dos problemas apresentados.

c) Nível III - Atendimento Presencial (On-Site): atendimentos técnicos realizados nas dependências do CONTRATANTE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto.

Todo “Suporte” deve ser solicitada inicialmente via Help Desk (Nível I), ficando a transferência do atendimento para o Atendimento Remoto (Nível II) condicionado à autorização da CONTRATANTE.

4.12.1.13. Todo “Suporte” solicitada inicialmente via Help Desk (Nível I), deve ser transferido para o Atendimento Presencial (Nível III) quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

4.12.1.14. Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte Acordo de Níveis de Serviços (ANS) e sua SEVERIDADE:

a) SEVERIDADE URGENTE – Solução totalmente inoperante.

Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado;

Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.

b) SEVERIDADE IMPORTANTE – Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.

Prazo máximo de início de atendimento de até 24 horas úteis contadas a partir do horário de abertura do chamado;

Prazo máximo de resolução do problema de até 48 horas úteis contadas a partir do início do atendimento.

c) SEVERIDADE NORMAL – Solução não inoperante mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.

Prazo máximo de início de atendimento de até 48 horas úteis contadas a partir do horário de abertura do chamado;

Prazo máximo de resolução do problema de até 96 horas úteis contadas a partir do início do atendimento.

d) SEVERIDADE EXTERNO – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela CONTRATADA. Neste caso, ficam suspensos todos os prazos de atendimento até que a CONTRATANTE resolva os problemas externos que provocam a inoperância da solução. Após a CONTRATANTE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução.

e) SEVERIDADE INFORMAÇÃO – Solicitações de informações diversas ou dúvidas sobre a solução.

Prazo máximo de resposta de até 5 dias úteis, contados a partir da data de abertura da ocorrência.

4.12.1.15. Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

4.12.1.16. Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e severidade do chamado.

4.12.1.17. A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

4.12.1.18. dia A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

4.13. REQUISITOS DE CAPACITAÇÃO TÉCNICA

4.13.1. O CONTRATANTE não custeará cursos e/ou treinamentos aos profissionais da CONTRATADA. A empresa CONTRATADA é responsável pela contínua reciclagem e aprimoramento do conhecimento dos seus técnicos, de modo a capacitá-los a atender as demandas atuais e futuras do CONTRATANTE, bem como às atualizações tecnológicas e/ou produtos que vierem a ser implementados durante a vigência contratual - além das qualificações técnicas mínimas já previstas.

4.13.2. A CONTRATADA promover a divulgação periódica (ou quando solicitado) de informações relativas a acesso, triagem, avaliação e consulta, por meio de publicações ou e-mails institucionais, que contenham orientações didáticas e de linguagem simples, tais como cartilhas, checklists e passo a passos.

4.13.3. Na linha da capacitação, a CONTRATADA deverá fornecer um treinamento da solução (da respectiva solução a ser ofertada) conforme os seguintes requisitos:

Requisito	Descrição
01	O treinamento contemplará todos os softwares que compõem a solução.
02	Deverá abordar de forma teórica e prática todas as funcionalidades solicitadas.
03	Possuir carga horária adequada e compatível com o conteúdo a ser ministrado.
04	O público-alvo deste treinamento são os servidores responsáveis pela execução de atividades de administração e auditoria dos ambientes monitorados pela solução.
05	O treinamento deverá ser realizado utilizando-se solução idêntica à adquirida, inclusive quanto à versão dos sistemas.
06	A atividade de treinamento e capacitação deverá ser realizada em dias úteis, com duração máxima de até 4 (seis) horas de instrução diária.
07	Deverá ser ministrada uma turma de treinamento que terá até 15 participantes.
08	Deverá ser fornecido material em formato digital ou impresso do conteúdo do treinamento.
09	O(s) instrutor(es) deverá(ão) ser comprovadamente certificado(s) nos sistemas e/ou ferramentas fornecidos no escopo da solução.
10	A avaliação do sucesso do treinamento deverá ser mensurada pela turma através de mecanismos objetivos.

4.14. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

4.14.1. Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão:

4.14.2. Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o grupo pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

I - Para fins da comprovação de que trata este subitem, o(s) atestado(s) deverá(ão) dizer respeito à

execução anterior, pelo licitante, dos seguintes serviços:

a) **GRUPO 1:** fornecimento de solução de segurança, auditoria, e prevenção de ameaças à base de dados não estruturados, com licenciamento de software e prestação de serviços agregados, tais como os serviços de atualização de versão, manutenção e suporte técnico, e/ou de serviços de consultoria, pelo período mínimo de 12 (doze)meses;

b) **GRUPO 2:** fornecimento de solução de gestão e controle de acesso para identidades privilegiadas, com licenciamento de software e prestação de serviços agregados, tais como os serviços de atualização de versão, manutenção e suporte técnico, e/ou de serviços de consultoria, pelo período mínimo de 12 (doze) meses;

II - atividade econômica principal ou secundária especificadas no contrato social vigente;

Os atestados deverão referir-se ao fornecimento e serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

II - Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior;

IV - Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante;

V- Será aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os 12 (doze) meses serem ininterruptos;

4.15. REQUISITOS DE FORMAÇÃO DA EQUIPE

4.15.1. A equipe técnica será composta dos profissionais envolvidos diretamente na prestação dos serviços e execução das etapas, sendo os responsáveis por desempenhar atividades sob sua competência.

4.16. REQUISITOS DE METODOLOGIA DE TRABALHO

4.16.1. A metodologia de trabalho será baseada no conceito de delegação de responsabilidade, onde o CONTRATANTE é responsável pela gestão e fiscalização do contrato e pela atestação da aderência aos padrões de qualidade exigidos, e a CONTRATADA como responsável pela execução dos serviços e gestão dos seus recursos humanos, não será admitida a subcontratação do objeto.

4.16.2. Todas as atividades devem estar de acordo com as especificações e melhores práticas dos fabricantes dos equipamentos/softwares e com as recomendações de organizações padronizadoras do segmento.

4.16.3. A CONTRATADA poderá contar com o apoio técnico direto do fabricante dos componentes fornecidos no escopo das especificações técnicas, devendo arcar com todas as despesas decorrentes da solicitação do referido apoio, inclusive com os custos de comunicação relacionados à abertura e acompanhamento de chamados técnicos.

4.16.4. Todas as despesas referentes a transporte, alimentação, hospedagem e demais despesas operacionais da equipe alocada ocorrerão a expensas da CONTRATADA.

4.16.5. O MPPI oferecerá acesso físico às suas instalações desde que os funcionários da CONTRATADA estejam devidamente identificados, bem como autorização e acesso aos recursos computacionais e apoio técnico às atividades de coordenação e gerência da implantação, desde que absolutamente dentro do escopo das atividades da equipe do MPPI e a seu critério.

4.17. REQUISITOS DE SEGURANÇA DOS ATIVOS DE TI

4.17.1. A contratação deve atender aos requisitos de segurança dos ativos de TI, conforme estabelece a Resolução CNMP nº 156, de 13 de dezembro de 2015, que institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, bem como a nova Lei de Licitações e Contratos Administrativos (Lei nº 14.133/2021);

4.18. OUTROS REQUISITOS APLICÁVEIS

4.18.1. REAJUSTE

4.18.1. O Contrato terá vigência de 36 (trinta e seis) meses, a contar da data de assinatura;

4.18.2. Dentro do prazo de vigência do contrato, os preços contratados são fixos e irreajustáveis no prazo de um ano contado da data orçamento estimado, aplicando-se o Índice de Custo de Tecnologia da Informação (ICTI), do Instituto de Pesquisa Econômica Aplicada (IPEA) exclusivamente para as obrigações

iniciadas e concluídas após a ocorrência da anualidade;

4.18.3. O orçamento estimado pela Administração baseou-se nas planilhas referenciais datadas de 22/07/2024;

4.18.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste;

4.18.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo;

4.18.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo;

4.18.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor;

4.18.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo;

4.18.8. O reajuste será realizado por apostilamento.

4.18.2. SUBCONTRATAÇÃO

4.18.2.1. Não é admitida a subcontratação do objeto contratual.

4.18.3. MARGENS DE PREFERÊNCIA

4.18.3.1. Não será aplicada margem de preferência na presente contratação.

4.18.4. GARANTIA DE CONTRATAÇÃO

4.18.4.1. Será exigida a garantia da contratação de que tratam os Art. 96 e seguintes da Lei nº 14.133, de 2021, no percentual e condições descritas nas cláusulas do contrato.

4.18.4.2. Em caso opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.18.4.3. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 dias úteis após a assinatura do contrato.

4.18.4.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

4.18.4.5. Para o item 4.18.4.1, a CONTRATADA deverá apresentar obrigatoriamente GARANTIA no montante de 5 % (cinco por cento) sobre o valor anual do contrato, assim como nas subsequentes prorrogações, podendo optar por qualquer das modalidades previstas no art. 96 da Lei nº 14.133, de 2021 conforme descrito no item anterior;

4.18.4.6. A CONTRATADA se obriga a manter esta Garantia durante toda a vigência do contrato;

4.18.4.7. Caso o Recebimento Definitivo se prolongue além do prazo estabelecido neste Termo de Referência, por ação ou omissão da CONTRATADA, essa garantia deverá também ser reforçada;

4.18.5. CONSÓRCIOS

4.18.5.1. Em observância ao princípio da ampla concorrência que integra a regra do edital, permitirá a participação de consórcio, desde que atendidas as demais regras do edital e a legislação aplicável, especialmente a Lei nº 14133, art 15.

4.18.5.2. Salvo vedação devidamente justificada no processo licitatório, pessoa jurídica poderá participar de licitação em consórcio, observadas as seguintes normas:

I - comprovação de compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados;

II - indicação da empresa líder do consórcio, que será responsável por sua representação perante a Administração;

III - admissão, para efeito de habilitação técnica, do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, do somatório dos valores de cada consorciado;

IV - impedimento de a empresa consorciada participar, na mesma licitação, de mais de um consórcio ou de forma isolada;

V - responsabilidade solidária dos integrantes pelos atos praticados em consórcio, tanto na fase de licitação quanto na de execução do contrato."

5. PAPÉIS E RESPONSABILIDADES

5.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, Art. 117, caput), observando-se, em especial, as rotinas a seguir.

I. Pelo CONTRATANTE:

a) Fiscalização técnica

Caberá ao fiscal técnico do contrato e, nos seus afastamentos e seus impedimentos legais, ao seu substituto, em especial:

I) Prestar apoio técnico e operacional ao gestor do contrato com informações pertinentes às suas competências;

II) Anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

III) Emitir notificações para a correção de rotinas ou de qualquer inexatidão ou irregularidade constatada, com a definição de prazo para a correção;

IV) Informar ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem a sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

V) Comunicar imediatamente ao gestor do contrato quaisquer ocorrências que possam inviabilizar a execução do contrato nas datas estabelecidas;

VI) Fiscalizar a execução do contrato para que sejam cumpridas as condições estabelecidas, de modo a assegurar os melhores resultados para a administração, com a conferência das notas fiscais e das documentações exigidas para o pagamento e, após o ateste, que certifica o recebimento provisório, encaminhar ao gestor de contrato para ratificação;

VII) Comunicar ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

VIII) Participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal administrativo e com o setorial, conforme o disposto no inciso vii do caput do Art. 21;

IX) Auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado, conforme o disposto no inciso viii do caput do Art. 21; e

X) Realizar o recebimento provisório do objeto do contrato referido no Art. 25, mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico.

b) Fiscalização administrativa

Caberá ao fiscal administrativo do contrato e, nos seus afastamentos e seus impedimentos legais, ao seu substituto, em especial:

I) prestar apoio técnico e operacional ao gestor do contrato, com a realização das tarefas relacionadas ao controle dos prazos relacionados ao contrato e à formalização de apostilamentos e de termos aditivos, ao acompanhamento do empenho e do pagamento e ao acompanhamento de garantias e glosas;

II) verificar a manutenção das condições de habilitação da contratada, com a solicitação dos documentos comprobatórios pertinentes, caso necessário;

III) examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias e, na hipótese de descumprimento, observar o disposto em ato do Secretário de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia;

IV). atuar tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

V) participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal técnico e com o setorial, conforme o disposto no inciso VII do caput do Art. 21;

VI) auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo

contratado, conforme o disposto no inciso VIII do caput do Art. 21; e

VII) realizar o recebimento provisório do objeto do contrato referido no Art. 25, mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo.

c) Gestor do Contrato

Caberá ao gestor do contrato e, nos seus afastamentos e seus impedimentos legais, ao seu substituto, em especial:

I) coordenar as atividades relacionadas à fiscalização técnica, administrativa e setorial, de que tratam os incisos II, III e IV do caput do Art. 19;

II) acompanhar os registros realizados pelos fiscais do contrato das ocorrências relacionadas à execução do contrato e as medidas adotadas, e informar à autoridade superior àquelas que ultrapassarem a sua competência;

III) acompanhar a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e de pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais;

IV) coordenar a rotina de acompanhamento e de fiscalização do contrato, cujo histórico de gerenciamento deverá conter todos os registros formais da execução, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, e elaborar relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração;

V) coordenar os atos preparatórios à instrução processual e ao envio da documentação pertinente ao setor de contratos para a formalização dos procedimentos de que trata o inciso I do caput do Art. 19;

VI) elaborar o relatório final de que trata a alínea "d" do inciso VI do § 3º do Art. 174 da Lei nº 14.133, de 2021, com as informações obtidas durante a execução do contrato;

VII) coordenar a atualização contínua do relatório de riscos durante a gestão do contrato, com apoio dos fiscais técnico, administrativo e setorial;

VIII) emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, a constarem do cadastro de atesto de cumprimento de obrigações conforme disposto em regulamento;

IX) realizar o recebimento definitivo do objeto do contrato referido no Art. 25, mediante termo detalhado que comprove o atendimento das exigências contratuais; e

X) tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o Art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso.

d) As figuras citadas abaixo serão consideradas e designadas unicamente como “fiscais do contrato” conforme estabelecido no ATO PGJ 462/2013, atualizado pelo ATO PGJ 806/2018 até que sejam regulamentadas pelo MPPI.

II. Pela CONTRATADA:

a) Representante legal: pessoa formalmente designada e devidamente autorizada a firmar contrato em nome da CONTRATADA;

b) Preposto: nomeado pelo representante legal no início da execução contratual, nos termos do Art. 118 da Lei nº 14.133/21, que atuará como representante da CONTRATADA durante a execução contratual.

5.2. São deveres e responsabilidades do CONTRATANTE

a) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

b) Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

c) Receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

d) Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando

ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

e) Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

f) Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;

h) Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

5.3. São deveres e responsabilidades da CONTRATADA

a) Indicar formalmente preposto apto a representá-la junto ao CONTRATANTE, que deverá responder pela fiel execução do contrato;

b) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

c) Reparar quaisquer danos diretamente causados ao 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 contrato pelo CONTRATANTE;

d) Propiciar todos os meios necessários à fiscalização do contrato pelo CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

e) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

f) Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

g) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

h) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

i) Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do CONTRATANTE ou da nova empresa que continuará a execução do contrato, quando for o caso;

j) Fazer a transição contratual, quando for o caso;

k) Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

l) Atender as demandas com agilidade e qualidade, independentemente da quantidade de ordens de serviço, observando-se os limites totais previstos para cada item contratado;

m) Reconhecer o Gestor do Contrato, bem como outros servidores que forem indicados pelo CONTRATANTE, para realizar as solicitações relativas aos contratos a serem firmados, tais como manutenção, configuração, entre outras;

n) Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

o) Executar o objeto do certame em estreita observância aos ditames estabelecido pela Lei n°13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD);

p) Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pelo CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

q) Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE, por intermédio de preposto designado para acompanhamento;

r) Paralisar, por determinação do CONTRATANTE, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de dados, de pessoas ou bens de terceiros;

s) Apresentar Nota Fiscal/Fatura com a descrição dos serviços prestados, nas condições do Termo de Referência, como forma de dar início ao processo de pagamento pelo CONTRATANTE;

t) Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da adjudicação da licitação oriunda do Termo de Referência;

u) Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo Fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

v) Dar ciência imediata e por escrito ao CONTRATANTE de qualquer anormalidade que verificar na execução dos serviços;

x) Prestar ao CONTRATANTE, por escrito, os esclarecimentos solicitados e atender prontamente as reclamações sobre seus serviços; Responder por quaisquer danos, perdas ou prejuízos causados diretamente ao CONTRATANTE ou a terceiros decorrentes da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização do CONTRATANTE em seu acompanhamento;

y) Obedecer às normas e rotinas do CONTRATANTE, em especial as que disserem respeito à segurança, à guarda, à manutenção e à integridade das informações existentes ou geradas durante a execução dos serviços;

z) Implantar, de forma adequada, a planificação, execução e supervisão permanente dos serviços, de maneira a não interferir nas atividades do CONTRATANTE, respeitando suas normas de conduta;

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. INTRODUÇÃO

6.1.1. Em conformidade com o art. 24 da Resolução CNMP nº 283, de 05 de fevereiro de 2024, o Modelo de Execução do Contrato deverá contemplar as condições necessárias ao fornecimento das soluções de TI.

6.2. ROTINAS DE EXECUÇÃO

6.2.1. DO ENCAMINHAMENTO FORMAL DAS DEMANDAS

6.2.1.1. O gestor do contrato emitirá a Ordem de serviço (OS) para a entrega dos serviços desejados.

6.2.1.2. A CONTRATADA deverá fornecer os objetos com as mesmas configurações/especificações e quantidades definidas na OS.

6.3. FORMA DE EXECUÇÃO E ACOMPANHAMENTO DO CONTRATO

6.3.1. CONDIÇÕES DE ENTREGA

I. O prazo de entrega dos produtos, equipamentos, softwares e licenças são de 45 (quarenta e cinco) dias úteis, a contar da confirmação do recebimento da OS.

I. Local de entrega dos equipamentos, softwares e licenças

a. Entrega dos equipamentos

- A entrega dos equipamentos será no **Edifício Sede do Ministério Público do Estado do Piauí, Rua Álvaro Mendes 2294, Centro, CEP: 64000-060, Teresina-Piauí, telefones: (86) 2222-8000 ramal: 8031**, de segunda a sexta-feira no horário das 8:00h às 14:00h, exceto nos feriados e dias facultativos, correndo por conta da contratada todas as despesas de embalagem, seguros, transporte, tributos, encargos trabalhistas e previdenciários, decorrentes do serviço e equipamentos necessários para o seu funcionamento, devendo a entrega ser agendada, com até 24h de antecedência;

b. Entrega do software e licenças

No caso do software e de licenças em que deverá ocorrer o download do aplicativo bem como exista relação de chaves de licença para ativação, deverá ser encaminhado um e-mail informativo para cti@mppi.mp.br;

II. Local de execução dos serviços

Os serviços técnicos de instalação, configuração e manutenção dos equipamentos, deverão acontecer na sede Centro do Ministério Público do Estado do Piauí, no endereço Rua Álvaro Mendes, 2294 - Centro Teresina-PI - CEP 64000-060.

- De segunda-feira a sexta-feira, das 8 horas às 14 horas;

6.3.2. FORMAS DE TRANSFERÊNCIA DE CONHECIMENTO

6.3.2.1. Os requisitos de arquitetura tecnológica serão tratados em tópico próprio no item 9.5.2.

6.3.3. PROCEDIMENTOS DE TRANSIÇÃO E FINALIZAÇÃO DO CONTRATO

6.3.3.1. Os procedimentos de transição e finalização do contrato serão tratados em tópico próprio no item 9.

6.3.4. QUANTIDADE MÍNIMA DE BENS OU SERVIÇOS PARA COMPARAÇÃO E CONTROLE

GRUPO 1 - ITENS 1 A 6			
Item	**Descrição**	**Unidade**	**Quantidade**
1	Licença para visibilidade, análise de dados locais, comportamento e prevenção de ameaças por 36 meses - **CATSER: 24333**	Usuários	1600
2	Licença para visibilidade, análise de dados em nuvem, comportamento e prevenção de ameaças por 36 meses - **CATSER: 24333**	Usuários	1600
3	Licença para visibilidade, análise de dados em caixas postais, comportamento e prevenção de ameaças por 36 meses - **CATSER: 24333**	Usuários	1600
4	Serviço de instalação e configuração para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. - **CATSER: 26972**	Serviço	2
5	Manutenção e Suporte Técnico para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. - **CATSER: 26972**	Serviço	2
6	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. - **CATSER: 3840**	Turma	2
GRUPO 2 - ITENS 7 A 17			
Item	**Descrição**	**Unidade**	**Quantidade**
7	Cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses **- CATSER: 469726**	Unidade	2
8	Balanceador de carga para cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses**- CATSER: 469726**	Unidade	2
9	Subscrição para usuários com acesso privilegiado por 36 meses**- CATSER: 24333**	Usuários	40
10	Subscrição para servidores físicos e virtuais por 36 meses**- CATSER: 24333**	Servidores	400
11	Subscrição para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN por 36 meses **- CATSER: 24333**	Equipamentos	1000
12	Subscrição para aplicações não conteinerizadas com senha embutida (hard coded) por 36 meses **- CATSER: 24333**	Aplicações	80
13	Subscrição para acesso remoto seguro por 36 meses -**CATSER: 24333**	Unidade	60

14	Subscrição de gerenciamento de certificados digitais por 36 meses **- CATSER: 24333**	Unidade	2
15	Serviço de instalação e configuração para solução de controle de acesso de usuários privilegiados. - **CATSER: 26972**	Serviço	2
16	Manutenção e Suporte Técnico para solução de controle de acesso de usuários privilegiados. - **CATSER: 26972**	Serviço	2
17	Treinamento para solução de controle de acesso de usuários privilegiados. - **CATSER: 3840**	Turma	2

6.3.5. MECANISMOS FORMAIS DE COMUNICAÇÃO

Como meios de comunicação oficiais entre o CONTRATANTE e a CONTRATADA, poderão ser utilizados os seguintes:

a) Portal de atendimento (com usuário e senha);

b) E-mail;

c) Relatório de Nível de Serviço;

c) Termo de Notificação;

d) Relatórios gerados pelo sistema de informação utilizado na prestação dos serviços.

Os documentos relacionados acima terão validade legal para fins de aferição de resultados, comprovação, contestação, pagamentos, entre outros.

Adicionalmente, também poderão ser utilizadas ligações telefônicas, sem ônus para o CONTRATANTE (0800), para abertura de chamados.

6.3.6. FORMA E PRAZO DE PAGAMENTO

6.3.6.1. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato, item 8, Critérios de Medição e Procedimentos para Pagamento.

6.3.7. VIGÊNCIA CONTRATUAL

6.3.7.1. O prazo de vigência do contrato é de 36 (trinta e seis) meses, prorrogável por até 84 meses, na forma dos artigos 106 e 107 da Lei n° 14.133/2021.

6.3.8. TERMO DE CIÊNCIA E MANUTENÇÃO DE SIGILO

6.3.8.1. A solução contratada deverá respeitar a adequação à legislação vigente, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

6.3.8.2. A solução contratada deverá observar a Norma Brasileira ABNT NBR ISO/IEC 27002.

6.3.8.3. A Contratada deverá manter a integridade da rede de dados e das informações do MPPI durante a prestação dos serviços.

6.3.8.4. A Contratada deverá respeitar a Política de Segurança da Informação do MPPI bem como demais políticas e normas internas que poderão ser instituídas durante a vigência do contrato.

6.3.8.5. A Contratada deverá guardar sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os 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 pelo Contratante a tais documentos.

6.3.8.6. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, deverá ser assinado por um representante da Contratada e encontra-se no ANEXO I. A Contratada deverá providenciar a assinatura do Termo de Ciência, disponível no ANEXO II, por todos os seus colaboradores que estejam relacionados com a execução do projeto. O Termo de Compromisso e o Termo de Ciência deverão ser entregues assinados durante a reunião inicial.

6.3.8.7. Qualquer unidade de armazenamento, tais como SSDs, HDDs e memórias, utilizadas deverão permanecer em posse de Contratante mesmo após o uso, após dano à unidade ou após o término do contrato. Caso seja necessária a remoção de alguma unidade de armazenamento, esta ação deverá ser realizada no prédio do CTI/MPPI e imediatamente entregue a Contratante. Caso haja necessidade de

manutenção fora das dependências do CTI/MPPI as unidades de armazenamento deverão ser removidas dentro das dependências do CTI/MPPI e deverão ficar sob responsabilidade da Contratante enquanto perdurar o conserto.

7. MODELO DE GESTÃO DO CONTRATO

7.1. INTRODUÇÃO

7.1.1. Em conformidade com o art. 25. da Resolução CNMP nº 283, de 05 de fevereiro de 2024, o Modelo de Gestão do Contrato deverá contemplar as condições necessárias ao fornecimento das soluções de TI.

7.1.2. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.1.3. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.1.4. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

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

7.2. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

7.2.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

a) Der causa à inexecução parcial do contrato,

b) Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo.

c) Der causa à inexecução total do contrato.

d) Deixar de entregar a documentação exigida para o certame.

e) Não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado.

f) Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.

g) Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado.

h) Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante o pregão eletrônico ou execução do contrato.

i) Fraudar a contratação ou praticar ato fraudulento na execução do contrato.

j) Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.

k) Praticar atos ilícitos com vistas a frustrar os objetivos do certame.

l) Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

m) Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

I. Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei).

II. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas b, c, d, e, f e g do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §4º, da Lei).

III. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas h, i, j, k e l do subitem acima deste Contrato, bem como nas alíneas b, c, d, e, f e g, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei).

IV. As multas serão aplicadas nas seguintes gradações:

1. Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias corridos.
2. Multa compensatória de 5% (cinco por cento) sobre o valor do contrato, no caso de inexecução total do objeto.

7.2.2. No caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima,

será aplicada de forma proporcional à obrigação inadimplida.

7.2.3. Considera-se inexecução total, entre outros, o atraso injustificado no prazo de entrega/prestação superior a 15 (quinze) dias.

7.2.4. O descumprimento de obrigações contratuais acessórias, a exemplo da garantia do objeto, sujeitará a CONTRATADA à multa de até 2% (dois por cento) do valor empenhado.

7.2.5. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º).

7.2.6. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º).

7.2.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157).

7.2.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º).

7.2.9. Em caráter excepcional, como medida de cautela, o Contratante poderá reter o valor presumido da multa, antes da instauração do procedimento administrativo.

7.2.10. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

7.2.11. Na aplicação das sanções serão considerados (art. 156, §1º):

a) a natureza e a gravidade da infração cometida.

b) as peculiaridades do caso concreto.

c) as circunstâncias agravantes ou atenuantes.

d) os danos que dela provierem para o Contratante.

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

7.2.12. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

7.2.13. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160).

7.2.14. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161).

7.2.15. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

8. CRITÉRIOS DE MEDIÇÃO E PROCEDIMENTOS PARA PAGAMENTO

8.1. PROCEDIMENTOS PARA RECEBIMENTO PROVISÓRIO E DEFINITIVO

8.1.1. Os serviços de TIC serão recebidos provisoriamente, de forma sumária, em até 1 (um) dia útil após a entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

8.1.2. Os serviços de TIC poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 (cinco) dias úteis, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

8.1.3. O recebimento definitivo ocorrerá no prazo de 20 (vinte) dias úteis, a contar do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado..

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

8.1.5. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.1.6. O prazo para a solução, pela CONTRATADA, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

8.1.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético profissional pela perfeita execução do contrato.

8.2. LIQUIDAÇÃO

8.2.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (dez) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do Art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022;

8.2.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do Art. 75 da Lei nº 14.133, de 2021;

8.2.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- O prazo de validade;
- A data da emissão;
- Os dados do contrato e do órgão CONTRATANTE;
- O período respectivo de execução do contrato;
- O valor a pagar; e
- Eventual destaque do valor de retenções tributárias cabíveis.

8.2.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a CONTRATADA providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao CONTRATANTE;

8.2.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no Art. 68 da Lei nº 14.133, de 2021;

8.2.6. AAdministração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (IN nº 3, de 26 de abril de 2018).

8.2.7. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE;

8.2.8. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

8.2.9. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa;

8.2.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

8.3. PRAZO PARA PAGAMENTO

8.3.1. Os pagamentos serão realizados em 3 (três) parcelas anuais, totalizando 36 meses conforme vigência contratual, conforme prazos e condições presentes na tabela a seguir:

Id	Evento	Condição de Pagamento (1ª Parcela anual - Referente a 12 meses)	Condição de Pagamento (2ª Parcela anual - Referente a 24 meses)	Condição de Pagamento (3ª Parcela anual - Referente a 36 meses)	Prazo para realização do Evento
1	Entrega dos equipamentos, dos softwares e das licenças ou subscrições e instalação, configuração e operacionalização da solução. (Itens 1, 2, 3,4,5 - Grupo 1 e Itens 7,8,9,10,11,12,13,14,15,16 - Grupo 2)	Pagamento de 100% (cem por cento) da parcela anual, mediante Termo de Aceite Definitivo de Entrega dos Softwares, após o ateste do recebimento das licenças, instalação de todos os componentes da solução no ambiente do MPPI e após recebimento da Nota Fiscal.	Pagamento de 100% (cem por cento) da parcela anual, mediante Termo de Aceite Definitivo	Pagamento de 100% (cem por cento) da parcela anual, mediante Termo de Aceite Definitivo	Até 10 (dez) dias úteis contados da finalização da liquidação da despesa
3	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. (Item 6 - Grupo 1)	Pagamento em parcela única, mediante Termo de Aceite Definitivo, após o treinamento ser ministrado e após comprovação de aprovação na avaliação do treinamento.	Não se aplica	Não se aplica	Até 10 (dez) dias úteis contados da finalização da liquidação da despesa
4	Treinamento para solução de controle de acesso de usuários privilegiados. (Item 17 - Grupo 2)	Pagamento em parcela única, mediante Termo de Aceite Definitivo, após o treinamento ser ministrado e após comprovação de aprovação na avaliação do treinamento.	Não se aplica	Não se aplica	Até 10 (dez) dias úteis contados da finalização da liquidação da despesa

8.3.2. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022; 7.11.3.2.

8.3.3. No caso de atraso pelo CONTRATANTE, os valores devidos a CONTRATADA serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice de Custo de Tecnologia da Informação (ICTI), do Instituto de Pesquisa Econômica Aplicada (IPEA) de correção monetária.

8.4. FORMA DE PAGAMENTO

8.4.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

8.4.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

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

8.4.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.4.5. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei

Complementar.

9. PLANO DE SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL

9.1. INTRODUÇÃO

A etapa de elaboração da Sustentação do Contrato compreende:

a. Definição de recursos materiais e humanos;
b. Elaboração de estratégia de continuidade;
c. Definição de atividades de transição e encerramento contratual;
d. Elaboração de Estratégia de Independência;
e. Devolução ao contratante dos dados pessoais confiados ao contratado e a eliminação das cópias, quando aplicável;

9.2. RECURSOS NECESSÁRIOS À CONTINUIDADE DO NEGÓCIO DURANTE E APÓS A EXECUÇÃO DO CONTRATO

9.2.1. RECURSOS MATERIAIS E HUMANOS

A sustentação da CTI não requer a disponibilização, por parte do órgão, de materiais e/ou recursos humanos além dos já existentes no MPPI.

9.3. ESTRATÉGIA DE TRANSIÇÃO CONTRATUAL

9.3.1. Na transição contratual a CONTRATADA deve, em conformidade com o parágrafo 1º do artigo 93 da Lei nº 14.133/2021, repassar para o CONTRATANTE todos os dados, documentos e elementos de informação utilizados na execução dos serviços;

9.3.2. Ao término da vigência do contrato o CONTRATANTE irá revogar os perfis de acesso concedidos à CONTRATADA para fins de atualização remota de versões.

9.4. EXTINÇÃO CONTRATUAL

9.4.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes;

9.4.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o CONTRATANTE, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem;

9.4.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo CONTRATANTE nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia;

9.4.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação;

9.4.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o
contraditório e a ampla defesa;

9.4.6. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei;

9.4.7. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato;

9.4.8. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva;

9.4.9. O termo de extinção, sempre que possível, será precedido:

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

b) Relação dos pagamentos já efetuados e ainda devidos;

c) Indenizações e multas;

9.4.10. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei n.º 14.133, de 2021).

9.5. ESTRATÉGIA DE INDEPENDÊNCIA

9.5.1. DEFINIÇÃO

Durante a execução das atividades de monitoração do ambiente, a CONTRATADA deverá proporcionar a transferência de conhecimento para a equipe do CONTRATANTE em relação às soluções adotadas, a fim de minimizar o risco na reincidência de problemas, permitindo que a equipe do CONTRATANTE esteja ciente do histórico de ocorrências.

9.5.2. TRANSFERÊNCIA DE CONHECIMENTO

A CONTRATADA deverá transmitir o conhecimento acerca dos serviços desenvolvidos aos técnicos do CONTRATANTE. Os meios utilizados para essa transferência serão previamente acordados entre CONTRATADA e CONTRATANTE, podendo consistir em um ou uma combinação dos seguintes meios:

- Divulgação eletrônica.
- Base de conhecimentos.
- Registro de lições aprendidas.
- Registro de soluções alternativas utilizadas.
- Registro de ocorrências, conhecimentos e procedimentos.
- Documentação de melhores práticas.
- Reuniões e suas respectivas atas
- Relatórios periódicos.
- Ferramentas de comunicação em geral: videoconferência, chat, e-mail

9.5.3. DIREITOS DE PROPRIEDADE INTELECTUAL

9.5.3.1. A CONTRATADA deverá entregar ao CONTRATANTE toda e qualquer documentação gerada como resultado da prestação de serviços, objeto da contratação. Entende-se por documentação quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e documentação didática em papel ou em mídia eletrônica.

9.5.3.2. A CONTRATADA fica proibida de comercializar a documentação supracitada que seja produzida no escopo específico da realização deste objeto, ficando sujeita às penalidades previstas na Lei 9609/98 em caso de descumprimento desta determinação.

9.5.3.3. A utilização de soluções ou componentes proprietários da CONTRATADA ou de terceiros, na execução dos serviços relacionados ao presente contrato, que possam afetar a propriedade do produto, deve ser formal e previamente autorizada pelo MPPI.

10. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

10.1. A contratação tem o custo total estimado em **R$ 29.806.104,76** (Vinte e nove milhões, oitocentos e seis mil, cento e quatro reais e setenta e seis centavos) , conforme detalhamento abaixo:

GRUPO 1 - ITENS 1 A 6				
Item	**Descrição**	**Quantidade**	**Valor Unitário (R$)**	**Valor Total (R$)**
1	Licença para visibilidade, análise de dados locais, comportamento e prevenção de ameaças por 36 meses	1600	R$ 5.540,39	R$ 8.864.624,00
2	Licença para visibilidade, análise de dados em nuvem, comportamento e prevenção de ameaças por 36 meses	1600	R$ 5.540,39	R$ 8.864.624,00
3	Licença para visibilidade, análise de dados em caixas postais, comportamento e prevenção de ameaças por 36 meses	1600	R$ 1.918,57	R$ 3.069.712,00
4	Serviço de instalação e configuração para solução	2	R$ 30.637,16	R$ 61.274,32

5	Manutenção e Suporte Técnico	2	R$ 916.925,26	R$ 1.833.850,52
6	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.	2	R$ 65.651,05	R$ 131.302,10
GRUPO 2 - ITENS 7 A 17				
7	Cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses	2	R$ 337.202,96	R$ 674.405,92
8	Balanceador de carga para cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses	2	R$ 337.202,96	R$ 674.405,92
9	Usuários para acesso privilegiado por 36 meses	40	R$ 7.444,70	R$ 297.788,00
10	Licença para servidores físicos e virtuais por 36 meses	400	R$ 372,13	R$ 148.852,00
11	Licença para equipamentos de conectividade de Rede, VOIP e Segurança- LAN, AP E WAN por 36 meses	1000	R$ 138,80	R$ 138.800,00
12	Licença para aplicações não conteinerizadas com senha embutida (hard coded) por 36 meses	80	R$ 4.763,43	R$ 381.074,40
13	Licença para acesso remoto seguro por 36 meses	60	R$ 12.635,08	R$ 758.104,80
14	Licença de gerenciamento de certificados digitais por 36 meses	2	R$ 14.101,20	R$ 28.202,40
15	Serviço de instalação e configuração para solução	2	R$ 52.520,84	R$ 105.041,68
16	Manutenção e Suporte Técnico	2	R$ 1.830.107,23	R$ 3.660.214,46
17	Treinamento para solução de controle de acesso de usuários privilegiados.	2	R$ 56.914,12	R$ 113.828,24

10.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre Contratante e Contratado, conforme especificado na matriz de risco constante do Contrato.

10.3. Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:
a) em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos im-previsíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal co-mo pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;
b) em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;
c) serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou
d) poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

11. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

11.1. A despesa decorrente da execução do objeto correrá à conta do orçamento do Ministério Público do Estado do Piauí, na dotação abaixo discriminada:

- Unidade Orçamentária: 25102 - Fundo de Modernização do Ministério Público do Estado do Piauí

- Fonte: 759

- Programa: 0111

- Projeto/Atividade: 6113

- Função: 03

- Natureza da Despesa: 339040

12. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

12.1. JUSTIFICATIVA PELA ADOÇÃO DO SISTEMA DE REGISTRO DE PREÇOS (Decreto Estadual nº 21.938/2023, Art. 4)

12.1.1. O artigo 4º do Decreto Estadual nº 21.938/2023 define as situações em que o Sistema de Registro de Preços (SRP) pode ser preferencialmente adotado, conforme segue:

Art. 4º O SRP será adotado preferencialmente nas seguintes hipóteses:

I. Quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes;

II. Quando for mais conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, por quantidade de horas de serviço ou em regime de tarefa;

III. Quando for conveniente para atendimento a mais de um órgão ou entidade;

IV. Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela administração.

12.1.2. É fundamental destacar que o Sistema de Registro de Preços tem como objetivo promover a economicidade. No caso em questão, optou-se por esse sistema em razão da necessidade de realizar a compra de forma parcelada, uma vez que não há demanda imediata para a entrega de todo o quantitativo previsto neste documento.

12.1.3. Essa abordagem evita a realização de novos pregões para a aquisição do mesmo material, resultando em economia para a Administração. A quantidade de materiais ou serviços a serem entregues será conforme a necessidade do setor requisitante.

12.1.4. Portanto, a adoção do Sistema de Registro de Preços é a opção mais adequada para este caso.

12.2. FORMA DE SELEÇÃO E CRITÉRIO DE JULGAMENTO DA PROPOSTA

12.2.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA;

12.2.2. A licitação será dividida em ITENS, dispostos em lotes, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos lotes forem de seu interesse.

12.2.3. O critério de julgamento adotado será o menor preço do LOTE, considerado o menor dispêndio para a Administração, nos termos do art. 34 da Lei nº 14.133/2021, e observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

12.2.4. O regime de execução do contrato será por EXECUÇÃO INDIRETA do tipo EMPREITADA POR PREÇO GLOBAL.

12.3. APRESENTAÇÃO DAS PROPOSTAS

12.3.1. A proposta de preços deverá ser apresentada contendo todos os elementos que influenciam no valor final da contratação, devendo conter:

12.3.2. Descrição clara e completa do objeto, contendo as especificações detalhadas, observada a descrição/especificação constante no item 2.2. ESPECIFICAÇÃO TÉCNICA DO OBJETO, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a ter mais de um resultado.

12.3.3. A proposta deverá conter as especificações do objeto de forma clara, descrevendo detalhadamente as características técnicas dos equipamentos e softwares ofertados, incluindo especificação de marca, modelo, part numbers, procedência e outros elementos que de forma inequívoca identifiquem e constatem as configurações cotadas, comprovando-os por meio de certificados, manuais técnicos, folders datasheets e demais literaturas editadas pelo fabricante.

12.3.4. Deverá comprovar em proposta, obrigatoriamente, todos os itens e subitens desta especificação, apontado a página do documento onde consta a comprovação do item/subitem proposto. A simples repetição das especificações do termo de referência sem a devida comprovação acarretará a desclassificação da proponente.

12.3.5. O prazo de validade das propostas será de 90 (noventa) dias, contados da data de abertura da

sessão pública estabelecida no preâmbulo do edital.

12.3.6. A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item;

12.3.7. Todos os itens especificados da solução deverão ser adquiridos em caráter permanente, podendo ser utilizados por tempo indeterminado, mesmo com o término do contrato;

12.4. EXIGÊNCIAS DE HABILITAÇÃO

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

12.4.1.1. HABILITAÇÃO JURÍDICA

12.4.1.1.1. 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;

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

12.4.1.1.3. 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;

12.4.1.1.4. 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;

12.4.1.1.5. 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.

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

12.4.1.1.7. 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

12.4.1.1.8. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o Art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

12.4.1.2. HABILITAÇÃO FISCAL, SOCIAL E TRABALHISTA

12.4.1.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

12.4.1.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

12.4.1.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

12.4.1.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

12.4.1.2.5. Prova de inscrição no cadastro de contribuintes Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

12.4.1.2.6. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

12.4.1.3. QUALIFICAÇÃO TÉCNICA

12.4.1.3.1. Comprovação de aptidão para o fornecimento de bens ou serviços similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item

pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

12.4.1.3.2.Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

12.4.1.3.3.O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto Contratado, dentre outros documentos.

12.4.1.3.4.Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

I) A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei nº. 5.764, de 1971;

II) A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

III) A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

IV) O registro previsto na Lei nº. 5.764, de 1971, art. 107;

V) A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

VI) Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

a) ata de fundação;

b) estatuto social com a ata da assembleia que o aprovou;

c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;

d) editais de convocação das três últimas assembleias gerais extraordinárias;

e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e

f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

VII) A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei nº. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

12.4.1.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

12.4.1.4.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da IN SEGES/ME nº 116, de 2021), ou de sociedade simples.

12.4.1.4.1.Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II).

12.4.1.4.1.Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

a) índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

b) As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e

c) Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

d) Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

12.4.1.4.1. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo de até 10% do valor total estimado da contratação.

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

12.4.1.4.1. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

13. CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) - LEI 13.709/2018

13.1. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal;

13.2. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual;

13.3. As partes responderão administrativa e judicialmente caso causarem danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados;

13.4. Em atendimento ao disposto na Lei Geral de Proteção de Dados, o CONTRATANTE, para a execução do serviço objeto desta contratação, tem acesso a dados pessoais dos representantes da CONTRATADA, tais como número do CPF e do RG, endereços eletrônico e residencial, e cópia do documento de identificação;

13.5. A CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo CONTRATANTE;

13.6. A CONTRATADA fica obrigada a comunicar ao CONTRATANTE em até 24 (vinte e quatro) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no Art. 48 da Lei Geral de Proteção de Dados;

13.7. A CONTRATADA, quando do encerramento da contratação, exceto se abrigados pelo disposto nos incisos do artigo 16 da LGPD, fica obrigada a eliminar todo os dados pessoais obtidos em razão da execução do contrato. O CONTRATANTE deverá ser formal e justificadamente comunicado da eventual impossibilidade da eliminação de dados pessoais que não se enquadrem na hipótese legal acima mencionada.

14. DEVERES E RESPONSABILIDADES DO ÓRGÃO GERENCIADOR DA ATA DE REGISTRO DE PREÇOS

14.1. Constituem obrigações do ÓRGÃO GERENCIADOR DA ARP, além de outras estabelecidas ou decorrentes deste TR:

14.1.1. Cumprir o estabelecido nos artigos. 82 a 86 da Lei nº 14.133/2021;

14.1.2. Prover o registro do licitante fornecedor e a assinatura da correspondente Ata de Registro de Preço;

14.1.3. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

14.1.4. Conduzir a aplicação das penalidades por descumprimento do pactuado na Ata de Registro de Preços;

14.1.5. Realizar a autorização ou não do fornecimento da Solução de TI para órgão não participante da Ata de Registro de Preços, desde que prevista no instrumento convocatório, consultado o beneficiário da Ata e verificadas as condições de fornecimento, de forma a evitar extrapolações dos limites de produtividade ou de capacidade mínima de fornecimento da Solução;

14.1.6. Definir os mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

a) as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível;

b) a definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável, a exemplo de ordem de serviço ou fornecimento de bens, aplicações de sanções administrativas, alteração de item registrado em Ata por modelo equivalente ou superior.

14.1.7. Definir os mecanismos de controle de fornecimento da Solução de TI, observando, entre outros:

a) a definição da produtividade ou da capacidade mínima de fornecimento da Solução de TI;

b) as regras para fornecimento da Solução de TI aos órgãos não participantes, desde que previsto no instrumento convocatório, cujo fornecimento não poderá prejudicar os compromissos já assumidos e as futuras contratações dos órgãos participantes do Registro de Preços;

c) as regras para gerenciamento da fila de fornecimento da Solução de TI aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela CONTRATADA;

d) as regras para a substituição da solução registrada por meio de apostilamento, garantida a realização de Prova de Conceito, observado o disposto na alínea “b” do inciso V do artigo 23 da Resolução 283/2024 do CNMP e desde que previsto o apostilamento, em função de atualizações tecnológicas existentes no seguimento de informática, na Ata de Registro de Preços; e

e) a previsão da exigência para realização de Prova de Conceito com o licitante provisoriamente classificado em primeiro lugar para fins de comprovação de atendimento das especificações técnicas.

14.1.8. Permitir a adesão à Ata de Registro de Preços por outros ramos ou unidades do Ministério Público.

14.2. Justificativa para a permissão de adesão de órgãos ou entidades não participantes (IN SGD 94/2022, Art. 15, inciso V)

14.2.1. A possibilidade de órgãos ou entidades que não participaram do procedimento licitatório aderirem à ata e adquirirem os bens e serviços licitados por outro órgão está respaldada no Art. 31 do Decreto Federal nº 11.462, de março de 2023, e no Art. 32 do Decreto Estadual nº 21.938, de 28 de março de 2023. A prática conhecida como "carona" é uma medida que promove a eficiência e a economia processual.

14.2.2. A adesão pressupõe a realização de uma licitação que observou os princípios da publicidade, isonomia e seleção da proposta mais vantajosa para a administração pública, garantindo a integridade e transparência do processo.

14.2.3. A utilização da ata de registro de preços por meio da adesão permite a redução de custos com novas licitações e promove a desburocratização dos processos administrativos. Esses fatores justificam a previsão dessa prática no presente processo licitatório.

14.2.4. Será vedada aos órgãos e entidades da Administração Pública federal a adesão à ata de registro de preços gerenciada por órgão ou entidade estadual, distrital ou municipal, conforme disposições do art. 86, §8º, da Lei nº 14.133/2021.

15. DOS ÓRGÃOS PARTICIPANTES

15.1. Itens da Intenção de Registro de Preços (IRP), conforme documento 0824576:

Nº do Item	Tipo do Item	Item	Unidade de Fornecimento	Critério de Julgamento	Valor Unitário (R$)	UASG - Município/UF de Entrega/Quantidade		
1	Serviço	Licença para visibilidade, análise de dados locais, comportamento e prevenção de ameaças por 36 meses - CATSER: 24333	Licença	Menor preço	5.540,39	453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	2
						456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	3000
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	4000
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1000
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	1600
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	2800

						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	800
2	Serviço	Licença para visibilidade, análise de dados em nuvem, comportamento e prevenção de ameaças por 36 meses - CATSER: 24333	Licença	Menor preço	5.540,39	453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	2
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	3000
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1000
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	1600
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	800
3	Serviço	Licença para visibilidade, análise de dados em caixas postais, comportamento e prevenção de ameaças por 36 meses - CATSER: 24333	Licença	Menor preço	1.918,57	453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	2000
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	3000
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1000
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	1600
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	800
4	Serviço	Serviço de instalação e configuração para solução - CATSER: 26972	Unidade	Menor preço	30.637,16	453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	1
						456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2

						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	10
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1
5	Serviço	Manutenção e Suporte Técnico - CATSER: 26972	Unidade	Menor preço	916.925,26	453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	1
						456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	5
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1
6	Serviço	Treinamento para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint. - CATSER: 3840	Turma	Menor preço	65.651,05	453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	1
						456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	5
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1

7	Serviço	Cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses - CATSER: 469726	Unidade	Menor preço	337.202,96	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	4
						926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	1
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1
8	Serviço	Balanceador de carga para cluster para prover recursos para solução de acesso a usuários privilegiados por 36 meses- CATSER: 469726	Unidade	Menor preço	337.202,96	453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	1
						456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	4
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1
9	Serviço	Subscrição para usuários com acesso	Unidade	Menor	7.444,70	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	40
						926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	30
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	100

		privilegiado por 36 meses - CATSER: 24333		preço		926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	40
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	200
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	30
10	Serviço	Subscrição para servidores físicos e virtuais por 36 meses - CATSER: 24333	Unidade	Menor preço	372,13	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	80
						926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	250
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	400
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	400
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	1500
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	200
11	Serviço	Subscrição para equipamentos de conectividade de Rede, VOIP e Segurança-LAN, AP E WAN por 36 meses - CATSER: 24333	Unidade	Menor preço	138,80	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	400
						926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	150
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1500
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	1000
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	1000
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	50
						456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	20

12	Serviço	Subscrição para aplicações não conteinerizadas com senha embutida (hard coded) por 36 meses - CATSER: 24333	Unidade	Menor preço	4.763,43	925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	150
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	80
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	200
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	50
13	Serviço	Subscrição para acesso remoto seguro por 36 meses - CATSER: 24333	Unidade	Menor preço	12.635,08	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	20
						926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	5
						453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	20
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	200
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	60
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	50
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	10
14	Serviço	Subscrição de gerenciamento de certificados digitais por 36 meses - CATSER: 24333	Unidade	Menor preço	14.101,20	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	2
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	10
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	1
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	80

						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	100
15	Serviço	Serviço de instalação e configuração para solução - CATSER: 26972	Unidade	Menor preço	52.520,84	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1
						926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	8
						925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	São Luis/MA	1
						453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Vitória/ES	1
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1
16	Serviço	Manutenção e Suporte Técnico - CATSER: 26972	Unidade	Menor preço	1.830.107,23	456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1
						926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	2
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1
						456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Porto Velho/RO	1

17	Serviço	Treinamento para solução de controle de acesso de usuários privilegiados. - CATSER: 3840	Turma	Menor preço	56.914,12	926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	Salvador/BA	1
						925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Belém/PA	1
						926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Teresina/PI	2
						926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Maceió/AL	5
						930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	Aracaju/SE	1

15.2. Endereço de entrega dos equipamento e prestação dos serviços:

UASG	Endereço
926092 - PROCURADORIA GERAL DE JUSTIÇA DO PIAUI	Rua Álvaro Mendes, 2294 - Centro Teresina-PI - CEP 64000-060.
453687 - SECRETARIA DE ESTADO DA JUSTIÇA DO ES	Avenida Governador Bley, 236 - Centro CEP: 29010-150 - Vitória / ES Tel.: (27) 3636-5700
456854 - AGÊNCIA DE DEF. SAN. AGROSILVOPASTORIL DE RO	Endereço: Av. Farquar, 2986 - Bairro Pedrinhas - Palácio Rio Madeira (CPA), 5º andar, edifício Rio Cautário CEP: 76801-470 - Porto Velho - Rondônia
925129 - PROCURADORIA GERAL DE JUSTIÇA DO MARANHÃO	Av. Prof. Carlos Cunha, nº 3261, Calhau CEP: 65076-820 - São Luis - Maranhão (98) 3219-1600
925980 - MINISTÉRIO PÚBLICO DO ESTADO DO PARÁ	Rua Joao Diogo, 100 - Cidade Velha - Belém-PA | CEP 66015-165 | (91) 3198-2400 (Promotorias) e (91) 4006-3400 (Edifício Sede)
926217 - INST. DE TEC. EM INF. E INFORMAÇ. DE ALAGOAS	Instituto de Tecnologia em Informática e Informação do Estado de Alagoas Rua Dr. Cincinato Pinto, nº 463, Centro, Maceió, Alagoas - CEP 57020-050
930780 - SECRETARIA DE ESTADO DA FAZENDA/SE	R. José Carvalho Pinto, 280, 3º andar, Jardins, Acaraju, Sergipe - CEP 49026-150
926302 - PROCURADORIA GERAL DE JUSTICA DA BAHIA	5ª Avenida, n° 750, CAB, Salvador, Bahia - CEP 41.745-004

16. DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

17. DO FORO

17.1. Para dirimir as questões oriundas deste instrumento, será competente o foro da Comarca de Teresina-PI.

18. APROVAÇÃO PELA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Equipe de Planejamento da Contratação		
Integrante Técnico	**Integrante Requisitante**	**Integrante Administrativo**
_____ Marcos Maciel Martins Brito Matrícula: 425	_____ Ítalo Garcia Nogueira Araújo Matrícula: 15807	_____ Thiago Nogueira de Sousa Martins Almeida Matrícula: 204
Teresina (PI), datado digitalmente.		

19. APROVAÇÃO DA AUTORIDADE SUPERIOR

19.1. Aprovo o Termo de Referência e determino à Coordenadoria de Licitações e Contratos a realização dos atos necessários à aquisição/contratação do objeto.

Ordenador de despesas do Ministério Público do Estado do Piauí
ASSINADO DIGITALMENTE
Dr. Hugo de Sousa Cardoso Procurador de Justiça Subprocurador-Geral de Justiça Institucional

ANEXO I

Termo de Compromisso e Manutenção de Sigilo

A _____, CNPJ _____, por intermédio de seu representante legal abaixo assinado, _____,CPF_____, doravante designados simplesmente CONTRATADA e RESPONSÁVEL, se comprometem, por intermédio do presente TERMO DE COMPROMISSO, a não divulgar sem autorização, quaisquer Informações Confidenciais (conforme definido abaixo) em relação ao Projeto de “Contratação de Empresa para fornecimento de Solução de Backup para a Procuradoria Geral de Justiça do Estado do Piauí”, CNPJ 05.805.924/0001-89, doravante designada MPPI, em conformidade com as seguintes cláusulas e condições:

1. Por este instrumento, a Contratada declara estar apta a aceitar e receber INFORMAÇÕES com respeito ao parque tecnológico do MPPI, se comprometendo a manter absoluta confidencialidade destas INFORMAÇÕES, independente de solicitação expressa neste sentido pelo MPPI ou quaisquer de seus representantes;
2. As INFORMAÇÕES abrangidas por este termo são de natureza técnica, operacional, comercial, jurídica e financeira expressas de forma escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, ficando expressamente vedada sua divulgação a terceiros, a qualquer título;
3. As partes deverão restringir a divulgação das INFORMAÇÕES para o pessoal que estiverem diretamente envolvidos na sua utilização em razão do fornecimento das INFORMAÇÕES e da elaboração do serviço a ser fornecido, ficando vedado o intercâmbio destas INFORMAÇÕES com terceiros que não estejam diretamente envolvidos com a prestação dos serviços;
4. A CONTRATADA obriga-se a informar imediatamente o MPPI qualquer violação das regras de sigilo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de

seus empregados, prepostos e prestadores de serviço;
5. A CONTRATADA deverá prestar obediência às políticas de segurança da informação vigentes no MPPI ou que poderão ser instituídas durante a vigência do contrato;
6. A não observância de qualquer das disposições estabelecidas neste instrumento sujeitará a CONTRATADA aos procedimentos judiciais cabíveis relativos a perdas e danos que possam advir ao MPPI e aos seus usuários;
7. O descumprimento de quaisquer das cláusulas do presente Termo acarretará a responsabilidade civil e criminal de acordo com as leis aplicáveis dos que, comprovadamente, estiverem envolvidos no descumprimento ou violação.

Gestor do Contrato da MPPI: _____

Representante da Contratada: _____

Teresina, PI, _____ de _____ de _____.

ANEXO II

Termo de Ciência

IDENTIFICAÇÃO DO CONTRATO

Contrato Nº: XXXXXX
Objeto: “Contratação de Empresa para fornecimento de Solução de Backup para a Procuradoria Geral de Justiça do Piauí”

Contratada:
CNPJ:
Representante da Contratada: CPF:

Pelo presente instrumento, o(s) funcionário(s) abaixo qualificado(s) e assinado(s) declara(m) ciência do Termo de Compromisso e Manutenção de Sigilo referente ao objeto contratado e as normas de segurança vigentes da Contratante.

Nome:
CPF:
Função/Cargo:

_____

Assinatura

Nome:
CPF:
Função/Cargo:

_____

Assinatura

Teresina, PI, _____ de _____ de _____.

Documento assinado eletronicamente por **Marcos Maciel Martins Brito**, **Chefe de Divisão**, em 28/01/2025, às 12:58, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **BRENO REIS DO NASCIMENTO**, **Técnico(a) Ministerial**, em 28/01/2025, às 13:03, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ITALO GARCIA ARAUJO NOGUEIRA**, **Coordenador(a) de Tecnologia da Informação**, em 28/01/2025, às 14:37, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.mppi.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0938941** e o código CRC **CAF42016**.