PROC. ADM. Nº. 936410/2023 **PREGÃO ELETRÔNICO Nº. 62/2023**

ATA DE REGISTRO DE PREÇOS n.º 48/2024

Pelo presente INSTRUMENTO, o Município de Várzea Grande pessoa jurídica de direito público, inscrita no CNPJ-MF nº. 03. 507.548/0001-10, situado na Av. Castelo Branco nº. 2500, bairro Água Limpa, Várzea Grande/MT, por intermédio das **Secretaria Municipal de Administração**, neste ato sendo representada pelo Secretário **Osvaldo Botelho de Campos Neto,** inscrito no CPF n. 655.387.221-04, denominada **CONTRATANTE**, e de outro lado à empresa **DEK SOLUCOES EM T.I. LTDA**, pessoa jurídica de direito privado, inscrita no CNPJ **21.191.387/0001-80** situada na Rua PEQUITITA, 179, CONJ 116 EDIF NEW CENTER OFFICES, Bairro VILA OLIMPIA, CEP: 04.552-060, Cidade/UF, SÃO PAULO-SP, Telefone (65) 3645-3535, endereço eletrônico: hermann@servdigital.com.br, sendo representada neste ato pelo Senhor HERMANN DRUMMOND JUNIOR, inscrito no CPF 820.636.051-49, denominada **CONTRATADA**, vencedora do **LOTE UNICO** com o total de **R$ 5.140.000,00** (cinco milhões, cento e quarenta mil), considerando o julgamento de **MENOR PREÇO POR LOTE**, na modalidade PREGÃO ELETRÔNICO Nº. 62/2023, após a classificação da sua proposta e respectiva homologação, **REGISTRA-SE** o preço da empresa de acordo com a classificação por ela alcançada, atendendo as condições previstas no Instrumento Convocatório e as constantes desta Ata de Registro de Preços, sujeitando-se as partes às normas constantes pela Lei Federal. 10.520/2002, Decreto Federal nº. 10.024/2019, Lei Complementar nº. 123/2006 e suas alterações, Lei Municipal nº. 3.515/2010, Decretos Municipais nº. 09/2010 e nº. 54/2019 e suas alterações, aplicando-se, subsidiariamente, no que couberem, as disposições da Lei Federal. 8.666/1993 e demais legislações complementares, e condições estabelecidas no Edital, e seus anexos, bem como em conformidade com as disposições a seguir.

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. **Registro de preço para eventual contratação de solução de segurança da informação para proteção inteligente de dados em repouso, estruturados e não estruturados, controle de acesso, visibilidade e rastreabilidade de utilização de dados em servidores de arquivos, banco de dados, custódia de chaves criptográficas composta por softwares e serviços de garantia e suporte técnico, serviços de instalação e configuração da solução, serviços de treinamento,**

serviços para integrações necessárias com soluções de terceiros e serviços especializados para atender às demandas da Prefeitura Municipal de Várzea.

Parágrafo Único - A execução do objeto aqui tratado obedecerá, fiel e integralmente, ao PREGÃO ELETRÔNICO Nº. 62/2023, e a proposta da CONTRATADA, nesta ordem, ambos constantes no processo administrativo nº. **936410/2023** que passa a fazer parte integrante deste instrumento.

CLÁUSULA SEGUNDA – DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1. Fica registrado conforme planilha abaixo, o preço, as especificações, os quantitativos, para a empresa detentora desta ata, e demonstrada também no relatório de vencedores do sistema no processo licitatório:

ITEM	CÓD TCE	DESCRIÇÃO DO PRODUTO	UND	QUANT	VALOR UNITÁRIO	VALOR TOTAL
01	422472-8	APPLIANCE DE GERENCIAMENTO DE SOLUÇÃO DE SEGURANÇA DE DADOS COM SERVIÇO DE SUPORTE	UND	01	R$ 976.956,50	R$ 976.956,50
02	00055997	MÓDULO DE SEGURANÇA DE DADOS NÃO ESTRUTURADOS MULTIPLATAFORMA COM SERVIÇO DE SUPORTE	UND	01	R$ 141.352,30	R$ 141.352,30
03	00055997	MÓDULO DE SEGURANÇA DE DADOS ESTRUTURADOS MULTIPLATAFORMA COM SERVIÇO DE SUPORTE	UND	02	R$ 143.927,00	R$ 143.927,00
04	00055997	MÓDULO PARA TRANSFERÊNCIA SEGURA DE BASE DE DADOS COM SERVIÇO DE SUPORTE	UND	01	R$ 727.841,30	R$ 727.841,30

05	00069841	MÓDULO DE SEGURANÇA PARA APLICAÇÕES WEB COM SERVIÇO DE SUPORTE	UND	01	R$ 196.317,30	R$ 196.317,30
06	00069841	MÓDULO DE GESTÃO DE CHAVES LOCAL COM SERVIÇO DE SUPORTE	UND	01	R$ 12.554,80	R$ 12.554,80
07	00069841	MÓDULO DE VALIDAÇÃO DE CONTROLE DE SEGURANÇA CONTRA AMEAÇAS DE REDE, ENDPOINT, APLICAÇÃO WEB, E-MAIL E VAZAMENTO DE DADOS COM SERVIÇO DE SUPORTE	UND	01	R$ 626.823,70	R$ 626.823,70
08	439506-9	SERVIÇO DE TREINAMENTO	UND	02	R$ 28.604,40	R$ 28.604,40
09	231423-1	SERVIÇO DE IMPLEMENTAÇÃO DE CONSOLE DE GERENCIAMENTO DE CHAVES DE CRIPTOGRAFIA.	UND	01	R$ 24.112,50	R$ 24.112,50
10	231423-1	SERVIÇO SOB DEMANDA PARA IMPLEMENTAÇÃO DE AGENTES DE CRIPTOGRAFIA.	UND	3000	R$ 360,80	R$ 360,80
11	375385-9	SERVIÇO DE CONSULTORIA PARA AVALIAÇÃO PERIÓDICA (HEALTHCHECK)	UND	02	R$ 113.466,70	R$ 113.466,70
12	324820-8	SERVIÇO DE ANÁLISE DE RISCO - 12 MESES	UND	12	R$ 25.544,60	R$ 25.544,60
13	375385-9	SERVIÇO DE DIAGNÓSTICO, AVALIAÇÃO, MAPEAMENTO E LEVANTAMENTO DO PARQUE TECNOLÓGICO	UND	06	R$ 10.920,50	R$ 10.920,50

14	354661-6	SERVIÇO DE GESTÃO DE PROJETOS E DOCUMENTAÇÃO - 12 MESES	UND	12	R$ 25.782,30	R$ 25.782,30
15	278817-9	SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO (HELPDESK) – 12 MESES	UND	06	R$ 16.366,60	R$ 16.366,60
Valor Total do Lote : R$ 5.140.000,00 (cinco milhões, cento e quarenta mil)						

2.2. ESPECIFICAÇÕES TÉCNICAS

2.2.1. ITEM 1 - APPLIANCE DE GERENCIAMENTO DE SOLUÇÃO DE SEGURANÇA DE DADOS

a) Appliance virtual com certificação FIPS 140-2 Nível 1, ou certificação compatível;

b) Deve ser compatível com ACROPOLIS HYPERVISOR (AHV). Não serão aceitas soluções baseadas em hardware;

c) O appliance deve oferecer recursos para proteger e controlar o acesso a dados estruturados e não estruturados hospedados em ambientes físicos e virtuais, ON PREMISES e em NUVEM.

d) Deve permitir o gerenciamento centralizado de todos os módulos de segurança de dados, suas chaves de criptografia, políticas de configuração, publicação e controle de acesso dos dados a serem protegidos.

e) Deve suportar a aplicação de módulos de segurança para as funcionalidades que seguem:

e.1.) Criptografia transparente – para criptografar, controlar o acesso ao dado e oferecer registros de auditoria de acesso aos dados sem impactar nas aplicações, base de dados ou infraestrutura onde quer que os servidores estejam instalados;

e.2.) Integração com SIEM–suportar integração com os sistemas de gerenciamento de logs do mercado, como: SPLUNK, QRADAR, ARCSIGHT, MCAFEE, LOGRHYTHM e etc;

e.3.) Segurança de Micro serviços - oferecer criptografia de dados, controle de acesso e registro de acesso ao dado;

e.4.) Gerenciamento de chaves em nuvem múltipla – permitir custódia e controle de dados em ambiente de software como serviço (SaaS), relatório de acesso e eficiência no gerenciamento do ciclo de vida da chave em nuvem com o conceito Traga sua Própria Chave (BYOK);

e.5.) Toquenização e mascaramento estático e dinâmico de dados de produção e não produção – reduzir os custos e o esforço necessários para cumprir com as políticas de segurança e normas regulatórias como o LGPD, dentre outras;

e.6.) Criptografia para aplicações – simplificar o processo de adição de criptografia em aplicações, por meio de API´s baseadas em padrões que potencializam operações criptográficas e de gerenciamento de chaves de alto desempenho.

e.7.) Descoberta e Classificação de dados para identificar e classificar dados de permitindo a aplicação de mecanismos adequados a sua proteção, acelerando a conformidade;

e.8.) Gerenciamento e armazenamento de chaves de criptografia nativa e certificados digitais;

e.9.) Detecção avançada e prevenção contra RANSOMWARE – Simplificar a prevenção dos ataques RANSOMWARE identificando, alertando e bloqueando RANSOMWARE utilizando modelos de aprendizado de máquina para detectar atividades suspeitas baseadas em atividade de I/O;

a) O appliance deve ser capaz de ser configurado em alta disponibilidade (HA) com um servidor primário e outro (s) secundário (s). A configuração de alta disponibilidade deve permitir a hospedagem dos servidores primário e secundário em datacenters distintos e conectados.

a.1.) Apoiar a incorporação de APPLIANCES adicionais para fins de configuração de esquemas de tolerância a falhas multinível.

a.2.) Os módulos de segurança devem operar de forma autônoma não causando impacto em caso de perda de comunicação com o appliance.

a.3.) Detalhes da chave de criptografia não devem ser divulgados para usuários do sistema para que o algoritmo de criptografia esteja protegido dos usuários da plataforma. Estes devem ser armazenados de forma segura no appliance.

a.4.) O appliance deve possuir capacidade de gerenciar chaves criptográficas padrão KMIP.

a.5.) Deve ser compatível com API PKCS # 11 e Microsoft Key Extensible Management.

a.6.) Deve ser capaz de oferecer suporte a certificados digitais (X. 509) PKCS # 7, PKCS # 8 e PKCS # 12, chaves de criptografia simétrica (algoritmos3DES, AES128, AES256) e assimétrica (algoritmos RSA2048, RSA4096).

a.7.) Deve ser escalável para oferecer suporte a gerenciamento de agente de vários serviços em uma estrutura de Multitenant e com suporte a configuração de segurança de vários domínios. Para isso, deve possibilitar configurar diferentes chaves criptográficas de acordo com cada área de operação, se necessário.

a.8.) Quando aplicada a separação de funções, o console deve permitir que o usuário do sistema crie chaves de criptografia, outro usuário pode aplicá-las e outro, que não seja o anterior, consiga monitorar o mesmo durante a aplicação.

a.9.) O appliance deve possibilitar gerenciamento via interface Web, possibilitar comandos (CLI) e API.

a.10.) A interface Web deve disponibilizar acesso a todos os módulos de segurança, implementados.

a.11.) Deve requerer autenticação de usuário e senha.

a.12.) Deve ser capaz de configurar cópias de backup de suas configurações automaticamente ou manualmente.

a.13.) Requerimentos complementares:

a.13.1.) Suportar usuários múltiplos;

a.13.2.) Toolkit e interface de programação;

a.13.3.) Integração infraestrutura de autenticação existente, com fácil configuração;

a.14.) Suporte para APIREST full;

a.15.) Autenticação multifator;

2.2.2. ITEM 2 - MÓDULO DE SEGURANÇA DE DADOS NÃO ESTRUTURADOS MULTIPLATAFORMA.

a) Este módulo deve fornecer criptografia para servidores de arquivos (dados não estruturados) para dados em repouso com gerenciamento centralizado de chaves, controle de acesso de usuários, incluindo usuários privilegiados, e registro detalhado de auditoria de acesso visando atender aos requisitos de conformidade e práticas recomendadas para proteger os dados, onde quer que estejam. Este módulo deverá residir no sistema operacional, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela.

b) O processo de criptografia deve ser executado por agentes que deverão ser instalados nos servidores de arquivos.

c) Sua implementação não deve exigir qualquer alteração no servidor ou processo para manuseio do dado pelo usuário final.

d) Deve ser capaz de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações não estruturadas (por exemplo: imagens, vídeos, arquivos voz,SYSLOG etc.).

e) Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso.

f) As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio.

g) Essas diretivas devem permitir serem baseadas em usuário, processo, tipo de arquivo.

h) Os agentes devem permitir a criptografia ou rotação de chaves sem bloquear o acesso de usuários ou de aplicativos aos dados em questão, ou seja, sem indisponibilidade nos serviços. Rotação de chaves significa descriptografar os dados com a chave criptográfica atual e criptografá-los com uma nova chave criptográfica.

i) Os agentes devem possuir certificação FIPS 140-2 Nível 1, ou certificação compatível;

j) As políticas devem ser aplicadas aos usuários locais, ou igualmente integradas no AD ou no LDAP.

k) Deve suportar autenticação multifator para ambientes Windows

l) Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com o console de gerenciamento para poder aplicar processos de criptografia e descriptografia.

m) Os logs de atividade do usuário devem ter a capacidade de ser enviado para uma solução de SIEM através de um servidor deSYSLOG ou no formato CEF, em tempo real e nativamente.

n) Este módulo deve suportar ambientes em nuvem, tais como AWS, Azure, pelo menos.

o) Este módulo deverá registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos.

p) Possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados.

q) Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não criptografado.

r) Compatibilidade com os sistemas operacionais, comprovada por matriz de compatibilidade:

r.1.) Windows Server: 2016 e superiores.

r.2.) Linux: RedHat 7-6;

r.3.) CentOS, Ubuntu e Debian.

2.2.3. ITEM 3 - MÓDULO DE SEGURANÇA DE DADOS ESTRUTURADOS MULTIPLATAFORMA.

a) Este módulo deve fornecer criptografia de banco de dados (dados estruturados) para dados em repouso com gerenciamento centralizado de chaves, controle de acesso de usuários, incluindo usuários privilegiados, e registro detalhado de auditoria de acesso visando atender aos requisitos de conformidade e práticas recomendadas para proteger os dados, onde quer que estejam. O módulo deverá residir no sistema operacional ou na camada de dispositivo, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela.

b) O processo de criptografia deve ser executado por agentes que serão instalados nos servidores de banco de dados.

c) Não serão aceitas soluções de criptografia nativa de sistemas operacionais;

d) Eles devem ser compatíveis com bancos de dados estruturados e não estruturados, incluindo MS-SQL Server, MySQL, DB2, Informix, Oracle, Sybase, Cassandra,Maria DB, MongoDB ePostgreSQL;

e) Deve ser compatível com servidores físicos e versões virtualizadas.

f) Sua implementação não deve exigir qualquer alteração no banco de dados ou na aplicação.

g) Estes devem usar os recursos de aceleração disponíveis, como o AES-NI. A implementação destes não deve gerar uma carga incremental, típica em servidores, de mais de 5%.

h) Além de criptografar o banco de dados, os agentes devem ser capazes de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações estruturadas e não estruturadas (por exemplo: imagens, vídeos, arquivos voz,SYSLOG).

i) Os agentes devem permitir a criptografia ou rotação de chaves sem bloquear o acesso de usuários ou de aplicativos aos dados em questão, ou seja, sem indisponibilidade nos serviços.

j) Rotação de chaves significa descriptografar os dados com a chave criptográfica atual e criptografá-los com uma nova chave criptográfica.

k) Os agentes devem possuir certificação FIPS 140-2 Nível 1, ou certificação compatível;

l) Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso.

m) As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio.

n) Essas diretivas devem permitir e serem baseadas em usuário, processo, tipo de arquivo.

o) As políticas devem poder ser aplicadas aos usuários locais, ou igualmente integradas no AD ou no LDAP.

p) Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com o console de gerenciamento, para poder aplicar processos de criptografia e descriptografia.

q) Os logs de atividade do usuário devem poder de ser enviados para uma solução de SIEM através de um servidor de SYSLOG ou no formato CEF, em tempo real e nativamente.

r) A solução deve suportar ambiente em nuvem, tais como AWS, Azure, pelo menos.

s) A solução deve ter a capacidade de integrar os serviços de gerenciamento de chaves fornecendo serviços de gerenciamento de chaves no local ou na nuvem, para aplicações como Salesforce.com.

t) Registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos.

u) Possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados.

v) Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não criptografado.

w) Requerimentos complementares:

x) Compatibilidade com os sistemas operacionais, comprovada por matriz de compatibilidade:

x.1.) Windows Server: 2016 e posteriores.

x.2.) Permitir criptografia para múltiplos fabricantes de banco de dados, tais como:

x.3.) MySQL (Windows, Linux);

x.4.) MS SQL (Windows).

2.2.4. ITEM 4 - MÓDULO PARA TRANSFERÊNCIA SEGURA DE BASE DE DADOS

a) Este Módulo deve permitir o mascaramento dos dados sensíveis para permitir o compartilhamento seguro com terceiros, ambientes de teste, ambientes de desenvolvimento e outros casos de uso aplicáveis.

b) O funcionamento deve ser baseado em tabela e/ou coluna. Informa-se o que deverá ser mascarado no novo banco de dados de destino. Com isso, dados não identificados podem ser compartilhados.

c) A solução de ser customizável e de alta performance.

d) A solução deve suportar, pelo menos, as operações de criptografia / Toquenização e descriptografia / destoquenização de tabelas e / ou colunas.

e) A solução deve ser transparente para a aplicação ou banco de dados com acesso via conexão ODBC. Ou seja, não deve requerer alterações ou instalações adicionais no servidor de banco de dados.

f) A solução deve suportar, pelo menos, arquivo CSV, Microsoft SQL Server, MySQL.

g) A solução deve permitir replicação de arquivo para arquivo, banco de dados para banco de dados, arquivo para banco de dados e banco de dados para arquivo.

h) Pelo menos os seguintes modelos devem ser suportados: Standard AES Encryption, Batch random Tokenization e Batch FPE FF3/FF1.

2.2.5. ITEM 5 - MODULO DE SEGURANÇA PARA APLICAÇÕES WEB

a) Este agente deve permitir a MASCARAÇÃO VAULTLESS com o DYNAMIC DATA MASKING, para eficientemente Anonimizar dados, incluindo dados pessoais, quer eles residem on premises, ambientes de big data ou a nuvem. Com isso, reduzir o escopo de conformidade substituindo dados confidenciais por um token não-sensível que olha e age como o original. Ou seja, proteção de dados sem a necessidade de alterar bancos de dados. Depois que os dados confidenciais são substituídos pelo token, os sistemas não estão mais sujeitos a conformidade, significando menos esforço para atender regulamentações.

b) Possuir alto desempenho com baixo impacto na performance da aplicação.

c) Possuir servidores de token virtual escalável.

d) Comunicação via TLS autenticado mutuamente.

e) Interface REST API com chamadas individuais e em lote.

f) Permitir geração de Tokens Aleatórios.

g) Compatível com FPE FF1, Tokens FF3.

h) Permitir Mascaramento Dinâmico ou Estático de Dados.

i) Gerenciamento de chaves e políticas.

j) Suporte AD / LDAP.

k) Suporte a dados numéricos e alfanuméricos.

l) Permitir a criação de tokens em formatos numéricos, de texto e de data para aplicativos únicos ou múltiplos.

m) Permitir utilizar grupos de usuários LDAP para decidir quais informações são exibidos para grupos específicos. Por exemplo, operadoras de call center versus gerentes de call center.

n) Suportar servidor de tokens no formato virtual de sua escolha: OVF, ISO, Microsoft Azure Marketplace ou Amazon AMI.

o) Restringir o acesso a ativos confidenciais sem alterar os esquemas do banco de dados, sem interrupções.

p) Proteger dados em trânsito e em repouso.

q) Mascarar os dados em ambiente de produção, homologação, desenvolvimento, teste e terceirizados com acesso ao banco de dados.

r) Proteger DBAs, administradores de sistema, root, e usuários mal-intencionados com acesso direto ao banco, uma vez que os dados que este irão acessar não são dados reais.

2.2.6. ITEM 6 - MÓDULO DE GESTÃO DE CHAVES LOCAL.

a) Ser capaz de potencializar o gerenciamento de chaves de aplicativos de terceiros que usam criptografia nativa, tal como bancos de dados.

b) O agente deve ter a capacidade de conectar-se com os aplicativos por meio de interfaces padrão e fornecer acesso às funções robustas de gerenciamento de chaves.

c) Prove simplificação e redução da carga operacional por meio do gerenciamento centralizado de chaves.

d) Elevar o nível de segurança pela separação das chaves de criptografia das aplicações, banco de dados, servidores de armazenamento etc.

e) Gerenciar chave utilizando soluções de hardware ou software com certificação FIPS ou equivalente.

f) Suportar o protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP / PKCS) que é o padrão do setor para troca de chaves de criptografia entre clientes (usuários principais) e um servidor (armazenamento de chaves). A padronização simplifica o gerenciamento de chaves externas.

g) Garantir a custódia de chaves para, pelo menos:

g.1.) A Oracle TDE;

g.2.) SQL TDE;

g.3.) Nutanix;

g.4.) Cisco;

g.5.) Netapp;

g.6.) Certificados;

g.7.) Aplicações desenvolvidas em casa;

2.2.7. ITEM 7 - MÓDULO DE VALIDAÇÃO DE CONTROLE DE SEGURANÇA CONTRA AMEAÇAS DE REDE, ENDPOINT, APLICAÇÃO WEB, E-MAIL E VAZAMENTO DE DADOS.

a) <u>Características Gerais</u>

a.1.) Deverá permitir que os usuários façam update dos agentes em um único click na manager.

a.2.) A solução proposta deve ter integração com solução de segurança para criação de um playbook personalizado para desenvolver cenários específicos para melhorar a eficácia dos analistas.

a.3.) A solução proposta deve ser integrável com solução de SEGURANÇA PELOS seguintes motivos:

a.4.) Criar playbooks personalizados para desenvolver cenários específicos para melhorar a eficácia dos analistas.

a.5.) Depois que uma nova ameaça é adicionada à Threat Library, usa ferramenta de segurança para agendar uma simulação de ataque.

a.6.) Pegar sugestões de mitigação diretamente da biblioteca de mitigação da Picus Platform para a solução de segurança e usá-las nos playbooks para acelerar a automação do processo.

a.7.) Ver quais ameaças foram bloqueadas ou perdidas e remediar lacunas automaticamente

b) <u>API e Integrações</u>

b.1.) A solução proposta deve suportar integração e comunicar com outras soluções baseado em acesso "Application Control Interface" (API) ou pelo protocolo Syslog, pelos motivos de:

b.1.1.) Relatórios personalizados

b.1.2.) Dashboards personalizadas

b.1.3.) Integração com soluções de terceiros como SOAR, SIEM ou outras plataformas

b.1.4.) Criar Templates dinâmicos e estáticos.

b.1.5.) Criar simulações e executá-las.

b.1.6.) Exportar mitigações

b.1.7.) Exportar listas de ameaças

b.2.) A solução proposta deve ter as seguintes opções disponíveis para funções GET via API:

b.2.1.) Listar Agentes e detalhes

b.2.2.) Integrações e detalhes de integrações

b.2.3.) Lista de dispositivos de mitigação e lista de assinaturas

b.2.4.) Lista de simulação e detalhes

b.2.5.) Resultados detalhados das simulações

b.2.6.) Mapeamento MITRE para resultados das simulações

b.2.7.) Templates para operações de ameaça

b.2.8.) Lista de ameaças e informações detalhadas

b.3.) A solução proposta deve ter as seguintes opções disponíveis para funções POST/PUT/DELETE via API:

b.3.1.) Informações do Token do Agente

b.3.2.) Criar/Começar/Pausar/Update/Deletar Simulação

b.3.3.) Criar templates de Ameaças

b.4.) A solução proposta deve ter a possibilidade de integrar com sistemas de ticket e comunicação como:

b.4.1.) ServiceNow

b.4.2.) Módulo de infiltração de E-mail

b.4.3.) A solução proposta deve performar um ataque de Attachment usando o protocolo SMTP da internet até o domínio da empresa

b.4.4.) Aplicação de Ataques Web

b.4.5.) A solução proposta deve permitir que os usuários alterem as portas HTTP e HTTPS padrões.

b.4.6.) O ataque a databases da solução proposta deve incluir pelo menos 204 (duzentos e quatro) ataques a web aplicações únicas na biblioteca de ameaças.

b.4.7.) Endpoint Attack para Modulo Linux

b.4.8.) A solução proposta deve imitar métodos maliciosos usados por APT's (Advanced Persistent Threats) enquanto testa os controles de segurança do Linux endpoint, sem infectar o sistema operacional subjacente.

b.4.9.) O ataque a database da solução proposta deve incluir cenários com Linux endpoint na biblioteca de ameaças.

b.4.10.) Endpoint Attack para Módulo MacOS

b.4.11.) A solução proposta deve imitar métodos maliciosos usados por APT's (Advanced Persistent Threats) enquanto testa os controles de segurança do MacOS endpoint, sem infectar o sistema operacional subjacente.

b.4.12.) O ataque a database da solução proposta deve incluir cenários com MacOS endpoint na biblioteca de ameaças.

b.4.13.) Módulo de Ataque Customizado

b.4.14.) A solução proposta deve permitir aos usuários adicionar processos de Play e Rewind com as seguintes informações a serem adicionadas:

b.4.15.) Caminho e Argumento

b.4.16.) Capacidade de Adicionar um arquivo remoto

b.4.17.) Capacidade de Usar um arquivo local

b.4.18.) Definir lógica de resultado

b.4.19.) Informações de Metadata

b.4.20.) Detalhes da Ação

b.4.21.) Gerenciamento e segurança

b.4.22.) O Gerenciamento da solução proposta deve ser capaz de operar em ambos On-Cloud ou On-Premises.

b.4.23.) A solução proposta deve permitir aos usuários a criação de dashboards para simulações selecionadas.

b.4.24.) A solução proposta deve acessar controles de Endpoint, Network e Email Security executados em sistema físico, virtual e em nuvem através de um agente unificado Windows com suporte a Windows 10 e 11 e sistemas Server versão 2016, 2019 e 2022.

b.4.25.) A solução proposta deve ser capaz de suportar autenticação 2FA com Aplicativos Autenticadores.

b.4.26.) A solução proposta deve permitir aos administradores acesso aos Audit Logs através da Web UI e analisar com opções de filtragem.

b.4.27.) A solução proposta deve permitir aos administradores configurarem integração Syslog para Audit Logs via TCP ou UDP a um coletor de logs com formatos CEF ou JSON.

b.4.28.) A solução proposta deve permitir administradores a exportarem Audit Logs em arquivos CSV.

b.4.29.) A solução proposta deve permitir a criação de múltiplos e customizáveis perfis - (i) admins, (ii) analistas e (iii) viewers com autorização de monitoramento apenas. Opções customizáveis deveriam ser:

b.4.29.1.) Simulações

b.4.29.2.) Templates

b.4.29.3.) Agentes

b.4.29.4.) Ameaças Personalizadas

b.4.29.5.) Ações Personalizadas

b.4.29.6.) REST API Token

b.4.29.7.) Gestão de Organização

b.4.29.8.) Mitigação

b.4.29.9.) Módulo de Detecção Analítica

b.4.29.10.) A solução proposta deve ter a infraestrutura necessária para integrar com as seguintes tecnologias:

b.4.29.11.) CrowdStrike EDR

b.4.29.12.) Elastic SIEM

b.4.29.13.) IBM Qradar SIEM

b.4.29.14.) Logrhythm SIEM

b.4.29.15.) Logsign SIEM

b.4.29.16.) Microfocus Arcsight ESM

b.4.29.17.) Microsoft Defender for Endpoint EDR

b.4.29.18.) Microsoft Sentinel SIEM

b.4.29.19.) Palo Alto Cortex XDR

b.4.29.20.) RSA Netwitness SIEM

b.4.29.21.) Securonix SIEM

b.4.29.22.) Sentinel One EDR

b.4.29.23.) Splunk SIEM (Onprem & Cloud)

b.4.29.24.) Trend Micro XDR

b.4.29.25.) VMware Carbon Black EDR (Onprem & Cloud)

c) <u>MÓDULO DE ANÁLISE DE DETECÇÃO</u>

c.1.) A solução proposta deve ser capaz de fornecer Log Source Information para REGISTRAR AS ações necessárias.

c.2.) A solução proposta deve ser capaz de fornecer Detecção de Conteúdo para os seguintes vendedores de SIEM ou EDR:

c.3.) Arcsight ESM

c.4.) Carbon Black EDR

c.5.) IBM Qradar

c.6.) Splunk SIEM

c.7.) A solução proposta deve ser capaz de fornecer Detecção de Conteúdo como regras de open-source SIGMA para outros vendedores de SIEM/XDR/EDR.

c.8.) A solução proposta deve permitir aos usuários visualizarem todas as regras de recomendação para ações através da seção dedicada UI. Solução deve permitir a filtragem de ações "Not Alerted".

d) <u>REPORTING</u>

d.1.) A solução deve ser capaz de exportar semanalmente ou mensalmente relatórios técnicos executivos em formato PDF.

d.2.) Relatórios técnicos mensais ou semanais para todas as simulações no sistema vão ser gerados automaticamente.

d.3.) Usuários devem ser capazes de gerenciar as preferências automáticas relatórios técnicos e executivos nas configurações de Relatórios para relatórios semanais e mensais.

d.4.) Usuários devem poder visualizar as simulações que são autorizados a ver nos relatórios.

d.5.) Quando relatórios semanais e mensais são criados, usuários devem ser notificados por e-mail. As pessoas que irão receber as notificações por e-mail devem ser determinadas através da tela de configurações.

d.6.) Usuários devem ser capazes de gerar relatórios através das páginas "Dashboard" e "Simulation History".

d.7.) Usuários devem ser capazes de selecionar simulações, conteúdo de relatório (prevenção, detecção ou ambos), seções do relatório (de seções pré-definidas) e editar a descrição do relatório no fluxo de geração de relatórios.

d.8.) A solução proposta deve ser capaz de compartilhar valores de benchmark para os top 5 resultados de templates mais simulados.

d.9.) A solução proposta deve ser capaz de compartilhar valores de benchmark para MITRE ATT&CK Tactics.

2.2.8. ITEM 8 - SERVIÇO DE TREINAMENTO OFICIAL.

a) O treinamento de capacitação técnica será ministrado para até 8 participantes selecionados pelo (a) (órgão), com carga horária mínima de 16 (dezesseis) horas, material oficial do fabricante, e conteúdo necessários a capacitá-los para utilizar o Sistema ofertado.

b) O treinamento de capacitação técnica será ministrado para até 8 participantes selecionados pelo (a) (órgão), com carga horária mínima de 16 (dezesseis) horas, material oficial do fabricante, e conteúdo necessários a capacitá-los para utilizar o Sistema ofertado.

c) Deverá ser emitido certificado de participação ao final do curso.

d) Todo o material didático deve ser repassado de forma impressa e em mídia para os alunos.

e) Somente serão aceitos materiais oficiais dos fornecedores do Sistema ofertado, e não será permitida a adaptação sobre apostilas/conteúdos de cursos não oficiais.

f) Os instrutores deverão possuir experiência em didática, além de possuir certificação comprovada na área de segurança, em pelo menos uma das seguintes certificações:

f.1.) CSSLP - Certified Secure Software Lifecycle Professional (ISO/IEC 17024).

f.2.) CISSP – Certified Information System Security Professional.

f.3.) ISSAP – Information System Security Architect Professional.

f.4.) CISM – Certified Information Security Manager;

f.5.) CompTIA Security+: Competency in system security, network infrastructure, access control and organizational security.

g) O treinamento deverá ocorrer nas dependências da CONTRATANTE, ou local por ela indicado na capital do estado, ficando responsável por montar o ambiente adequado para realização do mesmo, isto é, todo o espaço necessário assim como toda infraestrutura computacional e de rede necessária. Caberá à CONTRATADA instalar a solução ou possibilitar o acesso ao Sistema no ambiente de treinamento.

h) Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento e hospedagem, a confecção e distribuição dos originais do material didático e a emissão de certificados para os profissionais treinados.

2.2.9. ITEM 9 - SERVIÇO DE IMPLEMENTAÇÃO DE CONSOLE DE GERENCIAMENTO DE CHAVES DE CRIPTOGRAFIA

a) FORNECIMENTO DAS LICENÇAS.

a.1.) O fornecimento das licenças que compõem a solução deverá ocorrer por intermédio de ordem de fornecimento de bens.

a.2.) A CONTRATADA terá o prazo de 5 (cinco) dias úteis para realizar a entrega das licenças a partir da data de emissão da ordem de fornecimento de bens.

a.3.) As licenças deverão ser fornecidas na forma de certificado nomeado a PMVG, e com os respectivos números de série.

a.4.) Na ocasião do fornecimento das licenças, deverão ainda ser entregues os aplicativos instaladores (executáveis/binários) acompanhados de documentação técnica em formato digital (manuais de operação) de cada software que compõem a solução.

b) INSTALAÇÃO E CONFIGURAÇÃO.

b.1.) A implantação da solução será realizada por intermédio da abertura de Ordem de Serviço específica.

b.2.) As seguintes atividades fazem parte de seu escopo:

b.3.) Elaboração de plano de instalação, contendo todos os requisitos técnicos, etapas, prazos e matriz de responsabilidades;

b.4.) Instalação da solução todos os módulos que a compõe, no ambiente disponibilizado pela PMVG;

b.5.) Configurações necessárias para emissão de alertas através do sistema de correio eletrônico da PMVG

b.6.) Integração com NOC da PMVG.

b.7.) Caberá a PMVG disponibilizar o ambiente tecnológico para que a solução da CONTRATADA seja instalada e configurada.

b.8.) O prazo máximo para a execução do serviço é de 30 (trinta) dias úteis, a contar da data em que a PMVG disponibilizar o ambiente e credenciais de acesso para a execução da instalação e configurações.

b.9.) Ao término da execução do serviço, a CONTRATADA deverá elaborar um relatório com evidência de todo o processo de instalação, e ceder credenciais de acesso à equipe da PMVG.

b.10.) O serviço de instalação e configuração da solução foi estimado como atividade de ocorrência única, posto que uma vez concluído, servirá como base para todos os outros serviços que fazem parte do escopo do contrato.

b.11.) A instalação e configuração da plataforma deverá ser realizada nas dependências da PMVG, em horário comercial.

c) MANUTENÇÃO, SUPORTE TÉCNICO E GARANTIA.

c.1.) A CONTRATADA deverá disponibilizar o canal de suporte técnico, através de serviço telefônico, por no mínimo, 8x5 (oito horas por dia, cinco dias por semana), com atendimento, obrigatoriamente em língua portuguesa, falada no Brasil, devendo operar, no mínimo, em dias úteis no horário comercial, das 8h (oito horas) às 18h (dezoito horas), horário de Brasília.

c.2.) A CONTRATADA deverá fornecer suporte técnico no Brasil, obrigatoriamente em língua portuguesa, falada no Brasil para prestar atendimento e resolver todos os problemas relacionados às possíveis falhas ou interrupções de funcionamento da solução proposta, sempre que solicitado pela PMVG;

c.3.) A CONTRATADA deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da PMVG. De modo a assegurar alta disponibilidade do canal de suporte técnico para o Sistema fornecido, o registro de chamados deve estar disponível em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados).

c.4.) Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o serviço.

c.5.) A PMVG poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência do contrato, para suprir suas necessidades com relação aos produtos de segurança.

c.6.) Para efeito de avaliação dos níveis de serviços prestados no suporte técnico, considerar-se-á a contagem de tempo de atendimento apenas para os chamados abertos no curso do período de atendimento, em horário comercial, de modo que os chamados abertos foram deste período serão contabilizados apenas a partir do início do período útil operacional seguinte.

c.7.) Relatórios sobre a prestação dos serviços:

c.8.) A contratada fornecerá relatórios mensais sobre a prestação dos serviços, em papel e em arquivo eletrônico, preferencialmente em formato PDF, com informações analíticas e sintéticas sobre os serviços realizados, incluindo-se chamados abertos e fechados, enfatizando aqueles resolvidos no período.

c.9.) Constarão dos relatórios dados de todos os chamados ocorridos no período, data e hora de abertura do chamado, data e hora de início do atendimento, data e hora de fechamento do chamado, nome da pessoa que abriu o chamado, nome da pessoa que efetuou o atendimento, descrição do problema e descrição da solução.

c.10.) Também devem constar dados da reabertura de chamados, quando for o caso, que foram fechados sem serem devidamente resolvidos e que, por esse motivo, necessitaram ser reabertos.

c.11.) Deverá ainda apresentar relatório para cada solicitação de suporte remoto, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes.

c.12.) Os atendimentos das ocorrências técnicas devem ser realizados em acordo com os critérios definidos pelos níveis de serviço da tabela abaixo, estando sujeita a CONTRATADA, no caso do descumprimento dos prazos, às sanções especificadas a seguir:

	NÍVEL DE SEVERIDADE DO CHAMADO			
	BAIXA	**MÉDIA**	**ALTA**	**URGENTE**
Descrição do chamado	Problema técnico que gere pouco ou baixo impacto na utilização da solução.	Problema técnico que impeça a utilização parcial de uma funcionalidade, não impedindo por completo seu uso.	Problema técnico que impeça completamente a utilização de uma funcionalidade.	Problema técnico que impeça a utilização da solução em sua totalidade.
Prazo para atendimento da ocorrência	Até 12 horas úteis	Até 8 horas úteis	Até 4 horas úteis	Até 0,5 horas úteis

c.13.) Sempre que o fabricante da solução disponibilizar versões mais atuais da solução oferecida, a licitante deverá fornecer estas versões e releases dos softwares da solução para a PMVG, sem ônus adicionais, enquanto o contrato estiver vigente.

c.14.) Entende-se por manutenção corretiva a série de procedimentos destinados ao restabelecimento operacional da solução com todas suas funcionalidades, motivados pela ocorrência de incidentes na solução e/ou problemas recorrentes na solução, compreendendo, inclusive, atualização de softwares por

um substituto de igual ou maior configuração, ajustes, reparos, correções necessárias;

c.15.) Entende-se por suporte técnico aquele efetuado mediante atendimento telefônico ou remoto, para resolução de problemas e esclarecimentos de dúvidas sobre a configuração e utilização da solução.

c.16.) Os serviços deverão ser realizados por meio de técnicos especializados, devidamente credenciados para prestar os serviços de garantia e assistência técnica remoto, de forma rápida, eficaz e eficiente, sem quaisquer despesas adicionais para a PMVG, inclusive quanto às ferramentas, equipamentos e demais instrumentos necessários à sua realização.

2.2.10. ITEM 10 - SERVIÇO SOB DEMANDA PARA IMPLEMENTAÇÃO DE AGENTES DE CRIPTOGRAFIA

a) O FORNECIMENTO DOS SERVIÇOS ESPECIALIZADOS OBJETO DESTE CERTAME OBSERVARÁ O SEGUINTE QUANTITATIVO:

Item	Descrição	Unidade	Quantidade
10	Serviço sob demanda para Implementação de agentes de criptografia.	UST	3000

a.1.) Os serviços especializados tratam da operacionalização da gestão de chaves criptográficas, com apoio presencial de pessoal especializado ou remoto caso definido pela PMVG, devendo ser solicitado mediante emissão de ordem de serviço, informando às aplicações que farão parte do escopo do serviço.

a.2.) Todas as atividades desempenhadas relativas aos serviços especializados deverão ser executadas nas dependências da PMVG, respeitando o horário de funcionamento da PMVG, e com o acompanhamento e ciência dos servidores.

a.3.) Os serviços especializados serão demandados de acordo com a necessidade da PMVG, de forma proporcional ao número de agentes de criptografia instalados, mensurados através da métrica de UST, considerando que uma hora de trabalho equivale a uma UST.

a.4.) Dada as diferentes atividades que compõem os serviços especializados, foram definidos três níveis de complexidade que visam garantir o equilíbrio físico-financeiro de sua execução, conforme disposto na tabela abaixo:

Nível de Complexidade	Definição
Normal	Cada hora de trabalho equivale a uma UST.
Média	Cada hora de trabalho equivale a duas UST's
Alta	Cada hora de trabalho equivale a três UST's.

a.5.) Os serviços especializados deverão ser executados por colaboradores da CONTRATADA, respeitando as normas de segurança da informação da PMVG, executando as atividades observando criteriosamente o escopo definido nas respectivas ordens de serviços.

2.2.11. ITEM 11 - SERVIÇO DE CONSULTORIA PARA AVALIAÇÃO PERIÓDICA (HEALTH CHECK).

a) O Serviço deverá ser prestado pelo fabricante da solução e rever a implementação existente, validando as suas políticas de operação e proteção. Estes elementos serão avaliados contra as melhores práticas de mercado e as políticas específicas do cliente. Todos os procedimentos operacionais, e configurações deverão ser avaliados e documentados para garantir a estabilidade de integridade e tolerância a falhas.

b) O Serviço deverá contemplar toda a solução implementada desde as consoles até os agentes de proteção de dados.

c) Deverá ser executado mediante emissão de ordens de serviço.

d) Deverá ser executado periodicamente de não exceder o intervalo de dois meses entre as execuções.

e) O Serviço deverá ser executado nas dependências do cliente, prioritariamente, em horário comercial. Caso o CLIENTE julgue necessário poderá ser agendada uma janela de manutenção fora do horário comercial sem custos adicionais para a contratante.

f) As Seguintes atividades deverão ser cobertas pelo serviço:

g) Verificar a configuração da solução, versão instalada e os requisitos de atualização, provendo relatório de impacto e orientação de planejamento para atualização;

h) Verificar a configuração de alta disponibilidade e status de replicação;

i) Verificar os procedimentos para failover;

j) Verificar os procedimentos de backup e restauração da plataforma, e as configurações do custodiante da chave;

k) Verificar as configurações de contas de administradores e domínios em relação aos requisitos de segurança;

l) Verificar os níveis e configurações de log atuais, a integração com quaisquer ferramentas SIEM e fornecer qualquer orientação sobre melhorias;

m) Verificar se as melhores práticas para backup automático e chaves estão implementadas e documentadas;

n) Identificar quaisquer políticas atualmente no modo de aprendizagem e o impacto potencial de permanecer nesse estado;

o) Avaliar e verificar os procedimentos gerais de implantação para criar e atualizar políticas e verificar a eficácia geral das políticas;

p) Analisar as configurações de log da solução e fazer as recomendações para eliminar mensagens de log desnecessárias e reduzir o número de logs que a solução precisa processar;

q) Demonstrar e executar relatórios que podem ser usados para verificar os resultados;

r) Revisar os procedimentos de atualização dos agentes de proteção instalados, como políticas de criptografia, configuração de hosts e instalação dos agentes;

s) Revisar os procedimentos operacionais existentes ou procedimentos de implantação de melhores práticas definidos e fazer recomendações e alterações conforme necessário;

t) Emitir relatório de status de saúde geral (HealthCheck) do ambiente contemplando, no mínimo, todos os itens de revisão e verificação.

u) Ao término da execução dos serviços de "HealthCheck" os relatórios deverão serão apresentados à contratada em mídia eletrônica para emissão do termo de aceite da ordem de serviço.

2.2.12. ITEM 12 - SERVIÇO DE ANÁLISE DE RISCO – SAR

a) Planejamento do gerenciamento de risco

b) Identificação dos riscos

c) Realização de análise quantitativa (Probabilidade)

d) Realização da análise Qualitativa (impacto)

e) Planejar resposta aos riscos

f) Controlar os riscos

g) Fazer levantamento de ameaças, coletando informações acerca dos seus processos de tecnologia buscando pelas principais ameaças que possam ser claramente identificadas:

g.1.) Perda de dados;

g.2.) Incêndio em data center

g.3.) Software desatualizados;

g.4.) Sistemas fora do ar;

g.5.) Colaboradores sem treinamento;

g.6.) Excesso de usuários privilegiados.

g.7.) Sistemas operacionais desatualizados.

h) Criação de matriz de risco formada por dois eixos: a probabilidade da ocorrência do risco e o impacto que ele trará caso ocorra.

h.1.) Eixo da probabilidade: Quase certo: é praticamente impossível evitar que o risco aconteça, por isso vale a pena pensar em ações de mitigação do impacto do risco depois dele ocorrer;

h.1.1.) Alta: a chance de o risco ocorrer é grande e frequentemente ele ocorre de fato;

h.1.2.) Média: probabilidade ocasional de acontecimentos do risco. Ainda vale a pena planejar desdobramentos, mas não com tanta preocupação como nos casos anteriores;

h.1.3.) Baixa: pouca chance de acontecer algum problema advindo desse risco;

h.1.4.) Rara: É bastante improvável que o risco aconteça, só vale a pena se preocupar em casos de impacto grave ou gravíssimo para o seu projeto.

h.2.) Eixo do impacto:

h.2.1.) Gravíssimo: pode fazer com que o projeto seja cancelado ou que o dano ocasionado por ele seja irreversível;

h.2.2.) Grave: compromete de forma acentuada o resultado do projeto, ocasionando atraso ou insatisfação do cliente;

h.2.3.) Médio: perda momentânea ao longo do projeto que pode ser corrigida, mas com o impacto no escopo ou no prazo;

h.2.4.) Leve: desvio quase imperceptível dos objetos do projeto ser facilmente corrigido;

h.2.5.) Sem impacto: não gera nenhum tipo de problema perceptível para o projeto, por isso pode ser ignorado em 99% dos casos. Só dê atenção se esse risco ocorrer quase com certeza e com alta frequência.

2.2.13. ITEM 13 - SERVIÇO DE DIAGNÓSTICO, AVALIAÇÃO, MAPEAMENTO E LEVANTAMENTO DO PARQUE TECNOLÓGICO

a) Executar diagnóstico de conformidade sobre o ambiente tecnológico do cliente.

b) Executar levantamento de parque tecnológico, com todas as suas características:

b.1.) Quantidade de servidores de arquivos (dados não estruturados).

b.1.1.) Qual a versão do sistema operacional (SO) dos Servidores (Windows, Linux e etc)

b.2.) Quantidade de servidores de banco de dados (dados estruturados).

b.2.1.) Qual as versões dos Sistemas operacionais (SO) dos servidores. (Windows, Linux etc.).

b.2.2.) Quais os Banco de dados existentes (Oracle, Mysql, Sql e etc).

b.3.) Executar levantamento por serviço de aplicação que faz chamadas " API REST"

b.4.) Mapeamento de dados sensíveis e seus fluxos de interação entre usuários e dados não estruturados, aplicação/usuários e dados estruturados pré e pós-implantação.

2.2.14. ITEM 14 - SERVIÇO DE GESTÃO DE PROJETOS E DOCUMENTAÇÃO.

a) Resumo do Projeto, Apresentação, Objetivos, Benefícios, Responsabilidades, Recomendações, Premissas e Restrições;

b) Gerenciamento do escopo, declaração do escopo, plano de entrega, regras mudanças de escopo

c) Gerenciamento do Cronograma e prazos do projeto, bem como gestão dos recursos a serem utilizados

d) Gestão de Recursos Humanos alocados no projeto, definição comitê projeto

e) Responsabilidades do Comitê do Projeto

f) Gerenciamento de Riscos do Projeto e mitigação dos mesmos

g) Gerenciamento da Qualidade, métricas e metas de qualidade, lista de verificação de qualidades, documentação de entregas

h) Matriz de obrigatoriedade de documentos e artefatos a serem disponibilizados

i) Gerenciamento das Comunicações e documentação dos projetos

j) Diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico;

k) Detalhamento Do Plano de Projeto

l) A CONTRATADA deverá designar um profissional responsável pela gestão do projeto sendo esse o único ponto de contato com a CONTRATANTE;

m) Após a assinatura do contrato, com prazo máximo de 5 (cinco) dias úteis, a CONTRATADA deverá informar o nome, telefone e e-mail do Gerente de Projetos e agendar a data da reunião inicial de projeto (Kick-off meeting);

n) A reunião inicial de projeto deverá seguir a seguinte pauta:

o) Apresentação das equipes CONTRATADA e CONTRATANTE;

p) Apresentação do Detalhamento do Plano de Projeto – Projeto Executivo

q) Aprovação do Plano do Projeto, após essa etapa iniciar a execução do projeto conforme o plano do projeto – Projeto Executivo

r) Detalhamento do plano do projeto Executivo – Gestão de Projetos

s) Resumo do Projeto, Apresentação, Objetivos, Benefícios, Responsabilidades, Recomendações, Premissas e Restrições;

t) Gerenciamento do escopo, declaração do escopo, plano de entrega, regras mudanças de escopo.

u) Gerenciamento do Cronograma e prazos do projeto, bem como gestão dos recursos a serem utilizados

v) Estabelecimento de cronograma executivo;

w) Gestão de Recursos Humanos alocados no projeto, definição comitê projeto

x) Estabelecimento da lista de contatos e funções definindo claramente.

y) Responsáveis técnicos por cada equipe, profissionais responsáveis pelas definições técnicas do projeto;

z) Executivos de cada equipe, profissionais responsáveis pelos aspectos operacionais, jurídicos e financeiros do projeto;

aa) Analistas de cada equipe, profissionais envolvidos nas diversas atividades de projeto;

bb) Responsabilidades do Comitê do Projeto

cc) Estabelecimento da matriz de relacionamentos;

dd) Estabelecimento da matriz de responsabilidades identificando quem executa, quem precisa ser informado, quem avalia, quem aprova e quem aceita formalmente o resultado em nome da CONTRATANTE.

ee) Gerenciamento de Riscos do Projeto e mitigação dos mesmos

ff) Gerenciamento da Qualidade, métricas e metas de qualidade, lista de verificação de qualidades, documentação de entregas

gg) Matriz de obrigatoriedade de documentos e artefatos a serem disponibilizados

hh) Gerenciamento das Comunicações e documentação dos projetos

ii) Estabelecimento do plano de comunicação entre as equipes de forma que todos estejam atualizados em relação às diversas atividades de projeto;

jj) Estabelecimento do formato e dos meios de troca de informações entre as equipes da CONTRATADA e da CONTRATANTE;

kk) Definição da agenda das reuniões de acompanhamento de projeto.

2.2.15. ITEM 15 - SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO (HELP DESK)

a) A CONTRATADA deverá possuir um processo de Help-Desk;

a.1.) **NÍVEL 1**

a.1.1.) Realizar triagem para correta identificação de problemas;

a.1.2.) Prover atendimento via telefone, web, e-mail, chat e acesso remoto à equipamentos (quando disponível);

a.1.3.) Elaborar relatórios técnicos específicos;

a.1.4.) Solucionar dúvidas referentes ao comportamento, comandos, facilidades e características;

a.1.5.) Esclarecer dúvidas sobre mensagens de erro;

a.1.6.) Prestar Suporte técnico durante as mudanças;

a.2.) **NÍVEL 2**

a.2.1.) Prover atendimento especializado para ocorrências complexas;

a.2.2.) Solucionar problemas analisando a causa raiz e propondo planos de ações para evitá-los no futuro;

a.2.3.) Prover informações e recomendações para melhoria dos serviços;

a.2.4.) Contribuir para a base de conhecimento;

a.2.5.) Os profissionais da CONTRATADA executará todas as configurações e customizações necessárias para o pleno funcionamento do ambiente, proporcionando as condições para transferência de know-how;

a.2.6.) Esse serviço deverá ser realizado de forma presencial para assegurar que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos em regime 8 x 5 em horário comercial (08:00 às 18:00);

a.2.7.) A qualidade dos serviços deverá ser assegurada através de processos consolidados e da sólida formação, capacitação e experiência dos profissionais responsáveis pelas atividades;

a.2.8.) OS profissionais da CONTRATADA deverão execução os processos customização de configurações e mudanças, seja em decorrência de alarmes e processos e também por solicitação da CONTRATANTE;

a.2.9.) Os profissionais da CONTRATADA deverão executar as atividades operacionais, utilizando os procedimentos estabelecidos para cada rotina;

a.2.10.) Os profissionais da CONTRATADA deverão executar as atividades de manutenção corretiva, utilizando os procedimentos que permitam maior eficiência e eficácia na solução de falhas

a.2.11.) Os profissionais da CONTRATADA deverão executar as atividades de manutenção preventiva, rotinas de testes, análises e medidas, utilizando os procedimentos que assegurem mínima interferência na . operação e máxima disponibilidade da plataforma

a.2.12.) Os profissionais da CONTRATADA deverão elaborar procedimentos especiais ou detalhamento dos procedimentos padrão, caso seja necessário;

a.2.13.) As customizações e regras das diversas plataformas serão executadas mediantes chamados específicos obedecendo o SLA acordado;

a.2.14.) Os profissionais da CONTRATADA deverão elaborar relatórios de atividades detalhando os procedimentos realizados e eventuais ajustes, se necessário;

a.2.15.) A CONTRATADA deverá prestar o apoio -técnico para campanhas de segurança para usuários finais, em conjunto com as áreas internas da CONTRATANTE, em especial para as áreas de Tecnologia da Informação e Recursos Humanos, para esclarecimento de usuários sobre os riscos e sobre as boas práticas de segurança digital;

a.2.16.) A CONTRATADA deverá disponibilizar informações técnicas para preparação de material de palestras e informativos, bem como as métricas obtidas através

da própria plataforma para ilustração dos principais riscos detectados e mitigados;

a.2.17.) Os profissionais da CONTRATADA deverão promover a manutenção de APPLIANCES e equipamentos dedicados fornecidos pela CONTRATADA;

2.2.16. DESCRIÇÃO DA SOLUÇÃO TECNOLÓGICA NO GERAL

a) A plataforma tecnológica deverá atender às seguintes especificações técnicas e requisitos de gestão:

b) Reduzir a ocorrência de incidentes internos de segurança monitorando a atividade de credenciais com acessos privilegiados, bem como impedindo que estes usuários acessem o conteúdo dos dados. Isso tudo, sem que os mesmos percam privilégio para administrar o ambiente de tecnologia;

c) Estabelecer o controle de acesso para esse tipo de usuário e identificar atividades suspeitas gerando logs destas atividades;

d) Deve estabelecer um modelo de proteção para informações de tal forma que o dado seja devidamente criptografado no sistema de arquivos. Desta forma, além de impedir a extração não autorizada, mesmo em caso de vazamento acidental dos dados, deverá garantir que os dados não possam ser acessados fora do ambiente gerenciado pela plataforma de segurança, uma vez que não terão a chave de criptografia necessária para acessar a informação;

e) Deverá prover mecanismos de prevenção de infecção ou ataques a arquivos por malware, APT, RANSOMWARE, ataques gerados por acesso não autorizado, modificações em bibliotecas entre outros, quando estes forem originados de usuários com acesso privilegiado;

f) Deverá ser flexível e escalável, adequando-se às necessidades de crescimento da empresa contratante;

g) Deverá permitir a anonimização dos dados pessoais e/ou confidenciais, conforme definido no artigo 12 da Lei Geral de Proteção de Dados Brasileira (LGPD);

h) Deverá proteger sistemas de dados estruturados (bancos de dados) e sistemas de dados não estruturados (incluindo arquivos de aplicativos da Microsoft, voz, vídeo e

texto em geral) em um ambiente heterogêneo de sistemas operacionais e plataformas de operação;

i) Deverá suportar pelo menos:

I. Sistemas operacionais Microsoft Windows Server, e Linux;

II. Os bancos de dados suportados devem incluir MS-SQL, MySQL e arquivos;

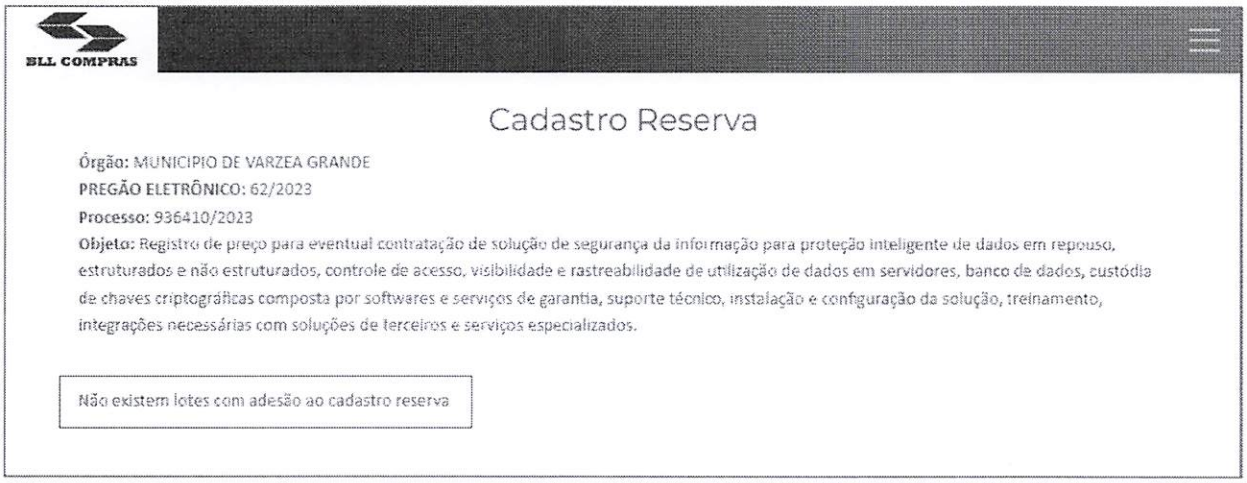
III. Provedores de nuvem suportados devem incluir AWS S3, Azure, Office 365, Oracle Cloud e IBM Cloud;

j) Deverá prover console de gerenciamento centralizado para facilitar o processo de administração, controle de acesso, gestão e logs e manutenção da plataforma de segurança de dados;

k) Soluções baseadas em software livre não serão aceitas.

CLÁUSULA TERCEIRA – DO CADASTRO RESERVA

3.1. Não houve cadastro reserva para este processo.



CLÁUSULA QUARTA – DA GERÊNCIA DA ATA DE REGISTRO DE PREÇOS

4.1. A **Secretaria Municipal de Administração** é o **ÓRGÃO GERENCIADOR** e responsável pela condução do conjunto de procedimentos para o registro de preços e gerenciamento da ata de registro de preços dele decorrente e à Procuradoria Geral do Município, nas questões legais. (Art. 2º, III, do Decreto nº. 7.892/2013).

PROC. ADM. Nº. 936410/2023 **PREGÃO ELETRÔNICO Nº. 62/2023**

CLÁUSULA QUINTA – DA VIGÊNCIA

5.1. O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses, contados da data da publicação, vedada sua prorrogação. (Art. 12 do Decreto 7.892/2013).

CLÁUSULA SEXTA – DAS ADESÕES DA ATA DE REGISTRO DE PREÇOS

6.1. Poderão utilizar-se desta Ata de Registro de Preços, durante sua vigência, qualquer órgão ou entidade de administração pública que não tenha participado do certame licitatório, mediante prévia consulta ao do órgão gerenciador, conforme as regras estabelecidas na Lei Federal nº 8.666/93, 10.520/02 e nos termos do Decreto Federal nº 7.892/2013 e Decreto Municipal nº. 54/2019.

6.2. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o órgão gerenciador e órgãos participantes, conforme Artigo 22, § 2º do Decreto 7.892/2013.

6.3. As aquisições ou as contratações adicionais não poderão exceder, por órgão ou entidade, a **cem por cento** dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes conforme preceitua o art. 1, §3º do Decreto Municipal 54/2019.

6.4. As ADESÕES à ata de registro de preços não poderão exceder, na totalidade, ao **quíntuplo do quantitativo** de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participante que aderirem conforme preceitua o art. 1, §4º do Decreto Municipal 54/2019.

6.5. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços, conforme preceitua o art. 22, §6º do Decreto 7.892/2013.

6.6. Ao órgão não participante que aderir à ata competem os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação as suas próprias contratações, informando as ocorrências ao órgão gerenciador. (Art. 22, §7º do Decreto 7.892/2013).

CLÁUSULA SÉTIMA - DOS ACRÉSCIMOS E ALTERAÇÕES NA ATA DE REGISTRO DE PREÇOS

7.1. É vedado efetuar acréscimos nos quantitativos e valores fixados pela Ata de Registro de Preço, inclusive o acréscimo de que trata o §1° do art. 65 da Lei n° 8.666/93. (Art. 12, § 1° do Decreto 7.892/2013).

7.2. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea "d" do inciso II do **caput** do art. 65 da Lei n° 8.666, de 1993. (Art. 17, do Decreto 7.892/2013).

7.2.1. Caso o preço registrado seja superior à média dos preços de mercado por motivo superveniente, a Prefeitura de Várzea Grande convocará os fornecedores registrados, para a negociação da redução do preço registrado, de forma a adequá-lo ao praticado no mercado. (Art. 18, do Decreto 7.892/2013).

7.2.2. Serão considerados compatíveis com os de mercado os preços registrados que forem iguais ou inferiores à média daqueles apurados pelo setor demandante, na pesquisa de estimativa de preços.

7.2.3. Quando o preço de mercado se tornar superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá conforme preceitua o art. 19 do Decreto 7.892/2013:

1) Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados.

2) Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

7.2.4. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

CLÁUSULA OITAVA — DO PRAZO, LOCAL E DAS CONDIÇÕES DA ENTREGA E RECEBIMENTO

8.1. As licenças deverão ser entregues em forma digitais em e-mail coorporativo indicado pelo Gerente de Departamento de Tecnologia da Informação e Modernização Institucional ou Secretaria Municipal de Ciência, Tecnologia e Inovação ou Prefeitura Municipal de Rondonópolis.

8.2. Os Serviços de Suporte serão recebidos mediante apresentação de relatórios descrevendo os serviços, diagnósticos e resultados e a descrição de quantas UST (Unidade de Serviço Técnico) para cada etapa dos Serviços necessários para a execução dos Serviços.

8.3. PRAZO DE ENTREGA

8.3.1. O prazo de entrega dos equipamentos deverá ser de no máximo 30 (trinta) dias corridos após o recebimento da ordem de fornecimento.

8.3.2. O prazo para execução dos serviços contratados deverá ser contado a partir da emissão da ordem de serviço seguindo o cronograma.

8.4. CRONOGRAMA DE EXECUÇÃO

8.4.1. As atividades a serem desenvolvidas deverão ter como Referência o Cronograma de Execução mostrado abaixo:

Cronograma de execução												
Etapa	**Ação**	**Mês**										
		1º	**2º**	**3º**	**4º**	**5º**	**6º**	**7º**	**8º**	**9º**	**10º**	**11º**	**12º**
Entrega Equipamentos e Software	Recebimento do Console de Gerenciamento em Alta Disponibilidade contemplando Software e Hardware.	X											
Configuração	Utilização do Suporte para Console de Gerenciamento para	x	x	x	x	x	x	x	x	x	x	x	X

	instalação, configurações e capacitação técnica.												
Entrega do Software	Recebimento do Software Agentes de Proteção de dados estruturados multiplataforma.	X											
Configuração	Utilização do Suporte para Agentes de Proteção de dados Estruturados multiplataforma para levantamento, instalação, configuração e capacitação técnica.	x	x	x	x	x	x	x	x	x	x	x	x
Entrega do Software	Recebimento do Software Solução para transferência Segura de Base de Dados	X											
Configuração	Utilização do Suporte para Solução para transferência Segura de Base de Dados para configuração e capacitação técnica	x	x	x	x	x	x	x	x	x	x	x	X
Entrega do Software	Recebimento do Software Agentes de Proteção de Dados não estruturados multiplataforma	X											

Configuração	Utilização do Suporte para agentes de Proteção de Dados não estruturados multiplataforma para levantamento, instalação, configuração e capacitação técnica.	x	x	x	x	x	x	x	x	x	x	x	X
Entrega do Software	Recebimento do Software Proteção de Dados para Aplicação multiplataforma	X											
Entrega do Software	Recebimento do Software Agentes para Descoberta e Classificação de Dados	x	x	x	x	x	x	x	x	x	x	x	X
SERVIÇO	Geração de relatórios utilizando Consultoria para Avaliação periódica (HealthCheck) baseado a coleta de dados	X					x						
SERVIÇO	Análise de risco - SAR	x	x	x	x	x	x	x	x	x	x	x	X
SERVIÇO	Serviço de diagnóstico, avaliação, mapeamento e levantamento do parque tecnológico	X		x		x		x		x		x	

SERVIÇO	Gestão de projetos e geração de documentação	x	x	x	x	x	x	x	x	x	x	X	X
SERVIÇO	Serviço de suporte técnico especializdo (Help desk)	x		x		x		x		x		X	

8.5. GARANTIA

8.5.1. A garantia dos equipamentos deverá ser de 12 (Doze) meses on-site, no local e sem custo de deslocamento para assistência técnica.

CLÁUSULA NONA — DA SUBCONTRATAÇÃO.

9.1. NÃO SERÁ ADMITIDA A SUBCONTRATAÇÃO DO OBJETO.

CLÁUSULA DÉCIMA — DAS OBRIGAÇÕES DA CONTRATADA

10.1. Realizar os serviços de acordo com todas as exigências contidas no Termo de Referência

10.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços

10.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízos, de qualquer natureza, que causar à CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas

10.4. Atender às determinações e exigências formuladas pela CONTRATANTE

10.5. Responsabilizar-se, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, sociais, tributárias, trabalhistas e previdenciárias, ou quaisquer outras previstas na legislação em vigor, bem como por todos os gastos e encargos com material e mão de obra necessária à completa execução dos serviços:

10.5.1. Em caso de ajuizamento de ações trabalhistas contra a CONTRATADA, decorrentes da execução do presente Contrato, com a inclusão da CONTRATANTE como responsável subsidiário ou solidário, a CONTRATANTE poderá reter, das parcelas vincendas, o montante

dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

10.5.2. No caso da existência de débitos tributários ou previdenciários, decorrentes da execução do presente Contrato, que possam ensejar responsabilidade subsidiária ou solidária da CONTRATANTE, as parcelas vincendas poderão ser retidas até o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

10.5.3. As retenções previstas nas alíneas "a" e "b" poderão ser realizadas tão logo tenha ciência a CONTRATANTE da existência de ação trabalhista ou de débitos tributários e previdenciários e serão destinadas ao pagamento das respectivas obrigações caso o a CONTRATANTE seja compelida a tanto, administrativa ou judicialmente, não cabendo, em nenhuma hipótese, ressarcimento à CONTRATADA;

10.5.4. Eventuais retenções previstas nas alíneas "a" e "b" somente serão liberadas pela CONTRATANTE se houver justa causa devidamente fundamentada.

10.6. Manter as condições de habilitação e qualificação exigidas para a contratação durante todo prazo de execução contratual;

10.7. Responsabilizar-se, na forma do Contrato, pela qualidade dos serviços executados e dos recursos empregados, em conformidade com as especificações do Termo de Referência, sem ônus para a CONTRATANTE e sem prejuízo da aplicação das sanções cabíveis;

10.8. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;

10.9. Indicar, nas notas fiscais emitidas, quando o objeto envolver prestação de serviços, o efetivo período do mês que está sendo faturado.

CLÁUSULA DÉCIMA PRIMEIRA — DAS OBRIGAÇÕES DA CONTRATANTE

11.1. Oferecer todas as informações necessárias para que a licitante vencedora possa executar o objeto dentro das especificações.

11.2. Efetuar os pagamentos nas condições e prazos estipulados.

11.3. Acompanhar a execução e fiscalização dos serviços durante toda a vigência do Contrato de Prestação de Serviços.

11.4. Notificar, por escrito, o (a) contratado (a), a ocorrência de eventuais imperfeições no curso da execução dos serviços, determinando seu refazimento.

11.5. Acompanhar a execução dos serviços, podendo intervir durante a sua realização, para fins de ajuste ou suspensão; inclusive rejeitando, no todo ou em parte, os resultados atingidos.

CLÁUSULA DÉCIMA SEGUNDA— DO PAGAMENTO

12.1. O pagamento será efetuado em até 30 (trinta) dias após o recebimento e atestado da nota fiscal. A contratada deverá no ato de apresentação da nota fiscal, durante a vigência da ata de registro de preços, apresentar todas às certidões de regularidade (Municipal, Estadual, União, Trabalhista).

12.2. Caso constatado alguma irregularidade nas Notas Fiscais, estas serão devolvidas ao fornecedor, para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo para pagamento da data da sua reapresentação;

12.3. Nenhum pagamento isentará a CONTRATADA das suas responsabilidades e obrigações.

CLÁUSULA DÉCIMA TERCEIRA — DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS.

13.1. A Ata de Registro de Preços poderá ser cancelada de pleno direito, nas seguintes situações, conforme preceitua o art. 20 do Decreto 7.892/2013:

a) Quando o fornecedor descumprir as condições da ata de registro de preços;

b) Quando o fornecedor não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

c) Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou;

d) Sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da Lei nº 8.666, de 1993, ou no art. 7º da Lei nº 10.520, de 2002.

13.2. O cancelamento de registros nas hipóteses previstas nas alíneas a; b e d do **item anterior** será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa, conforme preceitua o art. 20, parágrafo único do Decreto 7.892/2013:

13.3. O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados, conforme preceitua o art. 21, parágrafo único do Decreto 7.892/2013:

a) Por razão de interesse público; ou

b) A pedido do fornecedor.

13.4. A Ata de Registro de Preços, decorrente desta licitação, será cancelada, automaticamente, por decurso do prazo de sua vigência.

13.5. A solicitação do Fornecedor para cancelamento dos preços registrados poderá não ser aceita pelo Órgão/Entidade, facultando-se a este neste caso, a aplicação das penalidades previstas em Edital.

13.6. Havendo o cancelamento do preço registrado, cessarão todas as atividades do fornecedor relativas ao fornecimento de itens, permanecendo mantido o compromisso da garantia e assistência técnica dos equipamentos entregues anteriormente ao cancelamento.

13.7. Caso a Prefeitura de Várzea Grande não se utilize da prerrogativa de cancelar a Ata de Registro de Preços, a seu exclusivo critério, poderá suspender a sua execução e/ou sustar o pagamento até que o Fornecedor cumpra integralmente a condição infringida.

13.8. Efetivando o Cancelamento da Ata de Registro de Preços será acionado os demais licitantes na ordem de classificação, conforme as condições expressas na Ata de Registro de preços e Edital.

CLÁUSULA DÉCIMA QUARTA — DAS INCIDÊNCIAS FISCAIS, ENCARGOS, ETC.

14.1. Correrão por conta exclusivas do FORNECEDOR:

a) Todos os impostos e taxas que forem devidos em decorrência das contratações do objeto deste Edital.

b) As contribuições devidas à Previdência Social, encargos trabalhistas, prêmios de seguro e de acidentes de trabalho emolumentos e outras despesas que se façam necessárias à execução da entrega dos materiais.

CLÁUSULA DÉCIMA QUINTA — DOS ILICITOS PENAIS E DAS PENALIDADES

15.1. Comete infração nos termos da Lei nº 12.486 de 2013 aqueles que cometerem atos lesivos à administração pública, assim definidos, no tocante a licitações e contratos, a Contratada que:

a) Frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

b) Impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

c) Afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) Fraudar licitação pública ou contrato dela decorrente;

e) Criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

f) Obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais;

g) Manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

15.2. Nos termos do art. 49 do Decreto 10.024/2019, ficará **impedido de licitar** e de contratar com a União e será descredenciado no Sicaf e do CRC instituído pelo Decreto Municipal nº 86/2018, pelo prazo de até cinco anos, sem prejuízo de multa de até 30% (trinta por cento) do valor estimado para a contratação e demais cominações legais, nos seguintes casos, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta aquele que:

I - Não assinar o contrato ou a ata de registro de preços;

II - Não entregar a documentação exigida no edital;

III - Apresentar documentação falsa;

IV - Causar o atraso na execução do objeto;

V - Não mantiver a proposta;

VI - Falhar na execução do contrato;

VII - Fraudar a execução do contrato;

VIII - Comportar-se de modo inidôneo;

IX - Declarar informações falsas; e

X - Cometer fraude fiscal.

15.3. As sanções descritas no item anterior também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública. (Art. 49, §1º, do Decreto 10.024/2019).

15.4. Pela inexecução total ou parcial do contrato a Administração poderá, garantida a prévia defesa, aplicar ao contratado as seguintes sanções: (Art. 87, da lei 8.666/93).

15.4.1. DA ADVERTÊNCIA (Art. 87, I da lei 8.666/93).

15.4.1.1. A aplicação da sanção administrativa de advertência pode ser efetuada nos seguintes casos:

a) Descumprimento das obrigações assumidas contratualmente ou na licitação, desde que não acarretem prejuízos para a CONTRATANTE, independentemente da aplicação de multa;

b) Execução insatisfatória ou inexecução dos fornecimentos e/ ou serviços ora contratados, desde que a sua gravidade não recomende o enquadramento nos casos de suspensão temporária ou inidoneidade;

c) Outras ocorrências que possam acarretar pequenos transtornos ao desenvolvimento dos serviços da CONTRATANTE, a seu critério, desde que não sejam passíveis de sanção mais grave;

d) Atraso na entrega do bem ou na prestação do serviço contratado, pelo prazo não superior a 05 (cinco) dias úteis.

15.4.2. DA MULTA (Art. 87, II, da lei 8.666/93).

15.4.2.1. Conforme disposto no **(Art. 86 da Lei 8.666/93)**, na forma prevista no instrumento convocatório ou no contrato; neste caso a Contratante aplicará a MULTA CONTRATUAL correspondente a:

a) 0,5% (cinco décimos por cento) por dia de atraso no prazo de entrega dos materiais ou serviços, calculados sobre o valor correspondente à parte inadimplida;

b) O atraso para efeito de cálculo, mencionado no item anterior será contado em dias corridos, a partir do 1° dia útil subsequente ao término do prazo ajustado em até 20 (vinte) dias;

c) 10% (dez por cento) sobre o valor constante no contrato, pela inexecução total do objeto, sem prejuízo das outras sanções cabíveis;

d) 15% (quinze por cento) sobre o valor da Ordem de Fornecimento/Empenho, pelo descumprimento de qualquer clausula contratual exceto prazo de entrega;

15.4.2.2. A adjudicada/Contratada não incorrerá em multa quando houver prorrogação do prazo, previamente autorizado pela CONTRATANTE, em decorrência de impedimentos efetivamente verificados sem que a ela seja imputável a culpa, ou em decorrência de acréscimos ou modificações no objeto inicialmente ajustado, respeitado o limite legal;

15.4.2.3. A multa será descontada dos créditos constantes da Fatura, ou outra forma de cobrança Administrativa ou Judicial;

15.4.2.4. Não será aplicada multa se, comprovadamente, o atraso da execução dos serviços ou fornecimento advir de caso fortuito ou motivo de força maior.

15.4.3. DA SUSPENSÃO TEMPORÁRIA DE PARTICIPAÇÃO EM LICITAÇÃO E IMPEDIMENTO DE CONTRATAR COM A ADMINISTRAÇÃO, POR PRAZO NÃO SUPERIOR A 02 (DOIS) ANOS. (Art. 87, III da lei 8.666/93).

15.4.3.1. A suspensão do direito de licitar e contratar com a Contratante pode ser aplicada aos

inadimplentes culposos que prejudicarem a execução do Contrato por fatos graves, cabendo defesa prévia, no prazo de 10 (dez) dias úteis da data do recebimento da respectiva intimação;

15.4.3.2. A sanção administrativa de suspensão temporária do direito de licitar e contratar com a Prefeitura poderá ser aplicada nos seguintes prazos e situações:

a) Por 06 (seis) meses nos seguintes casos:

I. Atraso no cumprimento das obrigações assumidas contratualmente, que tenham acarretado prejuízos para a CONTRATANTE;

II. Execução insatisfatória dos fornecimentos e/ ou serviços contratados;

b) Por 02 (dois) anos, nos seguintes casos:

I. Não concluir os fornecimentos e/ ou os serviços contratados;

II. Se recusar a fornecer informações suficientes ou fornecê-las inadequadamente, no que diz respeito à sua fruição, qualidade e riscos de operacionalização;

III. Prestar o serviço em desacordo com as normas aplicáveis à execução do objeto deste ajuste;

IV. Cometer quaisquer outras irregularidades que acarretem prejuízo ao órgão licitador, ensejando a rescisão do contrato.

15.4.4. DA DECLARAÇÃO DE INIDONEIDADE PARA LICITAR OU CONTRATAR COM A ADMINISTRAÇÃO PÚBLICA (Art. 87, IV da lei 8.666/93).

15.4.4.1. Enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo do sansão aplicado com base no inciso anterior.

15.4.4.2. A declaração de inidoneidade para licitar ou contratar com toda a Administração Pública será proposta pela Seção Administrativa e Financeira para aplicação à ADJUDICADA/CONTRATADA nos casos a seguir indicados:

a) Condenação definitiva por praticar, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) Prática de atos ilícitos, visando frustrar a execução do contrato;

15.4.4.3. Demonstração de não possuir idoneidade para licitar e contratar com o órgão contratante, em virtude de atos ilícitos praticados, tais como:

a) Praticar ação maliciosa e premeditada em prejuízo da Contratante ou ações que evidenciem interesses escusos ou má-fé;

b) Apresentar qualquer documento falso ou falsificado, no todo ou em parte;

c) Reproduzir, divulgar ou utilizar, em benefício próprio ou de terceiros, quaisquer informações de que tenha tomado conhecimento em razão da execução dos serviços objeto deste contrato sem o consentimento da Contratante, por escrito.

Parágrafo Primeiro - Independentemente das sanções administrativas previstas neste Edital, a Contratada está sujeita ao pagamento de indenização por perdas e danos, quando a inadimplência acarretar prejuízos ao órgão contratante;

Parágrafo Segundo - Nenhuma sanção será aplicada sem o devido processo administrativo, que prevê defesa prévia do interessado e recurso dos prazos definidos em lei, sendo-lhe franqueada vista ao processo.

15.5. As sanções serão registradas e publicadas no Sicaf e no CRC instituído pelo Decreto Municipal nº 86/2018. (Art. 49, §1º, do Decreto 10.024/2019).

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

CLÁUSULA DÉCIMA SEXTA — DOS RECURSOS ORÇAMENTÁRIOS.

16.1. As despesas decorrentes da presente Ata correrão a conta dos recursos Próprios nas seguintes dotações orçamentária:

SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO

FONTE	PROJETO ATIVIDADE	ELEMENTO DESPESA	CODIGO REDUZIDO
01500	2295	3.3.90.40	04010033

CLÁUSULA DÉCIMA SÉTIMA — DO ACOMPANHAMENTO E DA FISCALIZAÇÃO.

17.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a prestação dos serviços, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

17.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº. 8.666, de 1993.

17.3. O representante da Secretaria anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

17.4. A fiscalização da futura Ata de Registro de Preços e do Contrato dela decorrente ficará a cargo dos servidores:

17.4.1. A SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO que designa neste ato fiscal, o servidor **JOSÉ ABREU DE LUCENA JUNIOR**, portador da Cédula de Identidade RG nº 1280647-1 SSP/MT, CPF nº 905.852.161-34, matrícula nº144036, domiciliado na Rua I, Qda. 07, Lote 20, Bairro Santa Izabel, Várzea Grande/MT, e Fiscal Suplente o servidor Lucas Scheid dos Santos, inscrita no CPF sob o nº034.283.091-03, matricula nº143931, Residente Veneza 07, Bairro Costa Verde, Várzea Grande/MT.

CLÁUSULA DÉCIMA OITAVA — DAS DISPOSIÇÕES FINAIS.

18.1. As partes ficam, ainda, adstritas as seguintes disposições:

a) Todas as alterações que fizerem necessárias serão registradas por intermédio da lavratura de termo aditivo.

b) Integra está ata o disposto no **PREGÃO ELETRÔNICO Nº. 62/2023**, conforme descrito no edital e seus anexos e as propostas da contratada de cada item.

c) É vedado caucionar ou utilizar o contrato para qualquer operação financeira, sem previa e expressa autorização da Prefeitura Municipal de Várzea Grande.

18.2. É vedado caucionar ou utilizar a ata decorrente do registro de preços para qualquer operação financeira sem a prévia e expressa autorização da Secretaria de Administração.

18.3. O presente Edital e seus Anexos, bem como a proposta do licitante vencedor deste certame, farão parte integrante da Ata de Registro de Preços, Contrato ou Instrumento equivalente, independente de transcrição.

Várzea Grande/MT, 01 de março de 2024.

Prefeitura Municipal de Várzea Grande:

OSVALDO BOTELHO DE CAMPOS DE NETO
Secretaria Municipal de Administração

Empresa:

Assinado de forma digital por HERMANN DRUMMOND JUNIOR:82063605149
Dados: 2024.03.01 11:50:34 -04'00'

DEK SOLUCOES EM T.I. LTDA
CNPJ 21.191.387/0001-80

EXTRATO DA ATA DE REGISTRO DE PREÇO DO PREGÃO ELETRÔNICO Nº. 62/2023

Processo nº 936410/2023- Objeto: Registro de preço para eventual contratação de solução de segurança da informação para proteção inteligente de dados em repouso, estruturados e não estruturados, controle de acesso, visibilidade e rastreabilidade de utilização de dados em servidores de arquivos, banco de dados, custódia de chaves criptográficas composta por softwares e serviços de garantia e suporte técnico, serviços de instalação e configuração da solução, serviços de treinamento, serviços para integrações necessárias com soluções de terceiros e serviços especializados para atender às demandas da Prefeitura Municipal de Várzea Grande.

ATA DE REGISTRO DE PREÇOS N.º 48/2024

Empresa: DECK SOLUÇÕES EM T.I. LTDA - CNPJ n.º 21.191.387/0001-80

ITEM	CÓD TCE	DESCRIÇÃO DO PRODUTO	UND	QUANT	VALOR UNITÁRIO	VALOR TOTAL
01	422472-8	APPLIANCE DE GERENCIAMENTO DE SOLUÇÃO DE SEGURANÇA DE DADOS COM SERVIÇO DE SUPORTE	UND	01	R$ 976. 956,50	R$ 976. 956,50
02	00055997	MÓDULO DE SEGURANÇA DE DADOS NÃO ESTRUTURADOS MULTIPLATAFORMA COM SERVIÇO DE SUPORTE	UND	01	R$ 141. 352,30	R$ 141. 352,30
03	00055997	MÓDULO DE SEGURANÇA DE DADOS ESTRUTURADOS MULTIPLATAFORMA COM SERVIÇO DE SUPORTE	UND	02	R$ 143. 927,00	R$ 143. 927,00
04	00055997	MÓDULO PARA TRANSFERÊNCIA SEGURA DE BASE DE DADOS COM SERVIÇO DE SUPORTE	UND	01	R$ 727. 841,30	R$ 727. 841,30
05	00069841	MÓDULO DE SEGURANÇA PARA APLICAÇÕES WEB COM SERVIÇO DE SUPORTE	UND	01	R$ 196. 317,30	R$ 196. 317,30
06	00069841	MÓDULO DE GESTÃO DE CHAVES LOCAL COM SERVIÇO DE SUPORTE	UND	01	R$ 12. 554,80	R$ 12. 554,80
07	00069841	MÓDULO DE VALIDAÇÃO DE CONTROLE DE SEGURANÇA CONTRA AMEAÇAS DE REDE, ENDPOINT, APLICAÇÃO WEB, E-MAIL E VAZAMENTO DE DADOS COM SERVIÇO DE SUPORTE	UND	01	R$ 626. 823,70	R$ 626. 823,70
08	439506-9	SERVIÇO DE TREINAMENTO	UND	02	R$ 28. 604,40	R$ 28. 604,40
09	231423-1	SERVIÇO DE IMPLEMENTAÇÃO DE CONSOLE DE GERENCIAMENTO DE CHAVES DE CRIPTOGRAFIA.	UND	01	R$ 24. 112,50	R$ 24. 112,50
10	231423-1	SERVIÇO SOB DEMANDA PARA IMPLEMENTAÇÃO DE AGENTES DE CRIPTOGRAFIA.	UND	3000	R$ 360,80	R$ 360,80
11	375385-9	SERVIÇO DE CONSULTORIA PARA AVALIAÇÃO PERIÓDICA (HEALTHCHECK)	UND	02	R$ 113. 466,70	R$ 113. 466,70
12	324820-8	SERVIÇO DE ANÁLISE DE RISCO - 12 MESES	UND	12	R$ 25. 544,60	R$ 25. 544,60
13	375385-9	SERVIÇO DE DIAGNÓSTICO, AVALIAÇÃO, MAPEAMENTO E LEVANTAMENTO DO PARQUE TECNOLÓGICO	UND	06	R$ 10. 920,50	R$ 10. 920,50
14	354661-6	SERVIÇO DE GESTÃO DE PROJETOS E DOCUMENTAÇÃO - 12 MESES	UND	12	R$ 25. 782,30	R$ 25. 782,30
15	278817-9	SERVIÇO DE SUPORTE TÉCNICO ESPECIALIZADO (HELPDESK) – 12 MESES	UND	06	R$ 16. 366,60	R$ 16. 366,60
Valor Total do Lote: R$ 5.140.000,00 (cinco milhões, cento e quarenta mil)						

12 (doze) meses Várzea Grande/MT, 11 de março de 2024.

PREFEITURA MUNICIPAL DE VÁRZEA GRANDE

Órgão Registrante

Osvaldo Botelho de Campos Neto
Secretário Municipal de Administração

ATO Nº 114/2024

KALIL SARAT BARACAT DE ARRUDA, Prefeito Municipal do Município de Várzea Grande, Estado de Mato Grosso, no uso das atribuições legais e na conformidade com as disposições do artigo 69, inciso VI, da Lei Orgânica Municipal e;

R E S O L V E:

EXONERAR Maria Clara Morales da Cunha, do cargo em Comissão de Gerente DNS 6, da Secretaria Municipal de Administração, a partir de 29 de fevereiro de 2024.

Registra-se, Publica-se, Cumpra-se.

Paço Municipal "Couto Magalhães", Praça dos Três Poderes, em Várzea Grande, 11 de março de 2024.

Kalil Sarat Baracat de Arruda

Prefeito Municipal

SECRETARIA DE GESTÃO FAZENDÁRIA

COORDENADORIA DE FISCALIZAÇÃO

AIIM - NOTIFICAÇÃO DE AUTO DE INFRAÇÃO DE IMPOSIÇÃO DE MULTA

Intima o(s) sujeito(s) passivo(s) que menciona para comparecimento no local citado para tratar de assunto do seu interesse.

A Administração Tributária Municipal responsável pelo ISSQN, nos termos do artigo 242, da Lei nº1.178/1991, **INTIMA** o[s] sujeito[s] passivo[s] abaixo relacionado [s], a comparecer[em], em dia útil, no horário normal de atendimento, à sede da administração tributária deste município para tomar ciência da[s] **Notificação[ões] do(s) AIIM** a seguir identificado[s].

Em caso de não comparecimento do sujeito passivo ou seu representante legal, considerar-se-á feita a intimação e cientificado pelo destinatário, nos termos artigo 323, **III**, c/c artigo 322, **III**, da Lei nº1.178/1991.