CONTRATO Nº 125 /2021/SCCC/ALMT

CONTRATO QUE ENTRE SI CELEBRAM A ASSEMBLEIA LEGISLATIVA DO ESTADO DE MATO GROSSO, ATRAVÉS DA MESA DIRETORA E A EMPRESA DEK SOLUÇÕES EM T.I. LTDA.

A ASSEMBLEIA LEGISLATIVA DO ESTADO DE MATO GROSSO, doravante denominada **CONTRATANTE**, com sede no Centro Político Administrativo - Cuiabá-MT, inscrita no CNPJ sob nº 03.929.049/0001-11, na Avenida André Antônio Maggi, Lote 06, Setor A, Centro Político Administrativo - CPA, Edifício Governador Dante Martins de Oliveira, Cuiabá – MT., CEP 78049-901, Cuiabá – MT neste ato representado pelo Senhor Presidente Deputado Max Russi e o Primeiro Secretário, Ordenador de Despesas – Deputado Eduardo Botelho, e de outro lado à Empresa **DEK SOLUÇÕES EM T.I. LTDA**, no CNPJ nº. 21.191.387/0001-80, com sede na Rua das Caviúnas, nº. 377, sala 01, térreo Bairro Loteamento Alphaville Cuiabá, Cuiabá/MT, CEP:78.061-302, telefone: (65) 2127-6030 / 99309-9889, e-mail: hermann@servdigital.com.br, neste ato representada pelo Senhor **Hermann Drummond Junior**, portador do RG nº 5.997.777 SSP/MG e CPF nº. 820.636.051-49, doravante denominada **CONTRATADA,** considerando o que consta no Processo Licitatório Pregão Eletrônico Registro de Preços nº 035/2021/ALMT Protocolo SGED. nº. 2021/7452-8) e sujeitando-se, ainda, às normas da Lei nº 8.666, de 21 de junho de 1993 e suas alterações, e a Lei Complementar Federal nº 101, de 04 de maio de 2.000, demais normas que regem a espécie, RESOLVEM celebrar o presente contrato, nos seguintes termos e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente contrato tem por objeto a contratação de empresa especializada no fornecimento de solução de segurança da informação para proteção inteligente de dados em repouso e dados em trânsito, estruturados e não estruturados, controle de acesso, visibilidade e rastreabilidade de utilização de dados em servidores de arquivos, banco de dados *on premise* e na nuvem, custódia de chaves criptográficas para ambientes em nuvem (pública, hibrida ou privada) composta por software 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 as demandas da Assembleia Legislativa do Estado de Mato Grosso, conforme especificações do Termo de Referência nº 010/2021/STI, constante no Processo Licitatório Pregão Eletrônico Registro de Preços nº. 035/2021/ALMT – SGED. nº. 2021/7452-8, e Ata de Registro de Preços nº. 83/2021.

CLÁUSULA SEGUNDA – DA DESCRIÇÃO DA SOLUÇÃO, ESPECIFICAÇÕES TÉCNICAS, QUANTIDADES E PREÇOS PRATICADOS

2.1. A descrição das soluções, especificações técnicas, quantidade e preços estão descritos na planilha abaixo:

LOTE ÚNICO						
Item	**Descrição da Solução**	**Métrica**	**Unid**	**Quant**	**Valor Unitário (R$)**	**Valor Total Anual**
1	Console de Gerenciamento em Alta Disponibilidade.	Hardware	Unid	2	R$669.267,35	R$1.338.534,70
2	Suporte para Console de Gerenciamento – 12 meses	Serviço	Unid	12	R$23.400,00	R$280.800,00
3	Agentes de Proteção de dados estruturados multiplataforma	Software	Unid	3	R$95.000,00	R$285.000,00
4	Suporte para Agentes de Proteção de dados Estruturados multiplataforma – 12 meses	Serviço	Unid	12	R$5.150,00	R$61.800,00
5	Solução para transferência Segura de Base de Dados	Software	Unid	2	R$555.000,00	R$1.110.000,00

6	Suporte para Solução para transferência Segura de Base de Dados– 12 Meses	Serviço	Unid	12	R$46.435,35	R$557.224,20
7	Agentes de Proteção de Dados não estruturados multiplataforma	Software	Unid	10	R$83.450,00	R$834.500,00
8	Suporte para agentes de Proteção de Dados não estruturados multiplataforma	Serviço	Unid	10	R$20.500,00	R$205.000,00
9	Agentes de Proteção de Dados para Aplicação multiplataforma	Software	Unid	5	R$115.870,38	R$579.351,90
10	Suporte para Agentes de Proteção de Dados para Aplicação multiplataforma – 12 meses	Serviço	Unid	5	R$34.110,00	R$170.550,00
11	Agentes para proteção e custodia de chaves multicloud– Termo de Licenciamento por 12 meses	Software	Unid	2	R$342.000,00	R$684.000,00
12	Agentes para Gestão de Chaves Local	Software	Unid	10	R$38.481,95	R$384.819,50
13	Suporte para Agentes para Gestão de Chaves Local – 12 meses	Serviço	Unid	12	R$9.425,50	R$113.106,00
14	Agentes para Descoberta e Classificação de Dados – Termo de Licenciamento por 12 meses – 50TB	Software	Unid	1	R$487.000,00	R$487.000,00
15	Serviços de Implementação de Console de Gerenciamento	Serviço	Unid	2	R$21.500,00	R$43.000,00
16	Serviços sob demanda para Implementação de Agentes	Serviço	UST	3000	R$248,00	R$744.000,00
17	Serviços de Treinamento	Serviço	Unid	10	R$20.000,00	R$200.000,00
18	Consultoria para Avaliação periódica (HealthCheck)	Serviço	Unid	6	R$66.421,07	R$398.526,42
19	Consultoria sob demanda para emissão de relatórios de conformidade com a LGPD	Serviço	Unid	6	R$71.740,30	R$430.441,80
Valor Total: R$ 8.907.654,52 (oito milhões, novecentos e sete mil, seiscentos e cinquenta e quatro reais e cinquenta e dois centavos).						

2.3. O valor global do presente contrato é de **R$ 8.907.654,52 (oito milhões, novecentos e sete mil, seiscentos e cinquenta e quatro reais e cinquenta e dois centavos).**

CLÁUSULA TERCEIRA – DOS RECURSOS ORÇAMENTÁRIOS

3.1. As despesas decorrentes do presente Contrato correrão pela dotação orçamentária – Exercício de 2021 da Assembleia Legislativa do Estado de Mato Grosso, a seguir:

	Número	Histórico
Projeto/Atividade	2.009	Manutenção de Ações de Informática
Elemento de Despesa	3.3.90.39.00.00	Outros Serviços de Terceiros – Pessoa Jurídica

CLÁUSULA QUARTA – DOS PRAZOS DE VIGÊNCIA E EXECUÇÃO

4.1. O prazo de vigência do contrato será de 12 (doze) meses.

4.1.2. Os itens 2, 4, 6, 8, 10, 13, 15, 16, 17, 18 e 19, tratam-se de prestação de serviço, e portanto, pode ser prorrogável se conveniente para a **CONTRATANTE**, conforme preceitua o art. 57, inciso II da lei nº 8.666/93. Trata-se de serviço continuado e a sua interrupção poderia comprometer a execução das atividades finalísticas da **CONTRATANTE**.

4.1.3. Os itens 1, 3, 5, 7, 9, 11, 12 e 14 tratam-se de equipamento e licenças, e portanto, não são prorrogáveis.

4.2. Caso as partes não se interessem pela prorrogação deste contrato, quanto aos itens descritos no item 4.1.2, deverão manifestar sua vontade, no mínimo, 90 (noventa) dias antes do término da vigência contratual.

4.3. Quando consultada, a manifestação positiva da **CONTRATADA** quanto ao interesse na prorrogação da vigência do contrato, nos termos do art. 422 do Código Civil, gera legítima expectativa para a **CONTRATANTE** quanto à assinatura do termo aditivo necessário à formalização da renovação da vigência.

4.4. Em atenção ao item anterior, exceto diante de fato superveniente e devidamente justificável, a recusa da **CONTRATADA** em assinar o termo aditivo de prorrogação de

vigência manifestada após o prazo de 90 (noventa) dias antes do encerramento da vigência do contrato poderá ensejar:

4.4.1. A aplicação de multa de 5% (cinco por cento) a 10% (dez por cento) sobre o valor global do contrato; II - conforme o interesse da Administração, a rescisão unilateral do contrato, de modo a, diante da impossibilidade prática de realização de novo procedimento licitatório, viabilizar a contratação do objeto remanescente do contrato nos termos do art. 24, XI, da Lei n° 8.666/1993.

4.4.2. Toda prorrogação de prazo deverá ser justificada por escrito e previamente autorizada pela autoridade competente.

CLÁUSULA QUINTA – DO LOCAL DA EXECUÇÃO DOS SERVIÇOS E DOS CRITÉRIOS DE ACEITAÇÃO DOS PRODUTOS E SERVIÇOS

5.1. O objeto deste Contrato será entregue na Secretaria de Tecnologia da Informação – Edifício Dante Martins de Oliveira, Piso Térreo, Avenida André Antônio Maggi, Lote 06, Setor A, CPA, CEP 78049-901 – Cuiabá, Mato Grosso, Brasil, das 08h00min às 12h00min e das 14h00min às 18h00min, de segunda à sexta-feira, com "pré-agendamento" pelo telefone (65) 3313-6459.

5.2. Nos termos dos artigos 73 a 76 da Lei 8.666/1993, o objeto do presente TERMO DE REFERÊNCIA será recebido:

5.2.1. Provisoriamente, pela Secretaria de Tecnologia da Informação, no ato da entrega, para posterior verificação da conformidade dos produtos e/ou serviços com as especificações;

5.2.2. Se for constatada desconformidade do(s) produtos e serviços apresentado(s) em relação às especificações, a **CONTRATADA** deverá efetuar a troca ou correção, no prazo estabelecido neste Contrato, a contar do recebimento da solicitação.

5.2.3. Neste caso, o recebimento do(s) produto(s) e/ou serviços escoimado(s) dos vícios que deram causa a sua troca será considerado recebimento provisório, ensejando nova contagem de prazo para o recebimento definitivo.

5.2.4. Definitivamente, no prazo de 30 (trinta) dias, contados do recebimento provisório, após criteriosa inspeção e verificação e análise por Comissão de Recebimento, a ser designada, de que os bens ou serviços a serem adquiridos encontram-se em perfeitas condições de utilização, além de atenderem às especificações do objeto contratado.

5.3. O aceite/aprovação do(s) produto(s) ou serviço(s) pela **CONTRATANTE** não

exclui a responsabilidade civil da **CONTRATADA** por vícios de quantidade ou qualidade do(s) produto(s) ou disparidades com as especificações estabelecidas, verificadas, posteriormente, garantindo-se a **CONTRATANTE** as faculdades previstas no art. 18 da Lei n.º 8.078/90.

5.4. A inspeção pode gerar a recusa de artefatos por motivo de vícios de qualidade ou por não observância dos padrões adotados pela STI.

CLÁUSULA SEXTA – DOS REQUISITOS FUNCIONAIS DA SOLUÇÃO

6.1. CONSOLE DE GERENCIAMENTO – ITEM 01:

6.1.1. A solução deverá prover um console de gerenciamento composta por um conjunto integrado de produtos baseados em uma infraestrutura comum e extensível, com gerenciamento centralizado de políticas e de chaves, reduzindo o esforço de administração e o custo total de propriedade.

6.1.2. O Console de Gerenciamento deve oferecer recursos para proteger e controlar o acesso a dados estruturados e não estruturados hospedados em ambientes físicos e virtuais, ON PREMISES e na NUVEM.

6.1.3. A solução deve prover um console único que permita o gerenciamento centralizado de todos os agentes de criptografia, suas chaves de criptografia, políticas de configuração, publicação e controle de acesso dos dados a serem protegidos.

6.1.4. O console deve possuir certificação FIPS 140-2, Common Criteria, ou outra equivalente, para garantir total segurança das chaves de criptografia.

6.1.5. O console de gerenciamento centralizado deve suportar agentes para as funcionalidades que seguem:

6.1.5.1. 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;

6.1.5.2. Integração com SIEM–suportar integração com os sistemas de gerenciamento de logs do mercado, como: Splunk, qRadar, Arcsight, McAfee, LogRhythm e etc;

6.1.5.3. Segurança de container - oferecer criptografia de dados, controle de acesso e registro de acesso ao dado;

6.1.5.4. 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);

6.1.5.5. Toquenização e mascaramento de dados - reduzir os custos e o esforço necessários para cumprir com as políticas de segurança e normas regulatórias como o LGPD, dentre outras;

6.1.5.6. Criptografia para aplicações – simplificar o processo de adição de criptografia em aplicações, por meio de Ais baseadas em padrões que potencializem operações criptográficas e de gerenciamento de chaves de alto desempenho.

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

6.1.7. Apoiar a incorporação de vários consoles adicionais para fins de configuração de esquemas de tolerância a falhas multinível.

6.1.8. Os agentes instalados nos servidores devem operar de forma autônoma não causando impacto em caso de perda de comunicação com o console.

6.1.9. Os agentes devem fazer a rotação/mudança de chaves "a quente", ou seja, sem indisponibilidade nos servidores de dados.

6.1.10. Cada console deve ter a capacidade de suportar o crescimento.

6.1.11. 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 em um dispositivo virtual dedicado aos serviços de segurança dentro do console.

6.1.12. É desejável que todos os elementos da solução sejam do mesmo fabricante, porém serão aceitas soluções compostas por mais de um fabricante desde que estes fabricantes comprovem interoperabilidade e suporte a solução ofertada.

6.1.13. O console deve possuir capacidade de gerenciar chaves criptográficas padrão KMIP.

6.1.14. Deve ser compatível com API PKCS # 11 e Microsoft Key Extensible Management.

6.1.15. 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, ARIA128 e ARIA256) e assimétrica (algoritmos RSA1024, RSA2048, RSA4096).

6.1.16. 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.

6.1.17. 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.

6.1.18. O console deve possibilitar gerenciamento via interface Web, possibilitar comandos (CLI) e API (SOAP, REST).

6.1.19. Deve requerer autenticação de usuário e senha e, opcionalmente, dois fatores RSA.

6.1.20. Deve ser capaz de configurar cópias de backup de suas configurações automaticamente ou manualmente.

6.1.21. Requerimentos complementares:

6.1.21.1. Suportar usuários múltiplos;

6.1.21.2. Escalabilidade comprovada para mais de 10.000 agentes;

6.1.21.3. Cluster para alta disponibilidade (HA);

6.1.21.4. Toolkit e interface de programação;

6.1.21.5. Integração infraestrutura de autenticação existente, com fácil configuração;

6.1.21.6. Suporte para API RESTfull;

6.1.21.7. Autenticação multi-fator;

6.1.21.8. Opções de instalação:

6.1.21.8.1. Sistema virtual com certificação FIPS 140-2 Nível, ou certificação compatível;

6.1.21.8.2. O sistema virtual deve ser compatível com VMware ou Hyper-V

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

6.2. AGENTES DE PROTEÇÃO DE DADOS ESTRUTURADOS MULTIPLATAFORMA – ITEM 03:

6.2.1. Este agente 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 agente 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.

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

6.2.3. Esses agentes devem oferecer suporte a sistemas operacionais Microsoft, e/ou Linux.

6.2.4. Eles devem ser compatíveis com bancos de dados estruturados e não estruturados, incluindo MS-SQL Server, MySQL.

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

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

6.2.7. 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%.

6.2.8. 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, etc.).

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

6.2.10. 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.

6.2.11. Essas diretivas devem permitir e serem baseadas em usuário, processo, tipo de arquivo e agendamento.

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

6.2.13. 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.

6.2.14. 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.

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

6.2.16. 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.

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

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

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

6.2.20. Requerimentos complementares:

6.2.20.1. Compatibilidade com os sistemas operacionais:

- Windows Server: 2008, 2012 e 2016.
- Windows: 7; 8,1 e 10.
- Linux: RedHat 6.7-6.10; CentOS 6.7-6.10, Red Hat 7.0-7.6, Ubuntu e Debian.

6.2.20.2. Permitir criptografia para múltiplos fabricantes de banco de dados, tais como:

- MySQL (Windows, Linux);
- MS SQL (Windows).

6.3. SOLUÇÃO PARA TRANSFERÊNCIA SEGURA DE BASE DE DADOS – ITEM 05:

6.3.1. A Este agente 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.

6.3.2. 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.

6.3.3. A solução de ser customizável e de alta performance.

6.3.4. A solução deve suportar, pelo menos, as operações de criptografia / toquenização e descriptografia / detoquenização de tabelas e / ou colunas.

6.3.5. 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.

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

6.3.7. 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.

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

6.4. AGENTES DE PROTEÇÃO DE DADOS NÃO ESTRUTURADOS MULTIPLATAFORMA – ITEM 07:

6.4.1. Este agente deve fornecer criptografia de servidor de arquivo (dado não estruturado) 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 agente 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.

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

6.4.3. Os agentes devem oferecer suporte a sistemas operacionais Microsoft e/ou Linux.

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

6.4.5. Sua implementação não deve exigir qualquer alteração no servidor de arquivo ou processo para manuseio do dado pelo usuário final.

6.4.6. 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.).

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

6.4.8. 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.

6.4.9. Essas diretivas devem permitir serem baseadas em usuário, processo, tipo de arquivo e agendamento.

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

6.4.11. 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.

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

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

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

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

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

6.4.17. Compatibilidade com os sistemas operacionais:

- Windows Server: 2008, 2012 e 2016.

- Windows: 7; 8,1 e 10.
- Linux: RedHat 6.7-6.10; CentOS 6.7-6.10, Red Hat 7.0-7.6, Ubuntu e Debian.

6.5. AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO MULTIPLATAFORMA – ITEM 09:

6.5.1. Este agente deve permitir a toquenização vaultless com o Dynamic Data Masking, para eficientemente Anonimizar dados, incluindo dados pessoais, quer eles residem onpremises, 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.

6.5.2. Possuir alto desempenho com baixo impacto na performance da aplicação.

6.5.3. Possuir servidores de token virtual escalável.

6.5.4. Comunicação via TLS autenticado mutuamente.

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

6.5.6. Permitir geração de Tokens Aleatórios.

6.5.7. Compatível com FPE FF1, Tokens FF3.

6.5.8. Permitir Mascaramento Dinâmico ou Estático de Dados.

6.5.9. Gerenciamento de chaves e políticas.

6.5.10. Suporte AD / LDAP.

6.5.11. Suporte a dados numéricos e alfanuméricos.

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

6.5.13. 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.

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

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

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

6.5.16. Proteger dados em trânsito e em repouso.

6.5.17. Mascarar os dados em ambiente de desenvolvimento, teste e terceirizados com acesso ao banco de dados.

6.5.18. 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.

6.6. AGENTES PARA PROTEÇÃO E CUSTODIA DE CHAVES MULTICLOUD – ITEM 11:

6.6.1. A Este agente deve prover o controle de chave pelo próprio cliente permitindo a separação, criação, propriedade, controle e revogação das chaves de criptografia sem a dependência do provedor. Deverá reduzir a complexidade do gerenciamento de chaves, dando ao próprio cliente controle de ciclo de vida de chaves de criptografia com gerenciamento centralizado, visibilidade e rastreabilidade.

6.6.2. Deverá cumprir com os regulamentos de proteção de dados e armazenamento de chaves rigorosos podendo chegar a FIPS 140-2 Nível 3, ou certificação equivalente.

6.6.3. Prover eficiência com gerenciamento de chave centralizado em ambientes de nuvem híbrida.

6.6.4. Fornecer acesso a cada provedor de nuvem a partir de uma única janela do navegador, incluindo várias contas ou assinaturas.

6.6.5. Rotacionar de forma automática as chaves para cumprir com regulamentações que exigem este serviço de rotação de chave.

6.6.6. Fornecer mecanismos simples, via login federado, para conceder acesso aos dados. Com isso, ser compatível com logins de serviços em nuvem que são autenticados e autorizados pelo provedor de serviços, isto é, nenhum banco de dados de login nem configuração AD ou LDAP é necessário.

6.6.7. Fornecer meios para solicitar a criação de chaves nos provedores de nuvem e fornecer gerenciamento completo do ciclo de vida das mesmas.

6.6.8. Controlar e gerenciar centralizadamente várias nuvens, IaaS e SaaS (Multicloud).

6.6.9. Prover registro (log), rastreabilidade e relatórios de conformidade totalmente

independente do provedor de nuvem.

6.6.10. O agente deve suportar, pelo menos, os provedores de nuvem que seguem:

6.6.10.1. Microsoft Azure;

6.6.10.2. Microsoft Office365;

6.6.10.3. Amazon Web Services.

6.7. AGENTES PARA GESTÃO DE CHAVE LOCAL – ITEM 12:

6.7.1. Ser capaz de centralizar o gerenciamento de chaves de aplicativos de terceiros que usam criptografia nativa, tal como bancos de dados.

6.7.2. 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.

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

6.7.4. Elevar o nível de segurança pela separação das chaves de criptografia das aplicações, banco de dados, storage e etc.

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

6.7.6. 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.

6.7.7. Garantir a custódia de chaves para, pelo menos:

6.7.7.1. A Oracle TDE;

6.7.7.2. SQL TDE;

6.7.7.3. Nutanix;

6.7.7.4. VMWare;

6.7.7.5. Cisco;

6.7.7.6. Netapp;

6.7.7.7. Certificados;

6.7.7.8. Aplicações desenvolvidas em casa;

6.7.7.9. Outros volumes compatíveis.

6.8. AGENTES PARA DESCOBERTA E CLASSIFICAÇÃO DE DADOS – ITEM 14:

6.8.1. A solução deverá possibilitar a descoberta de dados, em ambiente de dados estruturados e não estruturados, armazenados em diferentes repositórios, tais como:

6.8.1.1. Servidores de Arquivos;

6.8.1.2. Bancos de Dados;

6.8.1.3. Estações de trabalho.

6.8.2. A solução deve permitir, através de interface única, realizar o levantamento e entendimento dos dados existentes, sua localização e riscos associados, permitindo:

6.8.2.1. Atender aos requisitos de privacidade;

6.8.2.2. Obter visibilidade sobre os dados que estão em risco de exposição;

6.8.2.3. Suportar a criação de plano de privacidade e proteção de dados.

6.8.3. A solução ofertada deverá possibilitar, pelo menos, quatro níveis de classificação de dados por padrão:

6.8.3.1. Restrito;

6.8.3.2. Privado;

6.8.3.3. Interno;

6.8.3.4. Público.

6.8.4. A solução deve atribuir pontuações de risco que permitam identificar o nível de sensibilidade dos dados, como arquivos e bancos de dados, agregando os seguintes parâmetros:

6.8.4.1. Nível de proteção;

6.8.4.2. Quantidade de elementos encontrados;

6.8.4.3. Localização;

6.8.4.4. Quantidade de dados confidenciais.

6.8.5. As pontuações de risco devem permitir identificar os dados com maior exposição e permitir priorizar medidas de proteção.

6.8.6. A solução deve suportar os seguintes ambientes:

6.8.6.1. Armazenamento local em Hard Disk e Memória dos computadores;

6.8.6.2. Armazenamentos em rede;

6.8.6.3. Compartilhamento Windows CIS e SMB;

6.8.6.4. Network File System NFS;

6.8.6.5. Bancos de Dados:

6.8.6.6. SQL.

6.8.7. A solução deve suportar os seguintes tipos de arquivos:

6.8.7.1. Banco de Dados:

6.8.7.1.1. Access;

6.8.7.1.2. Dbase;

6.8.7.1.3. SQLite;

6.8.7.1.4. MSSQL MDF & LDF.

6.8.7.2. Arquivos de Imagens:

6.8.7.2.1. BMP;

6.8.7.2.2. FAX;

6.8.7.2.3. GIF;

6.8.7.2.4. JPG;

6.8.7.2.5. PDF;

6.8.7.2.6. PNG;

6.8.7.2.7. TIF.

6.8.7.3. Arquivos Compactados:

6.8.7.3.1. bzip2;

6.8.7.3.2. Gzip (todos os tipos);

6.8.7.3.3. TAR;

6.8.7.3.4. Zip (todos os tipos).

6.8.7.4. Microsoft Backup:

6.8.7.4.1. Microsoft Binary / BKF.

6.8.7.5. Microsoft Office: v5, 6, 95, 97, 2000, XP, 2003 e superiores.

6.8.7.6. Open Source:

6.8.7.6.1. Star Office;

6.8.7.6.2. Open Office.

6.8.7.7. Padrões abertos:

6.8.7.7.1. PDF;

6.8.7.7.2. HTML;

6.8.7.7.3. CSV;

6.8.7.7.4. TXT.

6.8.8. A solução deve classificar os dados como:

6.8.8.1. Dado pessoal;

6.8.8.2. Dados financeiros, com base em modelos integrados ou técnicas de classificação.

6.8.9. Deve possibilitar a identificação de informações padronizadas do Brasil, tais como:

6.8.9.1. Registro Geral (RG);

6.8.9.2. CPF;

6.8.9.3. CNH;

6.8.9.4. Passaporte.

6.8.10. A solução deve permitir a inclusão de modelos de políticas (descoberta e classificação) específicas para LGPD.

6.8.11. A solução deve fornecer relatórios detalhados para demonstrar conformidade com a Lei Geral de Proteção de Dados (LGPD).

6.8.12. A solução deve possibilitar a classificação de dados utilizando:

6.8.12.1. Regex,

6.8.12.2. Patterns,

6.8.12.3. Algoritmos,

6.8.12.4. Contexto.

6.8.13. A solução deve permitir ser implementada "com" ou "sem" agentes instalados.

6.8.14. A solução deve possuir as seguintes características funcionais:

6.8.14.1. Políticas: definir as políticas de privacidade de dados, locais e perfis de varredura e de classificação;

6.8.14.2. Descoberta: localizar dados estruturados e não estruturados, através de toda a organização em ambientes big data, banco de dados e sistema de armazenamento de arquivos;

6.8.14.3. Classificação: classificar dados pessoais e sensíveis, baseado em modelos pré-configurados e técnicas de classificação;

6.8.14.4. Análise de risco: entender a natureza do dado e seus riscos, oferecendo visualizações;

6.8.14.5. Relatórios: gráficos e relatórios de análise de risco, status e alertas durante todo o ciclo de vida do dado.

6.9. SERVIÇOS DE TREINAMENTO – ITEM 17:

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

6.9.2. Deverá ser emitido certificado de participação ao final do curso.

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

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

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

6.9.5.1. ISC2 CSSLP - Certified Secure Software Lifecycle Professional (ISO/IEC 17024);

6.9.5.2. ISC2 CISSP – Certified Information System Security Professional;

6.9.5.3. ISC2 ISSAP – Information System Security Architect Professional;

6.9.5.4. CISM – Certified Information Security Manager;

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

6.9.6. 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.

6.9.7. 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.

6.10. CONSULTORIA PARA AVALIAÇÃO PERIÓDICA (HEALTHCHECK) – ITEM 18:

6.10.1. O Serviço deverá 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.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

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

6.10.3. Deverá ser executado mediante emissão de ordens de serviço.

6.10.4. Deverá ser executado periodicamente de não excedendo o intervalo de dois meses entre as execuções.

6.10.5. O Serviço deverá ser executado nas dependências da **CONTRATANTE**, prioritariamente, em horário comercial. Caso a **CONTRATANTE** julgue necessário poderá ser agendada uma janela de manutenção fora do horário comercial sem custos adicionais para a contratante.

6.10.6. As Seguintes atividades deverão ser cobertas pelo serviço:

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

6.10.6.2. Verificar a configuração de alta disponibilidade e status de replicação;

6.10.6.3. Verificar os procedimentos para fail-over;

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

6.10.6.5. Verificar as configurações de contas de administradores e domínios em relação aos requisitos de segurança;

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

6.10.6.7. Verificar se as melhores práticas para backup automático e chaves estão implementadas e documentadas;

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

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

6.10.6.10. 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;

6.10.6.11. Demonstrar e executar relatórios que podem ser usados para verificar os resultados;

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

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

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

6.10.7. 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.

6.11. CONSULTORIA SOB DEMANDA PARA EMISSÃO DE RELATÓRIOS DE CONFORMIDADE COM A LGPD – ITEM 19:

6.11.1. O Serviço deverá realizar uma varredura no ambiente protegido pela solução identificando, neste ambiente, todos os pontos de não-conformidade com a LGPD.

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

6.11.3. O Serviço deverá ser executado nas dependências da **CONTRATANTE**, prioritariamente, em horário comercial. Caso a **CONTRATANTE** julgue necessário poderá ser agendada uma janela de manutenção fora do horário comercial sem custos adicionais para a contratante.

6.11.4. As seguintes atividades deverão ser cobertas pelo serviço:

6.11.4.1. Verificar a configuração do agente de descoberta e classificação de dados, versão instalada e os requisitos de atualização, provendo relatório de impacto e orientação de planejamento para atualização;

6.11.4.2. Verificar as configurações de classificação de dados, fazendo as recomendações de melhorias;

6.11.4.3. Verificar a programação de varredura implementada, comparando com as políticas de segurança da **CONTRATANTE**;

6.11.4.4. Verificar os logs das últimas varreduras identificando ocorrências de falhas e

gerando recomendações para correções;

6.11.4.5. Avaliar as configurações de classificação de dados pessoais / sensíveis de acordo com a LGPD e suas atualizações, quando ocorrerem;

6.11.4.6. Realizar a varredura em todo ambiente atendido pela solução de proteção;

6.11.4.7. Gerar relatório de riscos e painéis gráficos;

6.11.4.8. Gerar relatório de conformidade com a LGPD;

6.11.4.9. Gerar recomendações de correção;

6.11.4.10. Emitir relatório consolidado da varredura com a evidência de todas as atividades realizadas, Painel de conformidade e lista de recomendações.

6.11.5. Ao término da execução dos serviços de "Consultoria sob demanda para emissão de relatórios de conformidade com a LGPD" o (s) relatório (s) deverão ser apresentados à **CONTRATADA** em mídia eletrônica para emissão do termo de aceite da ordem de serviço.

CLÁUSULA SÉTIMA – DO FORNECIMENTO DAS LICENÇAS

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

7.2. A **CONTRATADA** terá o prazo de 05 (cinco) dias úteis para realizar a entrega das licenças a partir da data de emissão da ordem de fornecimento de bens.

7.3. As licenças deverão ser fornecidas na forma de certificado nomeadas a **CONTRATANTE**, e com os respectivos números de série.

7.4. 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 compõe a solução

CLÁUSULA OITAVA – DA INSTALAÇÃO E CONFIGURAÇÃO

8.1. A implantação da solução será realizada por intermédio da abertura de Ordem de Serviço específica.

8.2. As seguintes atividades fazem parte de seu escopo:

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

8.2.2. Instalação da solução todos os módulos que a compõe, no ambiente disponibilizado pela **CONTRATANTE**;

8.2.3. Configurações necessárias para emissão de alertas através do sistema de correio eletrônico da **CONTRATANTE**;

8.2.4. Integração com NOC da **CONTRATANTE**.

8.3. Caberá a **CONTRATANTE** disponibilizar o ambiente tecnológico para que a solução da **CONTRATADA** seja instalada e configurada.

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

8.5. 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 **CONTRATANTE**.

8.6. 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.

8.7. A instalação e configuração da plataforma deverá ser realizada nas dependências da **CONTRATANTE**, em horário comercial.

CLÁUSULA NONA – DA MANUTENÇÃO, SUPORTE E GARANTIA

9.1. 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.

9.2. 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 **CONTRATANTE**;

9.3. 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 **CONTRATANTE**. 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).

9.4. 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.

9.5. A **CONTRATANTE** 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.

9.6. 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 fora deste período serão contabilizados apenas a partir do início do período útil operacional seguinte.

9.7. Relatórios sobre a prestação dos serviços:

9.7.1. 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.

9.7.2. 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.

9.7.3. 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.

9.7.4. 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.

9.8. 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

9.9. 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 **CONTRATANTE**, sem ônus adicionais, enquanto o contrato estiver vigente.

9.10. Entende-se por manutenção corretiva a série de procedimentos destinados ao reestabelecimento 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;

9.11. 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.

9.12. 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 ALMT, inclusive quanto às ferramentas, equipamentos e demais instrumentos necessários à sua realização.

CLÁUSULA DÉCIMA – DA DESCRIÇÃO DA SOLUÇÃO TECNOLÓGICA

10.1. A plataforma e/ou ferramental tecnológico deverá atender às seguintes especificações técnicas e requisitos de gestão:

10.1.1. A solução ofertada deve reduzir ao máximo a ocorrência de incidentes internos de segurança monitorando a atividade de credenciais com acessos privilegiados (ex. Administradores, root, etc.), 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;

10.1.2. A solução ofertada deve estabelecer o controle de acesso para esse tipo de usuário e identificar atividades suspeitas gerando logs destas atividades;

10.1.3. A solução ofertada 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;

10.1.4. A solução ofertada deve 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;

10.1.5. A solução ofertada deve ser flexível e escalável, adequando-se às necessidades de crescimento da empresa contratante;

10.1.6. A solução ofertada precisa permitir a anonimização dos dados pessoais e/ou confidenciais, conforme definido no artigo 12 da Lei Geral de Proteção de Dados Brasileira (LGPD);

10.1.7. A solução ofertada deve proteger sistemas de dados estruturado (bancos de dados) e sistemas de dados não estruturado (incluindo arquivos de aplicativos da Microsoft, voz, vídeo e texto em geral) em um ambiente heterogêneo de sistemas operacionais e plataformas de operação;

10.2. A solução ofertada deve suportar pelo menos:

10.2.1. Sistemas operacionais Microsoft Windows Server, e Linux;

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

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

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

10.2.4. A solução ofertada deve suportar tudo com console de gerenciamento centralizada para facilitar o processo de administração, controle de acesso, gestão e logs e manutenção da solução de proteção de dados;

10.2.5. Soluções baseadas em software livre não serão aceitas.

CLÁUSULA DÉCIMA PRIMEIRA – DA DESCRIÇÃO DOS SERVIÇOS ESPECIALIZADOS

11.1. O fornecimento dos serviços especializados objeto deste certame observará o seguinte quantitativo:

Item	Descrição	Unidade	Quantidade
	Serviços sob demanda pra implementação de agentes	UST	3000

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

11.3. Todas as atividades desempenhadas relativas aos serviços especializados deverão ser executadas nas dependências da **CONTRATANTE**, respeitando o horário de funcionamento da **CONTRATANTE**, e com o acompanhamento e ciência dos servidores.

11.4. Os serviços especializados serão demandados de acordo com a necessidade da **CONTRATANTE**, 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.

11.5. 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.

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

CLÁUSULA DÉCIMA SEGUNDA – DO SERVIÇO DE SUPORTE PARA CONSOLE DE GERENCIAMENTO E SEUS AGENTES DE PROTEÇÃO

12.1. Suporte técnico 24x7.

12.2. Troubleshooting problemas de comunicação com os agentes.

12.3. Escalação de problemas para as áreas responsáveis de Administração e Operação.

12.4. Atuação em chamados de problemas e incidentes abertos no Help Desk.

12.5. Atualização dos chamados.

12.6. Apoio e esclarecimento de causa raiz do problema.

12.7. Detalhamento da solução adotada.

12.8. Documentação de evidências.

12.9. Confecção de relatórios mensais da saúde e principais eventos do gerenciamento

CLÁUSULA DÉCIMA TERCEIRA – DAS ORDENS DE SERVIÇOS (OS)

13.1. Todo e qualquer serviço somente será executado pela **CONTRATADA** mediante uma Ordem de Serviço (O.S.), autorizada por representante da Secretaria de Tecnologia da Informação (Gestor do Contrato).

13.2. As Ordens de Serviço serão consideradas como adendos ao Contrato e deverão descrever os serviços de forma detalhada, contemplando a identificação do tipo de serviço, a complexidade, os prazos, os requisitos de qualidade, e o responsável pelo atesto na **CONTRATANTE**.

CLÁUSULA DÉCIMA QUARTA – DA SUBCONTRATAÇÃO

14.1. Dispõe a Lei nº 8.666/93, em seu art. 72, que a **CONTRATADA**, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar partes do serviço ou fornecimento, até o limite admitido, em cada caso, pela Administração.

14.2. Será admitida a subcontratação parcial do objeto entre os limites mínimo e máximo de 5% e 50%, respectivamente, do valor total do contrato, nas seguintes condições:

14.2.1. É vedada a sub-rogação completa ou da parcela principal da obrigação. São obrigações adicionais da **CONTRATADA**, em razão da subcontratação:

14.2.2. Apresentar a documentação de regularidade fiscal das microempresas e empresas de pequeno porte subcontratadas, sob pena de rescisão, aplicando-se o prazo para regularização previsto no § 1º do art. 4º do Decreto nº 8.538, de 2015;

14.2.3. Substituir a subcontratada, no prazo máximo de trinta dias, na hipótese de extinção da subcontratação, mantendo o percentual originalmente subcontratado até a sua execução total, notificando o órgão ou entidade contratante, sob pena de rescisão, sem prejuízo das sanções cabíveis, ou a demonstrar a inviabilidade da substituição, hipótese em que ficará responsável pela execução da parcela originalmente subcontratada;

14.2.4. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da **CONTRATADA** pela perfeita execução contratual, bem como pela padronização, pela compatibilidade, pelo gerenciamento centralizado e pela qualidade da subcontratação, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a **CONTRATANTE** pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação. Não será aplicável a exigência de subcontratação quando a **CONTRATADA** for qualificada como microempresa ou empresa de pequeno porte

CLÁUSULA DÉCIMA QUINTA – DA PRIORIEDADE INTELECTUAL

15.1. A **CONTRATADA** deverá entregar a **CONTRATANTE** toda e qualquer documentação gerada em função da prestação de serviços, objeto desta contratação.

15.2. A **CONTRATADA** cederá a **CONTRATANTE**, em caráter definitivo, o direito patrimonial dos resultados produzidos durante a vigência do Contrato, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas,

dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

15.3. A **CONTRATADA** fica proibida de veicular e comercializar os produtos e informações geradas, relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da **CONTRATANTE**.

CLÁUSULA DÉCIMA SEXTA – DO SIGILO

16.1. A **CONTRATADA** deverá manter sigilo absoluto sobre quaisquer dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias de que venha a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob as penas da lei, independentemente da classificação de sigilo conferida a tais documentos.

16.2. A **CONTRATADA** não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da ALMT, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

CLÁUSULA DÉCIMA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

17.1. Na execução do objeto do contrato, obriga-se a **CONTRATADA** a:

17.1.1. Executar fielmente os serviços objeto deste contrato, em conformidade com o presente Contrato e o Termo de Referência nº. 010/2021/STI;

17.1.2. Manter-se, durante toda execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação (inciso XIII, Art. 55, da Lei Federal n. 8.666/93);

17.1.3. Responsabilizar-se por quaisquer danos pessoais e/ ou materiais, causados por técnicos (empregados) e acidentes causados por terceiros, bem como pelo pagamento de salários, encargos sociais e trabalhistas, tributos e demais despesas eventuais, decorrentes da prestação de serviços;

17.1.4. Responsabilizar-se pelas eventuais despesas para execução do serviço solicitado, qualquer que seja o valor, e cumprir todas as obrigações constantes do presente contrato;

17.1.5. Apresentar à **CONTRATANTE** até o terceiro dia útil do mês subsequente, comprovante de recolhimento dos encargos previdenciários, resultantes da execução do Contrato e comprovante de recolhimento dos encargos trabalhistas, fiscais e

comerciais;

17.1.6. Prestar o serviço obedecendo às disposições legais;

17.1.7. Atender prontamente quaisquer exigências do representante da **CONTRATANTE**, para a solução de quaisquer dificuldades ou problemas técnicos ou administrativos, relativos ao objeto da contratação.

CLÁUSULA DÉCIMA OITAVA - DAS OBRIGAÇÕES DA CONTRATANTE

18.1. Na execução do objeto do contrato, obriga-se o **CONTRATANTE** a:

18.1.1. Efetuar os pagamentos devidos à **CONTRATADA**, nas condições estabelecidas neste Contrato e no Termo de Referência;

18.1.2. Exercer a fiscalização do contrato,

18.1.3. Receber provisória e definitivamente o objeto do contrato nas formas definidas; e verificar se a **CONTRATADA** está realizando as obrigações estabelecidas neste Contrato e no Termo de Referência;

18.1.4. Permitir ao pessoal técnico da **CONTRATADA**, desde que identificado e incluído na relação de técnicos autorizados, o acesso às unidades para a execução dos serviços, respeitadas as normas de segurança vigentes nas suas dependências;

18.1.5. Notificar a **CONTRATADA** quanto a defeitos ou irregularidades verificados na execução dos serviços objeto deste Contrato, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para a **CONTRATANTE**;

18.1.6. Informar à **CONTRATADA** as normas e procedimentos de acesso às instalações, e eventuais alterações;

18.1.7. Acompanhar a execução do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos serviços. Sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais;

18.1.8. Comunicar à **CONTRATADA** a necessidade de substituição de qualquer profissional que seja considerado inadequado para o exercício da função;

18.1.9. Emitir, antes da execução de qualquer serviço, a competente O.S., definindo claramente os requisitos técnicos, administrativos e financeiros relativos ao serviço objeto deste Contrato;

18.1.10. Especificar e estabelecer normas, diretrizes e metodologias para a execução dos serviços, definindo as prioridades, regras, bem com os prazos e etapas para cumprimento das obrigações;

18.1.11. Avaliar o relatório mensal das atividades executadas pela **CONTRATADA**;

18.1.12. Indicar representante para acompanhar e fiscalizar a execução do contrato nas respectivas áreas de atuação.

18.1.13. Disponibilizar os recursos físicos e tecnológicos (equipamentos, instrumentos, softwares etc.), para a execução dos serviços nas suas instalações.

CLÁUSULA DÉCIMA NONA – CONDIÇÕES DE SUSTENTABILIDADE

19.2. Todo documento deverá ser entregue pela **CONTRATADA**, quer seja pelo processo de cópia ou impresso, deverão ser feitos, preferencialmente, através de papel A4 ou papel ofício oriundos de processo de reciclagem, inclusive, os envelopes que forem entregues ao Pregoeiro, preferencialmente deverão ser todos em material reciclado.

CLÁUSULA VIGÉSIMA - DO PAGAMENTO

20.1. O pagamento será em até 30 (trinta) dias da entrada da Nota Fiscal/Fatura na Secretaria de Planejamento, Orçamento e Finanças, de acordo com a Nota de Empenho e a Nota de Autorização de Despesa - NAD, após o atesto pela fiscalização do recebimento pela **CONTRATANTE**.

20.2. A **CONTRATADA** deverá indicar no corpo da Nota Fiscal/Fatura, descrição do produto (com detalhes), o número e o nome do Banco, Agência e número da conta corrente onde deverá ser feito o pagamento, via ordem bancária e apresentação dos comprovantes atualizados de regularidade abaixo, sob pena de aplicação das penalidades específicas previstas na Cláusula Vigésima Terceira:

a) Prova de regularidade fiscal para com a Fazenda Federal, Estadual e Municipal do domicílio ou sede da Contratada, consistindo em certidões ou documento equivalente, emitidos pelos órgãos competentes e dentro dos prazos de validade expresso nas próprias certidões ou documentos;

b) Prova de regularidade fiscal para com a Procuradoria da Fazenda Nacional e para com a Procuradoria Geral do Estado, nos casos em que não sejam emitidas em conjunto às regularidades fiscais;

c) Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço – FGTS (art. 27 da Lei 8.036/90), em plena validade, relativa à Contratada;

d) Prova de regularidade perante o Instituto Nacional de Seguridade Social - INSS (art. 195, § 3° da Constituição Federal), em plena validade, relativa à Contratada;

e) Certidão Negativa de Débitos Trabalhista – TRT.

20.3. A **CONTRATADA** deverá apresentar **NOTA FISCAL ELETRÔNICA** correspondente produtos efetivamente entregues, nos termos previstos em contrato.

20.4. As Notas Fiscais deverão ser emitidas em nome da Assembleia Legislativa do Estado de Mato Grosso – com o seguinte endereço: Edifício Gov. Dante Martins De Oliveira, Avenida André Antônio Maggi, S/N - CPA - Cuiabá/MT, CNPJ nº 03.929.049/0001-11, e deverão ser entregues no local indicado pela **CONTRATANTE**.

20.5. O pagamento efetuado à adjudicatária não a isentará de suas responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade e validade, nem implicará aceitação definitiva do fornecimento;

20.6. Deverá apresentar a Nota Fiscal de fornecimento/entrada dos produtos/serviços no ato da liquidação, procedimento de conferência.

20.7. Não haverá, sob hipótese alguma, pagamento antecipado;

20.8. Havendo vício a reparar em relação à nota fiscal/fatura apresentada ou em caso de descumprimento pela **CONTRATADA** de obrigação contratual, o prazo constante no item 20.1, poderá ser suspenso até que haja reparação do vício ou adimplemento da obrigação;

20.9. Caso constatado alguma irregularidade nas Notas Fiscais/Faturas, estas serão devolvidas pela Secretaria de Planejamento, Orçamento e Finanças ao fornecedor, para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo para pagamento da data da sua reapresentação;

20.10. Nenhum pagamento será efetuado à empresa adjudicatária enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária;

20.11. A **CONTRATANTE** não efetuará pagamento de título descontado, ou por meio de cobrança em banco, bem como, os que forem negociados com terceiros por intermédio de operação de *factoring*;

20.12. O pagamento somente será efetuado mediante apresentação da regularidade documental.

20.13. As eventuais despesas bancárias decorrentes de transferência de valores para outras praças ou agências são de responsabilidade da **CONTRATADA**;

20.14. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I=(TX/100)$$
$$365$$
$$EM = I \times N \times VP, \text{ onde:}$$

I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual;
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso.

20.14.1. Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos e submetidos à apreciação da autoridade competente, que adotará as providências para eventual apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa à mora.

20.15. Caso haja aplicação de multa, o valor será descontado de qualquer fatura ou crédito existente na Assembleia Legislativa em favor da Contratada, se esse valor for superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário.

20.15.1. Caso a **CONTRATADA** não tenha nenhum valor a receber da **CONTRATANTE**, ser-lhe-á concedido o prazo de 15 (quinze) dias úteis, contados de sua intimação, para efetuar o pagamento.

20.15.2. Após esse prazo, não sendo efetuado o pagamento, seus dados serão encaminhados ao Órgão competente para que seja inscrita na dívida ativa do Estado, podendo, ainda a Administração proceder a cobrança judicial do valor devido.

20.16. O pagamento da fatura não será considerado como aceitação definitiva do objeto contratado e não isentará a **CONTRATADA** das responsabilidades contratuais quaisquer que sejam.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO REAJUSTE

21.1. Os preços são fixos e irreajustáveis no prazo de 12 (doze) meses contados da assinatura do contrato.

21.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de 12 (doze) meses contados da data de assinatura do contrato, aplicando-se o IPCA – Índice Nacional de Preços ao Consumidor Amplo, ou outro índice oficial que vier a substituí-lo, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência do prazo acima mencionado.

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

21.4. 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.

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

21.6. 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.

21.7. 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.

21.8. O reajuste será realizado por apostilamento.

21.9. O reajuste somente será concedido após análise pelo setor competente e mediante motivação e comprovação, por parte da **CONTRATADA**.

21.10. De forma a explanar acerca do índice escolhido, se faz necessário ressaltar que ante a ausência de normativa própria desta Assembleia Legislativa, que disponha sobre as contratações na área de tecnologia da informação, utilizamos para subsidiar as

contratações de serviços e produtos a Instrução Normativa n.º 01/2019 do Governo Federal, que trata das contratações relacionadas a Tecnologia da Informação e que vincula os órgãos da administração pública federal.

21.11. A referida normativa dispõe sobre a necessidade de a utilização do ICTI – Índice de Custos da Tecnologia da Informação, para serviços relacionados a TI, ocorre que em pesquisas realizadas em órgãos públicos da administração federal, tais como TCU e STF (Contrato SEI/STF 0746706, SEI/STF 0489055 Contrato n.º 063/2017, Pregão Eletrônico TCU n.º 080/2019, Pregão Eletrônico n.º 23/2020), observamos que os referidos órgãos utilizam o IPCA – Índice Nacional de Preços ao Consumidor, pois é o que mais se aproxima do efetivo índice inflacionário.

CLÁUSULA VIGÉSIMA SEGUNDA – DA RESCISÃO

22.1. O presente Contrato poderá ser rescindido pelos motivos previstos nos artigos 77 e 78 e nas formas estabelecidas no art. 79, acarretando as consequências do art. 80, todos da Lei nº 8.666/93, nas seguintes hipóteses:

22.1.1. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento;

22.1.2. O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos;

22.1.3. O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos;

22.1.4. A lentidão do seu cumprimento, levando a Administração a comprovar a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;

22.1.5. O atraso injustificado no início da obra, serviço ou fornecimento;

22.1.6. A paralisação da obra, do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração;

22.1.7. A subcontratação total do seu objeto, a associação da **CONTRATADA** com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no edital e no contrato;

22.1.8. Desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores;

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

22.1.9. O cometimento reiterado de faltas na sua execução, anotadas na forma do § 1º do art. 67 desta Lei;

22.1.10. A decretação de falência ou a instauração de insolvência civil;

22.1.11. A dissolução da sociedade ou o falecimento da **CONTRATADA**;

22.1.12. A alteração social ou a modificação da finalidade ou da estrutura da empresa, que prejudique a execução do contrato;

22.1.13. Razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinado a **CONTRATANTE** e exaradas no processo administrativo a que se refere o contrato;

22.1.14. A supressão, por parte da Administração, de obras, serviços ou compras, acarretando modificação do valor inicial do contrato além do limite permitido no § 1° do art. 65 da Lei 8666/93;

22.1.15. A suspensão de sua execução, por ordem escrita da Administração, por prazo superior a 120 (cento e vinte) dias, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, ou ainda por repetidas suspensões que totalizem o mesmo prazo, independentemente do pagamento obrigatório de indenizações pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas, assegurado a **CONTRATADA**, nesses casos, o direito de optar pela suspensão do cumprimento das obrigações assumidas até que seja normalizada a situação;

22.1.16. O atraso superior a 90 (noventa) dias dos pagamentos devidos pela Administração decorrentes de obras, serviços ou fornecimento, ou parcelas destes, já recebidos ou executados, salvo em caso de calamidade pública, grave perturbação da ordem interna ou guerra, assegurado ao contratado o direito de optar pela suspensão do cumprimento de suas obrigações até que seja normalizada a situação;

22.1.17. A não liberação, por parte da Administração, de área, local ou objeto para execução de obra, serviço ou fornecimento, nos prazos contratuais, bem como das fontes de materiais naturais especificadas no projeto;

22.1.18. A ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução do contrato;

22.1.19. Descumprimento do disposto no inciso V, do art. 27 da Lei n° 8.666/93, sem prejuízo das sanções penais cabíveis.

22.2. A rescisão, por algum dos motivos previstos na Lei nº 8.666/93 e suas alterações, não dará à **CONTRATADA** direito a indenização a qualquer título, independentemente de interpelação judicial ou extrajudicial;

22.3. A rescisão acarretará, independentemente de qualquer procedimento judicial ou extrajudicial por parte da **CONTRATANTE**, a retenção dos créditos decorrentes deste Contrato, limitada ao valor dos prejuízos causados, além das sanções previstas neste ajuste até a completa indenização dos danos;

22.4. Fica expressamente acordado que, em caso de rescisão, nenhuma remuneração será cabível, a não ser o ressarcimento de despesas autorizadas pela **CONTRATANTE** e, previstas no presente Contrato e comprovadamente realizadas pela **CONTRATADA.**

22.5. Os casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

CLÁUSULA VIGÉSIMA TERCEIRA – DAS SANÇÕES

23.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a **CONTRATADA** que:

23.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

23.1.2. Ensejar o retardamento da execução do objeto;

23.1.3. Falhar ou fraudar na execução do objeto;

23.1.4. Comportar-se de modo inidôneo;

23.1.5. Não mantiver a proposta; e

23.1.6. Cometer fraude fiscal.

23.2. Pela inexecução total ou parcial do objeto deste contrato, a **CONTRATANTE** pode aplicar à **CONTRATADA** as seguintes sanções:

23.2.1. Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

23.2.2. Multa de:

23.2.2.1. Multa moratória de 0,33% (trinta e três centésimos por cento) por dia de

atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

23.2.2.2. Multa compensatória de 10% (dez por cento) sobre o valor total contratado, no caso de inexecução total do objeto;

23.2.3. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

23.2.4. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

23.2.5. Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos, quando a contratada possuir o cadastro junto ao SICAF.

23.2.6. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, 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 a Contratada ressarcir a Contratante pelos prejuízos causados;

23.3. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

23.3.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

23.3.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

23.3.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

23.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à **CONTRATADA**, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

23.5. 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 Administração, observado o princípio da proporcionalidade.

23.6. As penalidades serão obrigatoriamente registradas no SICAF.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

CLÁUSULA VIGÉSIMA QUARTA – DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

24.1. No momento da contratação será realizada a nomeação, pela CONTRATANTE, da Comissão ou servidor do quadro para exercer a fiscalização dos Contrato.

24.2. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos pelos representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993.

24.3. As atividades de gestão e fiscalização da execução contratual são o conjunto de ações que tem por objetivo aferir o cumprimento dos resultados previstos pela Administração para o serviço contratado, verificar a regularidade das obrigações previdenciárias, fiscais e trabalhistas, bem como prestar apoio à instrução processual e o encaminhamento da documentação pertinente ao setor de contratos para a formalização dos procedimentos relativos a repactuação, alteração, reequilíbrio, prorrogação, pagamento, eventual aplicação de sanções, extinção do contrato, dentre outras, com vista a assegurar o cumprimento das cláusulas avençadas e a solução de problemas relativos ao objeto.

24.4. As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

24.5. A fiscalização poderá ser efetivada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

24.6. O fornecimento dos materiais e a execução dos serviços em desacordo com o objeto deste Contrato, sujeitará a aplicação das sanções legais cabíveis.

24.7. O representante da **CONTRATANTE** anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

24.8. As decisões e providências que ultrapassarem a competência do fiscal do Contrato deverão ser solicitadas aos seus superiores em tempo hábil para a adoção das medidas convenientes.

24.9. É assegurado à fiscalização o direito de ordenar a suspensão dos serviços sem prejuízo das penalidades a que fica sujeito a **CONTRATADA** e sem que esta tenha direito a indenização, no caso de não ser atendida em até 04 (quatro) horas, a contar da comunicação pelo gestor do contrato, qualquer reclamação sobre defeito em serviço executado.

24.10. Caberá à fiscalização atestar os serviços que forem efetivamente executados e aprovados.

24.11. A gestão e fiscalização do contrato se darão mediante o acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que compõem o acordo de níveis de serviços entre a **CONTRATANTE** e a **CONTRATADA**.

CLÁUSULA VIGÉSIMA QUINTA – DA GARANTIA

25.1. A **CONTRATADA** deverá apresentar a garantia de execução contratual de 5% (cinco por cento), sobre o valor global da contratação, em uma das modalidades previstas no §1º do art. 56 da Lei nº 8.666/93, no momento da assinatura do contrato.

CLÁUSULA VIGÉSIMA SEXTA – DA GARANTIA DE ENTREGA

26.1. A **CONTRATADA** garante a entrega dos produtos e serviços no prazo descrito neste Contrato, ficando sujeita às penalidades previstas na legislação vigente em caso de descumprimento.

CLÁUSULA VIGÉSIMA SÉTIMA – DA GARANTIA DE ENTREGA

27.1. Os produtos gerados pela **CONTRATADA** terão garantia durante todo o período de vigência do contrato, dentro do qual a **CONTRATADA** corrigirá os defeitos identificados sem custos adicionais a **CONTRATANTE**.

27.2. A emissão de aceite dos serviços pela **CONTRATANTE** não exime a **CONTRATADA** da responsabilidade pela correção de erros porventura identificados dentro do prazo de vigência do Contrato e após o seu encerramento, dentro do prazo de garantia fornecido pela **CONTRATADA**, sem ônus para a **CONTRATANTE**, desde que o erro ou falha, comprovadamente, não se dê em função de falhas da unidade solicitante dos serviços ou da Secretaria de Tecnologia da Informação.

CLÁUSULA VIGÉSIMA OITAVA – CLÁUSULA ANTICORRUPÇÃO

28.1. Para Execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de que quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação vantagens financeiras ou benefícios de qualquer espécie, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele relacionada, o que deve ser observado, ainda, pelos prepostos e colaboradores.

CLÁUSULA VIGÉSIMA NONA – DA SUJEIÇÃO ÀS NORMAS LEGAIS E CONTRATUAIS

29.1. A legislação aplicável a este Contrato será a Lei Estadual nº 10.534 de 13 de abril de 2017, e, subsidiariamente pela Lei Federal nº 8.666, de 21 de junho de 1993 e suas alterações posteriores, Lei nº 8.078/1990 (Código de Defesa do Consumidor), demais legislações pertinentes e as condições e especificações estabelecidas no Processo Licitatório Pregão Eletrônico nº 035/2021/ALMT, Protocolo SGED 202174528/2021 e no Termo de Referência nº 010/2021-STI, bem como as cláusulas deste Instrumento.

CLÁUSULA TRIGÉSIMA – DAS DISPOSIÇÕES GERAIS

30.1. Integram este Contrato, o Termo de Referência nº 010/2021/STI e seus anexos, e a proposta comercial apresentada pela **CONTRATADA**.

30.2. Os casos omissos serão resolvidos conforme dispõem as Leis Federais nº 8.078/1990 (Código de Defesa do Consumidor), nº 10.534/2017 e nº 8.666/1993, Código Civil e demais legislações vigentes e pertinentes à matéria;

30.3. A abstenção, por parte da **CONTRATANTE**, de quaisquer direitos e/ou faculdades que lhe assistem em razão deste contrato e/ou lei não importará renúncia a estes, não gerando, pois, precedente invocável.

CLÁUSULA TRIGÉSIMA PRIMEIRA – DO FORO

30.1 - Fica eleito o foro da cidade de Cuiabá, Estado de Mato Grosso, como competente para dirimir quaisquer dúvidas ou questões decorrentes da execução deste Contrato.

ASSEMBLEIA LEGISLATIVA DE MATO GROSSO | CNPJ: 03 929 049/0001-11
Avenida André Antônio Maggi, nº 6, setor A, CPA, CEP 78049-901, Cuiabá/MT
www.al.mt.gov.br FaceALMT (65) 3313-6411

E, por se acharem justas e contratadas, as partes assinam o presente instrumento na presença das testemunhas abaixo, em 3 (três) vias de igual teor e forma, para que produza todos os efeitos legais.

Cuiabá – MT 13 de dezembro de 2021.

CONTRATANTE **ASSEMBLÉIA LEGISLATIVA DO ESTADO DE MATO GROSSO** **CNPJ nº 03.929.049/0001-11**	**DEPUTADOS – MESA DIRETORA** Max Russi: _____ **Presidente** Eduardo Botelho: _____ **1º Secretário**
CONTRATADA **DEK SOLUÇÕES EM T.I. LTDA** **CNPJ nº 21.191.387/0001-80**	**REPRESENTANTE LEGAL** Hermann Drummond Junior RG nº 5.997.777 SSP/MG e CPF nº. 820.636.051-49 ASSINATURA: _____
TESTEMUNHA NOME: Luzia S. Ribeiro RG Nº: CPF nº 124.852.498-92 CPF Nº: RG nº 23382713-X SSP/SP ASSINATURA: _____	**TESTEMUNHA** NOME: _____ RG Nº: JENIFER CRISTINA DA SILVA CPF Nº : CPF: 013.172.711-73 ASSINATURA: RG: 1735117-0 SSP/MT