Processo nº 00023.01.01-2026

ESTUDO TÉCNICO PRELIMINAR

1 PROCESSO

1.1. Estudo Técnico Preliminar para contratação de empresa de serviços de segurança cibernética, proteção de dados, gerenciamento de ativos de TI e gerenciamento de backup e armazenamento de arquivos local e em nuvem, incluindo implantação, configuração, treinamento e suporte contínuo para atender as necessidades da Câmara Municipal de Unaí-MG, conforme especificações técnicas em anexo.

2 REQUISITANTE

2.1 Requisitante: Anderson Alves Ribeiro - Chefe do Serviço de Informática

3 DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1 Atualmente a Câmara Municipal de Unaí possui apenas um ponto de armazenamento de backup que se encontra no mesmo prédio da Câmara Municipal de Unaí, onde os dados estão armazenados. No cenário atual, a ausência de uma política estruturada de backup externo em nuvem representa um risco significativo à integridade e disponibilidade das informações, uma vez que a manutenção de cópias de segurança em ambiente distinto do local de produção é uma das principais recomendações das boas práticas de segurança da informação. Em casos de incidentes como falhas de hardware, ataques cibernéticos, sequestro de dados (ransomware) ou desastres físicos, a inexistência dessa redundância pode ocasionar perdas irreversíveis.

3.2 Isso contraria as boas práticas de segurança que recomendam a replicação dos dados em outro ambiente físico, pois em caso de acidentes ou catástrofes os mesmos estariam protegidos. Além de um amplo gerenciamento dos recursos de tecnologia do Legislativo de Unaí.

3.3 A Câmara conta com solução de antivírus em uso, porém faz-se necessária a realização de novo processo licitatório para a continuidade dos serviços, bem como a ampliação da proteção do ambiente tecnológico com a inclusão de solução de backup em nuvem, portanto, apesar de possuir contratação de solução de antivírus e proteção contra sequestros de dados e malwares em geral ou solução para gerenciamento das atualizações e inventário de hardware ou controle dos dispositivos externos, necessita de aumento da quantidade de licenças de 95 para 165, além do contrato em vigor vencer no dia 09/05/2026.

3.4 Embora exista proteção antivírus, é fundamental garantir uma solução mais robusta e integrada, que contemple não apenas a proteção contra vírus tradicionais, mas também ameaças avançadas, como malwares sofisticados, ataques de ransomware e outras vulnerabilidades, bem como recursos de gerenciamento centralizado, controle de dispositivos, inventário de ativos e atualização automatizada dos sistemas.

3.5 A CMU necessita garantir a integridade, confidencialidade e disponibilidade de seus dados institucionais, processos legislativos eletrônicos e registros administrativos. O aumento de ameaças cibernéticas e a necessidade de conformidade com a LGPD (Lei Geral de Proteção de Dados) tornam indispensável uma solução robusta de backup que ofereça:

3.5.1 Segurança e Conformidade: Proteção contra perda de dados por falhas técnicas ou ataques.
3.5.2 Continuidade de Negócios: Garantir que o trabalho legislativo não seja interrompido.
3.5.3 Proteção em Nuvem: Armazenamento externo seguro e automatizado.

3.6 A contratação prevê o treinamento do servidor da Câmara com a finalidade de capacitá-lo para operar as ferramentas, monitorar alertas de segurança e realizar restaurações de dados de forma autônoma e segura.

4 DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

4.1 O objeto da contratação está previsto no Plano de Contratações Anual - PCA 2026 do órgão, conforme item 234.

4.2 Consta ainda previsão desta despesa no orçamento de 2026 da Câmara Municipal de Unaí com recursos financeiros para ser empenhada na seguinte dotação orçamentária 01.01.00.01.031.1000.2002.3.3.90.40, ficha 15, conforme declaração do departamento financeiro (ID: 6F8.B79).

5 REQUISITOS DA CONTRATAÇÃO

5.1 Todas as aplicações e licenças do objeto deverão ser legítimas. Será inadmissível a utilização de licenças e aplicações pirateadas/craqueadas.

5.2 Os dados deverão ser armazenados em datacenter que possua as características mínimas necessárias para a certificação ISO/IEC 27001 ou TIER III e estar localizado em território nacional.

5.3 A execução dos serviços do objeto deverá ser feita nos equipamentos, em funcionamento, que serão atendidos com a solução.

5.4 A solução contratada não deverá possuir restrição de uso, devendo estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias/semana, 365 (trezentos e sessenta e cinco) dias por ano.

5.5 Em caso de rescisão contratual, a contratada deverá garantir a disponibilização dos dados para restauração, assegurando um prazo mínimo de 10 (dez) dias para que os arquivos possam ser baixados.

5.6 A portabilidade de migração dos dados deverá ser realizada pela contratada sem custos adicionais de "egress fees" (taxas de saída).

5.7 A solução e seu fornecedor deverão estar devidamente alinhados à Lei nº 9.609, de 19 de fevereiro de 1998 (Lei de direitos autorais), bem como cientes que, o descumprimento de qualquer regulamentação referente aos direitos de propriedade intelectual de programa de computador, incorrerá em penalidades contratuais, além das previstas pela Lei.

5.8 A contratada deverá realizar toda a implantação e configuração da solução contratada, bem como ministrar o treinamento necessário, com a finalidade de capacitar o servidor responsável a operar as ferramentas, monitorar alertas de segurança e realizar restaurações de dados de forma autônoma e segura.

5.9 O armazenamento dos dados deverá ser realizado exclusivamente em servidores (datacenter) de nuvem localizados em território nacional, garantindo que todas as informações permaneçam sob jurisdição brasileira, em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e demais normativos aplicáveis à proteção de dados e à segurança da informação.

5.10 A contratada deverá fornecer o suporte durante a vigência do contrato.

5.11 Os demais requisitos estão dispostos no anexo II e nada impede de constar no termo de referência outros.

6 ESTIMATIVAS DAS QUANTIDADES E VALOR PARA CONTRATAÇÃO

6.1 A quantidade da contratação está conforme o documento de formalização da demanda. O valor total anual do objeto fica estimado em **R$65.387,84 (sessenta e cinco mil trezentos e oitenta e sete reais e oitenta e quatro centavos).**

6.2 A estimativa de valor desta contratação foi definida através da combinação dos incisos II e IV do § 1º do art. 23 da Lei nº 14.133/2021, com base na mediana dos valores obtidos, conforme demonstrado na tabela abaixo. Para tanto, foram realizadas pesquisas de contratações similares realizadas por órgãos da Administração Pública e pesquisa direta com fornecedores, este ano, e reconhecidos no mercado. Após a análise, verificou-se que o valor apurado é compatível com os preços praticados no mercado, portanto, utilizado como referência para a estimativa do custo da contratação.

6.3 As pesquisas de preços utilizadas para estimar esta contração encontram-se no anexo III deste documento.

Pesquisa de Preço	Valor mensal	Valor anual
BACKUPJA segurança cibernética	R$5.448,99	R$65.387,88
HMC Serviços	R$5.454,60	R$65.455,22

LOBUS Software	R$5.417,66	R$65.011,92
CONSELHO REGIONAL DE CONTABILIDADE DO ESPIRITO SANTO/ES https://crc-es.org.br/novas-licitacoes	R$8.000,00	R$96.000,00
CAMARA MUNICIPAL DA SERRA/ES https://www.camaraserra.es.gov.br/transparencia/contrato/ver/72	R$5.333,33	R$64.000,00
Valor estimado para a contratação conforme a mediana	**R$5.448,99**	**R$65.387,88**

7 LEVANTAMENTO DE MERCADO

7.1 Foram analisadas diferentes abordagens para atender à demanda de segurança cibernética e backup, considerando a relação custo-benefício, a eficácia e a complexidade de gerenciamento;

a) Descrição: Continuar com o sistema de backup local falho e permitir o vencimento do contrato de antivírus sem substituição e sem solução de gestão de ativos e backup Office 365.

b) Justificativa para Descarte: Esta alternativa é inviável e inaceitável. Manteria a Câmara em uma situação de alta vulnerabilidade a ataques cibernéticos e perda de dados, com graves implicações para a continuidade dos serviços e a conformidade com a LGPD. Os riscos associados superam qualquer economia de curto prazo.

7.2 Contratação de Soluções Separadas

a) Descrição: Adquirir licenças de antivírus, soluções de gestão de ativos e serviços de backup em nuvem (incluindo Office 365) de diferentes fornecedores, por meio de processos de contratação distintos.

b) Justificativa para Descarte: Embora possa oferecer flexibilidade na escolha de "melhores de cada categoria", esta alternativa apresenta desvantagens significativas:- Maior Complexidade de Gerenciamento: Múltiplos contratos, fornecedores, interfaces de gerenciamento e equipes de suporte, aumentando a carga de trabalho da equipe de TI.- Possíveis Incompatibilidades: Dificuldade de integração entre soluções de diferentes fabricantes, criando lacunas de segurança.- Custo Total Elevado: A negociação de cada item separadamente pode resultar em um custo total maior do que um pacote integrado.- Dificuldade na Resolução de Problemas: Em caso de incidentes, a identificação da causa raiz pode ser complexa devido à multiplicidade de sistemas e fornecedores.

7.3 Contratação de Soluções Integradas (Alternativa mais viável)

a) Descrição: Contratação de um pacote de serviços e licenças que englobe antivírus, gestão de ativos, backup local e em nuvem incluindo o Oficce 365 (Exchange Online, Teams, Sharepoint e One Driver), implantação, treinamento e suporte, preferencialmente de um único fornecedor com soluções integradas.

b) Justificativa para Escolha: Esta alternativa é a mais vantajosa para a Câmara, pelos seguintes motivos:- Otimização de Custos: A aquisição de um pacote integrado geralmente resulta em um custo total mais competitivo.- Gerenciamento Simplificado: Uma única interface de gerenciamento e um ponto de contato para suporte técnico simplificam a administração e reduzem a complexidade operacional.- Maior Eficácia na Proteção: Soluções integradas são projetadas para funcionarem em conjunto, proporcionando uma camada de segurança mais robusta e sem lacunas.- Conformidade Regulatória: Facilita o atendimento aos requisitos da LGPD por meio de uma abordagem unificada de segurança e proteção de dados.- Suporte Unificado: Um único fornecedor responsável por todas as soluções agiliza a resolução de problemas e garante a responsabilidade. Portanto, esta alternativa busca racionalidade técnica e econômica.

8 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

8.1 A contratação de empresa para o fornecimento de solução de proteção de dados e gerenciamento de ativos em nuvem visa modernizar a infraestrutura tecnológica da Câmara Municipal de Unaí, garantindo a conformidade com a Lei Geral de Proteção de Dados (LGPD) e assegurar a continuidade das atividades legislativas e administrativas de forma segura.

8.2 Este planejamento observa a necessidade crítica de substituição do contrato vigente (vencimento em 09/05/2026), evitando a descontinuidade dos serviços de segurança, o que deixaria a rede da Câmara Municipal vulnerável a ataques e falhas críticas logo após o encerramento do vínculo atual.

8.3 Ademais o aumento das licenças e a contratação do backup em nuvem irão potencializar a segurança de dados para a Câmara.

9 JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

9.1 A contratação em LOTE ÚNICO é vantajosa, pois o seu parcelamento seria inviável por se tratar de um conjunto complexo que opera de forma interdependente, a divisão comprometeria a segurança da informação e a estabilidade do ambiente computacional. O fracionamento do objeto comprometeria a padronização técnica, a compatibilidade entre as ferramentas, a gestão unificada do ambiente e a solução de possíveis problemas. Além disso, ter uma única empresa responsável pelo serviço impede conflitos de responsabilização entre diferentes fornecedores. Ademais, a contratação conjunta proporciona a integração e interoperabilidade das soluções e maior segurança para a Administração, especialmente diante da necessidade de continuidade dos serviços e da proteção dos dados institucionais.

9.2 Portanto, a opção por lote único refere-se à integração interna dos componentes da própria solução, o que assegura compatibilidade, padronização, eficiência, responsabilização definida e melhor aproveitamento dos recursos públicos.

10 DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

10.1 O principal objetivo é mitigar o risco de perda definitiva de dados. Com a implementação da replicação em nuvem, a Câmara deixa de depender exclusivamente de um único ponto físico de armazenamento, dessa forma o resultado esperado é a garantia de que, mesmo em cenários de sinistros físicos (incêndios, inundações ou furtos) no prédio da Câmara, o acervo digital e os sistemas administrativos permaneçam íntegros e disponíveis para recuperação rápida.

10.2 Ademais, a contratação suprirá as necessidades da Câmara Municipal de Unaí no que tange à realização de backup e armazenamento de arquivos, segurança e proteção de dados, gerenciamento dos recursos de tecnologia, visto que a contratação apresentada no presente documento de análise de viabilidade é serviço fundamental para a segurança das informações e a perca ou vazamento dos mesmos geraria enormes prejuízos e transtornos à Administração.

11 PROVIDÊNCIAS A SEREM ADOTADAS

11.1 Que a empresa contratada se reúna com o chefe do serviço de informática para alinharem a implantação, transação e o funcionamento do objeto de forma segura evitando interrupção dos demais serviços administrativos. O planejamento da solução deve ser elaborado e promovido com capacitação do gestor e do fiscal do contrato para que ocorra de forma segura o levantamento do ambiente atual, parametrização das ferramentas, integração com sistemas existentes, se for o caso, testes de funcionamento e validação. As etapas de implantação, treinamento, execução, testes e transição da solução devem ter adequação técnica e operacional relacionados à segurança da informação, proteção de dados pessoais, política de backup, recuperação de arquivos, uso da solução em nuvem, tratamento de incidentes e verificação do cumprimento de todas as obrigações contratuais e legais pela contratada, de modo a assegurar a continuidade dos serviços, a mitigação dos riscos de indisponibilidade e perda de dados e a plena operação das ferramentas contratadas.

12 CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

12.1 Embora a presente contratação se insira no universo da tecnologia da informação, seu objeto possui identidade material própria, consistente em solução integrada de segurança de endpoints, backup corporativo e gerenciamento de ativos, distinta das licenças de produtividade, edição gráfica e audiovisual já contratadas pela Câmara. Assim, as contratações atualmente vigentes nesta Casa (Contratos n.º 3/2022, 24/2024 e 25/2024), embora relacionadas à área de TI em sentido amplo, não integram o mesmo núcleo funcional da solução ora pretendida, pois tratam

de objetos de natureza de produtividade, design técnico e ilustração, design de gráficos e layout, edição de vídeos e com finalidades operacionais distintas.

12.2 As contratações mencionadas não se caracterizam como interdependentes em relação ao presente objeto, uma vez que a solução pretendida possui escopo funcional e arquitetura técnica autônomos, bem como mercado fornecedor nem sempre coincidente, resultado operacional específico voltado à proteção contra malware/ransomware, comportamento malicioso, resposta em estações e servidores, falhas de segurança, cópias de segurança, recuperação de dados, inventário e gestão dos ativos, governança e continuidade operacional, atuando em camadas técnicas diferentes e de natureza diversa. Eventual integração com ambiente já existente ocorrerá apenas no plano da implantação, sem impor unificação contratual com objetos distintos.

12.3 Portanto, o presente objeto possui autonomia funcional com os demais contratos, podendo ser contratado em separado sem perda de eficiência, sem risco de incompatibilidade e sem fracionamento indevido.

13 DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS

13.1 Impactos ambientais potencialmente associados

- Consumo de energia elétrica: A operação de servidores locais, estações de trabalho, equipamentos de rede e a infraestrutura de data center utilizada para armazenamento em nuvem pode ampliar o consumo de energia elétrica.
- Geração de resíduos eletrônicos: A implantação de novas soluções pode exigir substituição, descarte ou atualização de equipamentos obsoletos, como servidores, dispositivos de armazenamento, nobreaks e computadores.
- Uso de infraestrutura de terceiros: O serviço em nuvem depende de data centers operados por fornecedores, cujas operações também consomem energia e recursos naturais.
- Redução de deslocamentos: Em contrapartida, soluções de monitoramento remoto, suporte remoto e backup automatizado podem reduzir a necessidade de deslocamentos presenciais para manutenção e recuperação de dados, diminuindo emissões associadas ao transporte.
- Aumento indireto de equipamentos ativos: A ampliação da camada de proteção e de controle pode demandar maior permanência de equipamentos ligados e monitorados continuamente.

13.2 Avaliação qualitativa dos impactos

- Os impactos ambientais associados à presente contratação são considerados baixos a moderados, pois o objeto da contratação não envolve obras civis, grandes movimentações de terra, uso intensivo de insumos físicos ou geração expressiva de resíduos. Os principais efeitos decorrem do consumo energético e eventual descarte de bens de tecnologia da informação.

13.3 **Medidas de mitigação e boas práticas**

- Para reduzir ou neutralizar eventuais impactos ambientais, recomenda-se a adoção das seguintes medidas:
- Priorizar soluções em nuvem com eficiência energética, preferencialmente fornecidas por data centers que adotem práticas de sustentabilidade e uso racional de energia.
- Estender a vida útil dos equipamentos existentes, sempre que tecnicamente viável, antes de qualquer substituição.
- Adotar política de descarte ambientalmente adequado para resíduos eletroeletrônicos, observando a legislação aplicável e as normas de logística reversa.
- Reduzir a necessidade de impressão de relatórios e documentos, priorizando meios digitais de gestão e auditoria.
- Configurar políticas de uso racional de recursos, evitando processamento e armazenamento desnecessários.

13.4 **Conclusão sobre os impactos ambientais**

- Considerando a natureza da contratação e a execução remota, conclui-se que os impactos ambientais são limitados e controláveis, sendo plenamente mitigáveis por medidas de gestão sustentável da solução de proteção. Além disso, a digitalização e a centralização de backups e controles contribuem indiretamente para maior eficiência operacional e menor uso de recursos materiais.

14 POSICIONAMENTO CONCLUSIVO

14.1 Os estudos preliminares evidenciaram que a contratação é viável, bem como existem empresas no mercado que podem concorrer e fornecer o serviço descrito neste estudo preliminar.

Unaí MG, 29 de abril de 2026.

Claudiane Alves de Melo
Laura Eduarda Bueno da Cruz
Membros da Equipe de Apoio

ANEXO I – ANÁLISE DE RISCOS

Não conformidade com a Lei 14.133/2021.

Probabilidade Média. **Dano:** Nulidade do processo licitatório. **Impacto**: Alto. **Ação de Contingência:** Realizar consultas jurídicas prévias e encaminhar processo para parecer após a conclusão da fase preparatória para assegurar a aderência total aos requisitos legais da Lei.

Superfaturamento na aquisição.

Probabilidade: Baixa. **Dano:** Prejuízo aos cofres públicos. **Impacto:** Alto. **Ação de Contingência:** Pesquisa de preços elaborada com esmero, refletindo os preços praticados no mercado para o objeto a ser contratado.

Atrasos na execução do serviço.

Probabilidade: Média. **Dano:** Comprometimento da continuidade das atividades administrativas e da segurança do parque tecnológico da administração. **Impacto:** Alto. **Ação de Contingência:** Colocar no Termo de Referência e no edital a execução imediata dos serviços e incluir cláusulas contratuais que prevejam penalidades para atrasos na disponibilização do serviço.

Entrega do serviço fora das especificações técnicas descritas no termo de referência.

Probabilidade: Média. **Dano:** Não atendimento das necessidades da administração que justificaram a contratação. **Impacto:** Alto. **Ação de Contingência:** Atuação do fiscal e do gestor durante o acompanhamento da execução, o treinamento e no ato de recebimento do serviço mensalmente deve observar se as especificações técnicas estão sendo atendidas.

ESPECIFICAÇÕES TÉCNICAS E QUANTITATIVO

OBJETO: Contratação de empresa de serviços de segurança cibernética, proteção de dados, gerenciamento de ativos de TI e gerenciamento de backup e armazenamento de arquivos local e em nuvem, incluindo implantação, configuração, treinamento e suporte contínuo para atender as necessidades da Câmara Municipal de Unaí-MG, conforme especificações técnicas em anexo.

Descrição
Solução e segurança de proteção de dados em nuvem (cloud computing) com armazenamento em datacenter, incluindo suporte e treinamento e segurança. Composto por: - 20 servidores vitualizados totalizando uma massa de **1,5 TB de dados;** - 02 Servidores físicos de Virtualização Hyper-V com **0,5 TB de dados;** - File server com uma massa de dados de **09 TB**.
165 licenças de antivírus, com Anti-Ransomware nativo; Solução de proteção para servidores e estações de trabalho;
Solução de gestão avançada de ativos para **165** estações de trabalhos, servidor e máquinas virtualizadas.
Licença de backup do Office 365 Business em nuvem para **107** seats. A solução deverá fazer backup dos serviços: (Exchange Online, Teams, Sharepoint e One Driver) de cada usuário sem restrição de espaço.

4. DESCRIÇÃO DO SERVIÇO

A solução de backup deverá prover

A Solução deve proteger o ambiente atual da CÂMARA que é composto por 20 servidores virtualizados totalizando uma massa de **1,5 TB** de dados, e também, 02 Servidores Físicos de Virtualização Hyper-V com uma massa de **0,5 TB** cada, 01 File server com uma massa de dados de **09 TB.** Além de 165 estações de trabalho.

A solução deverá ser entregue como serviço e todos os dados deverão ser armazenados em datacenter externo ao Ambiente da CÂMARA.

A solução proposta deverá dispor de console/portal para gerência e execução de backup e restauração de dados em nuvem.

A Solução deve ter garantia de atualizações durante o período do contrato sem ônus financeiro para a CÂMARA.

O software deverá oferecer funcionalidade completa de backup e restauração através de gerência centralizada;

O software de backup deverá ser capaz de enviar alertas através de correio eletrônico com o objetivo de reportar eventos ocorridos na operação e configuração do software;

O software deverá possuir painel de gerenciamento de ambiente de backup (dashboard) com suporte a visualização de todas as rotinas de backup, com opção de gerar relatórios online ou enviar os mesmo por e-mail;

O software deverá ser capaz de emitir relatórios com informações completas sobre os jobs executados e porcentagem de sucesso de backups e restaurações;

O sistema deve prover quantidade ilimitada de restaurações, durante a vigência deste contrato.

O tráfego de dados de internet deve ser ilimitado, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados.

A CÂMARA deve garantir o acesso à internet como cliente da solução.

A solução proposta deverá possibilitar comunicação criptografada e protegida para transferência de dados (HTTPS, VPN ou outros);.

A solução proposta deverá permitir a criptografia dos dados na armazenagem e na transmissão dos dados;

O agente (cliente) deve ter um suporte nativo para os seguintes bancos de dados:

- MySQL
- Microsoft SQL Server
- ORACLE

A solução deverá possuir forma de criar scripts de comando para backup de outros bancos de dados além dos citados acima.

Os agentes (clientes) devem possuir suporte do fabricante durante todo o período do contrato, permitindo assim, atualizações constantes dos agentes e da solução como um todo.

Os agentes (clientes) devem poder ser instalados nativamente nas seguintes plataformas de sistemas operacionais e plataformas de virtualização:

- VMware;
- Hyper-V;

- Windows Server;
- Linux.

Deverá ser compatível por instalação de agente com os demais virtualizadores:

– Virtuozzo;

– KVM;

– Red Hat Virtualization;

– Citrix Xen Server;

– Nutanix;

– MV Oracle;

– Scale Computing HC3.

Deverá possuir compatibilidade para backup de dispositivos móveis no mínimo Android e IOS.

Deverá ser compatível com backup de NETWORK ATTACHED STORAGE (NAS) Synology.

O sistema deve ser capaz de gerar relatórios acerca da realização e/ou não realização das rotinas de backup. Os relatórios devem poder ser acessados ou gerados das seguintes formas:

- Por e-mail.
- Via web

Deverá possuir integração nativa para backup das seguintes plataformas online:

- Office 365 Business online;
- Google Workspace.

A solução deve permitir que as cópias de segurança ocorram simultaneamente, de forma a otimizar as janelas de backup.

As tarefas de restauração também devem ocorrer de forma simultânea, seja durante as tarefas de backup ou de restauração.

Dos recursos da solução

- Deve permitir replicação de um mesmo dado da origem para vários destinos.
- Deve permitir replicação criptografada.
- Deve possuir proteção antimalware nativa na ferramenta, com varredura por agendamento.
- A solução de backup deverá possuir tecnologia de desduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados.
- Deverá possuir backup sintético, ou seja, criar uma imagem a partir dos backups incrementais já armazenados no backup
- Deverá suportar política de disasterrecovery para prevenir perda de dados e uma restauração mais rápida e segura.
- Deverá possuir mecanismos que não permitam a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental.
- A solução deverá ter a possibilidade de validar continuamente de forma automática a integridade lógica dos dados, armazenados no hardware com correção automática das falhas encontradas, de forma a garantir a consistência de todo o conteúdo em sua total capacidade.
- Possibilitar predefinir arquivos, pastas ou tipos de arquivos que não devem fazer parte dos backups mesmo quando backup da VM toda;
- Deverá possuir interface de administração GUI.
- Deverá permitir executar múltiplos processos de backup em paralelo e otimizar a restauração de arquivos individuais.
- O sistema de armazenamento de backup deverá ser escalável conforme a necessidade do CONTRATANTE.
- Backup sintético otimizado (funcionalidade que permite criar uma imagem full, a partir dos backups incrementais, sem movimentação de dados);
- Deverá prover o envio de alertas e relatórios através de e-mail, de modo automático, manual ou programado.

- Deverá suportar software de replicação remota do próprio FABRICANTE;
- Deve ter capacidade de restauração de dados granular, a partir de dispositivos de armazenamento em discos, sendo possível a recuperação de um simples arquivo, uma base de dados, ou até mesmo uma completa recuperação do servidor, suportar backup e restore de máquina virtual VMware, Hyper-V, XenServer, com Sistemas Operacionais Windows e Linux, suportando backup “de guest” (agente instalado na máquina virtual) e backup “de imagem” com restore individual de arquivos e diretórios. O restore granular de arquivos a partir do backup da imagem deve ser realizado preferencialmente sem necessidade de instalação de agentes na máquina virtual. Para Banco de Dados sendo eles Oracle, SQL Server, MySQL, MariaDB com instalação de agente.
- A solução de backup a ser ofertada deverá atender integralmente os requisitos especificados neste TERMO DE REFERÊNCIA, devendo ser fornecida com todas as licenças que forem necessárias para entrega funcional da solução proposta onde o licenciamento deverá possuir capacidade ilimitada de retenções.
- Deverá permitir o backup e restore de arquivos abertos, garantindo a integridade do backup.
- Deverá possuir a capacidade de reiniciar backups a partir do ponto de falha, após a ocorrência da mesma.
- Deverá possuir mecanismo de atualização de clientes e agentes de backup de forma remota, através da interface de gerenciamento.
- O suporte e atualização da solução de backup será válido durante todo o período contratado.
- Deverá ter compatibilidade com aplicações, bancos de dados e sistemas de arquivos (File System).
- Deverá possuir correções e atualizações adicionais disponíveis para o funcionamento do produto no Sistema Operacional alvo.
- Deverá possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup.
- Deverá permitir a programação de tarefas de backup automatizadas em que sejam

definidos prazos de retenção dos arquivos personalizáveis.

- Deverá permitir a programação de jobs de backup automatizadas em que sejam definidos prazos de retenção das imagens.
- Deverá permitir a realização do backup completo de servidor para recuperação de desastres.
- Deverá permitir restaurar o backup de recuperação de desastres para hardware diferente do original.
- Deverá ser capaz de recuperar dados para servidores diferentes do equipamento de origem.
- Deverá permitir integração do controle de acesso com sistemas de diretório Active Directory.
- A Solução de Backup deverá, a partir de uma única interface, gerenciar operações de Backup e Restore de diferentes sistemas operacionais Linux e Windows bem como operações de recuperação bare metal de forma nativa sem software de Terceiros.
- Para servidores Windows, deverá ser possível a recuperação das imagens de recuperação de desastres em um hardware ou em ambiente virtual.
- Deverá permitir a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorreção.
- Deverá possuir capacidade nativa de efetuar criptografia dos backups em no mínimo 256 bits nos Clientes de Backup e em dispositivos de mídia que suportem criptografia., tanto no tráfego quanto em repouso com senha personalizável na segunda opção.
- Deverá possuir mecanismo de auditoria, permitindo a emissão de relatórios.
- Deverá possuir capacidade de resumo de tarefas de backup com falha, retomando a partir do momento da falha.
- Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ativadas e executadas periodicamente.
- Base de dados de relatórios para suportar armazenamento de dados históricos

superior a 30 dias.

- Deverá suportar o uso da funcionalidade CBT (ChangeBlockTracking) para as operações de backup.
- Deverá permitir o descobrimento automático das máquinas virtuais nos ambientes VMWare e Hyper-V.
- Deverá permitir restaurar e iniciar a execução de uma máquina virtual instantaneamente, diretamente a partir do seu repositório de backup, sem a necessidade de manter réplicas ou snapshots disponíveis para o processo de recuperação instantânea.
- Deverá prover otimização do backup e recursos, permitindo que somente blocos utilizados sejam copiados no processo de backup.
- Deverá possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais.
- Deverá possuir capacidade de realizar backup de máquinas virtuais em estado online ou off-line.
- Deverá possuir a capacidade de realizar backup On-Host e Off-host das máquinas virtuais Windows.
- Deverá possuir a capacidade de realizar backup de maneira Full, Incremental ou Diferencial.
- Deverá suportar ambientes configurados com Cluster Shared Volumes.
- Deve implementar backup utilizando Microsoft Volume Shadow Copy Service (VSS).
- Os mesmos agentes de backup deverão possuir recurso de acesso remoto aos computadores permitindo assim uma maior facilidade ao suporte;
- Deverá possuir opção para mapeando de dados no backup, com relatório que mostre de acordo com as extensões configuradas se existem dados relevantes fora do plano de backup, se assim contrato em licença adicional.
- Os mesmos agentes (client) de backup deverão realizar inventário de hardware que serão acessados e auditados pela equipe técnica da CÂMARA, sem custo

adicional.

- A solução deverá possuir recursos básicos de segurança como anti-malware e avaliação de vulnerabilidade sistemas operacionais e aplicativos visto que 60% dos vazamentos de dados estão relacionados a falhas em aplicativos;
- O acesso ao portal de gestão deverá possibilitar acesso com autenticação multifator (MFA) via aplicativos de autenticação, sms ou e-mail.

Contratação de antivírus integrado na mesma console, que deverá prover:

- A solução deverá possuir recursos básicos de segurança como anti-malware e avaliação de vulnerabilidade sistemas

operacionais e aplicativos visto que 60% dos vazamentos de dados estão relacionados a falhas em aplicativos;

- Possuir console central único de gerenciamento. As configurações do Antivírus, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através do mesmo console;
- O produto deverá possuir no mínimo os seguintes módulos:
    - Console de Gerenciamento fornecendo funcionalidades de gestão;
    - Módulos para estações físicas, laptops e servidores e VMs;
- Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo os seguintes Hypervisors: VMWare vSphere;
    - Citrix XenServer;
    - Microsoft Hyper-V;
    - Red hat Enterprise Virtualization;
    - Kernel-based Virtual Machine ou KVM;
    - Oracle VM;
- Deverá ser fornecido com base de dados embutido no Console em Nuvem, sem a necessidade de baixar para máquina do administrador do Console.
- Permitir a instalação remota via console WEB de gerenciamento para ambientes

de rede com ou sem domínio configurado.

- Licenciamento flexível, ou seja, permitir remover e adicionar licenças entre dispositivos de forma autônoma, sem precisar depender do suporte técnico;
- Arquitetura simples de atualização, com um simples clicar de botão todas as funções do antivírus.
- Descoberta de rede para máquinas em grupo de trabalho;
- Possuir busca em tempo real pelo menos com os seguintes filtros: Nome e Endereço IP;
- Possibilitar a instalação remota do antivírus;
- Através da console o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;
- Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;
- Deverá reportar o estado atual das máquinas no mínimo, protegida/desprotegida;
- O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado;
- Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- Possuir tarefas remotas e configuráveis de Scan;
- Filtro de sites maliciosos com opção de notificar e bloquear o acesso do usuário, sendo possível gerar uma lista manual de sites bloqueados ou bloqueá-los por categoria;
- Proteção antivírus e antimalware: Detecção de arquivos baseada em assinatura em nuvem em tempo real;
- Analisar arquivos baseados em inteligência artificial de pré-execução, Cyber Engine baseado em comportamento;
- Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit); exploração de memória, injeção de códigos e encaminhamento de privilégios.

- Detecção e interrupção de processos de criptomineração;
- Impedir alterações não autorizadas em registros, processos e aplicações com opção de proteção por senha se necessário.
- Oferecer proteção por base de assinaturas;
- Realizar proteção não só dos discos físicos, mas também de pastas recebidas e enviadas através de compartilhamento de rede.
- Possibilitar gerenciamento do Windows Defender ou Microsoft Security Essentials de forma centralizada na console web permitindo configurar proteção em tempo real, varreduras, exceções e demais funcionalidades do mesmo.
- Possuir alternativa para que o usuário escolha qual ação será tomada em cada item de proteção, por exemplo, se quer ser apenas notificado, que o processo seja interrompido ou revertido.
- Antiransomware baseado em Inteligência Artificial, capaz de detectar e reverter processos de criptografia e sequestro de dados.
- Opção de acesso remoto as máquinas com agentes instalados, podendo essa função ser adicionada individualmente ao antivírus nas estações de forma ilimitada.
- Inventário de hardware para proteção e acompanhando das modificações realizadas nos computadores, permitindo uma proteção completa do patrimônio de informática, essa função também deve poder ser instalada separadamente ao antivírus de forma ilimitada.
- Possuir opção de bloqueio do uso de portas USB e FireWire por dispositivos removíveis, bloqueio do uso de impressões, acesso a área de transferência, dispositivos móveis, capturas de tela, bluetooth e unidades mapeadas.
- Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos.
- O produto deverá possuir no mínimo os seguintes módulos e funcionalidades:
- Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas;

- Módulos para estações físicas, notebooks e servidores;
- Módulo para ambientes virtualizados;
- Utilizar o conceito de heurística para combate e ações contra possíveis malwares;
- Oferecer tecnologia onde a solução identifique vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
- Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware;
- Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução dele no ambiente de produção;
- Oferecer proteção por base de assinaturas.

CONSOLE DE GERENCIAMENTO

- Instalação e configuração
- Permitir instalação remota via console WEB de gerenciamento.
- Deve ser totalmente em português.
- Funcionalidades Gerais
- Licenciamento flexível;
- A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:
- Nome;
- IP;
- Sistema Operacional;
- Política Aplicada;
- A console de gerenciamento deverá incluir sessão de log com as seguintes informações:
- Login;
- Edição;

- Criação;
- Log-out;
- Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços da solução;
- Permitir que o administrador escolha qual o pacote será atualizado;
- As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail;
- No mínimo enviar notificações para as seguintes ocorrências:
- Problemas com licenças;
- Alertas de surto de vírus;
- Máquinas desatualizadas;
- Eventos de antimalware.
- Deverá prover o acesso via HTTPS;
- Possuir no mínimo as integrações abaixo:
- Múltiplos domínios do Active Directory;
- Descoberta de rede para máquinas em grupo de trabalho;
- Possuir busca em tempo real pelo menos com os seguintes filtros:
- Nome;
- Sistema Operacional;
- Endereço IP;
- Possibilitar a instalação remota e desinstalação remota do antivírus;
- Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- Assinar políticas para no mínimo os níveis:
- Computador;
- Máquina Virtual;
- Grupo de Endpoints;

- Possuir a propriedade detalhada de objetos gerenciados para:
- Nome;
- IP;
- Sistema Operacional;
- Grupo;
- Política Assinada;
- Último status de malware.

Políticas

- Modelo único para todos os equipamentos, sejam físicos ou virtuais;
- Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;
- Através da console de gerenciamento o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;
- Deverá permitir quantidade ilimitada de políticas cadastradas.

Relatórios

- Deverá apresentar as seguintes funcionalidades:
- Relatório para cada serviço de segurança;
- Facilidade de usar e visualização simplificada;
- Dashboard de relatórios configurável, para selecionar quais relatórios devem ser exibidos.

Administração de Usuários:

- Deverá apresentas no mínimo as seguintes funcionalidades:
- Administração baseada em regras;
- Deverá ser possível customizar um tipo de usuário:
- Deverá permitir a integração de usuários com o Active Directory para autenticação da console de gerenciamento;

- Registrar as ações do usuário na console de gerenciamento;
- Detalhar cada ação do usuário;
- Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

SEGURANÇA PARA ESTAÇÕES E SERVIDORES

- Proteção para ambientes físicos
- Deverá proteger em tempo real e agendado as máquinas físicas em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac;
- Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:
- Windows 11 64Bits;
- Windows 10 64Bits;
- Windows 8.1 64Bits;
- Windows 8 64Bits;
- Windows 7 64Bits;
- Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:
- Windows Server 2025 ou superior;
- Windows Server 2019;
- Windows Server 2012R2;
- Windows Server 2012;
- Windows Server 2008 R2;
- Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:
- Ubuntu 14.04 LTS ou superior
- Red Hat Enterprise Linux / CentOS 6 ou superior
- SUSE Linux Enterprise Server 11 SP4 ou superior
- OpenSUSE Leap 42.x

- Fedora 25 ou superior
- Debian 8.0 ou superior
- Oracle Linux 6.3 ou superior
- Proteção para ambientes virtuais
- Para plataforma de virtualização com VMWare, deverá:
- A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;
- Deverá proteger em tempo real e agendado as máquinas virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac;
- Possuir opção de bloqueio do uso de portas USB e FireWire por dispositivos removíveis, bloqueio do uso de impressões, acesso a área de transferência, dispositivos móveis, capturas de tela, bluetooth e unidades mapeadas.
- Realizar proteção não só dos discos físicos, mas também de pastas recebidas e enviadas através de compartilhamento de rede.
- Detecção e interrupção de processos de criptomineração.
- Filtro de sites maliciosos com opção de notificar e bloquear o acesso do usuário, sendo possível gerar uma lista manual de sites bloqueados ou bloqueá-los por categoria.

- Instalação e Configuração Remota
- Deverá permitir ao administrador customizar a instalação;
- Deverá permitir a instalação customizada do antivírus com no mínimo:
- Instalar o antivírus sem o controle de acesso à internet;
- A instalação deverá ser possível executar com no mínimo das seguintes maneiras:
- Executar o pacote de antivírus diretamente na estação de trabalho;
- Instalar remotamente, distribuído via console de gerência web;
- Deverá ser possível ter uma visualização com as estações instaladas e as faltantes

da instalação;

- Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;
- Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;
- O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado.

Funções Gerais

- Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança;
- Deverá permitir a configuração do scan do antivírus do cliente como:
- Scan local;
- Scan híbrido (local\remoto);
- Scan remoto;
- Deverá reportar o estado atual das máquinas virtuais no mínimo, protegida/desprotegida;
- Deverá fazer scan em tempo real e automático;
- Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;
- Deverá possuir escaneamento baseado em análise heurística;
- Deverá permitir a escolha e configuração de pastas a serem scaneadas;
- Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:
- Baseada em assinaturas;
- Baseada em heurística;
- Baseada em monitoramento contínuo de processos;
- Antiexploit disponível para servidores e estações de trabalho baseado em Machine Learning para proteger contra vulnerabilidades de softwares;

- Deve possuir módulo de mitigação de Ransomware para detecção e recuperação de possíveis arquivos criptografados.
- Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL nas estações de trabalho;
- Deve possuir módulo de proteção contra-ataques de rede que fornece uma camada de segurança a mais que detecta e executa ações contra-ataques de rede projetados para obter acesso em endpoints através de técnicas específicas, tais como: ataques de força bruta, explorações de rede, ladrões de senha, movimentação lateral, etc.
- Inventário de hardware para proteção e acompanhando das modificações realizadas nos computadores, permitindo uma proteção completa do patrimônio de informática, essa função também deve poder ser instalada separadamente ao antivírus de forma ilimitada.
- Opção de acesso remoto as máquinas com agentes instalados, podendo essa função ser adicionada individualmente ao antivírus nas estações de forma ilimitada.
- Possibilitar gerenciamento do Windows Defender ou Microsoft Security Essentials de forma centralizada na console web permitindo configurar proteção em tempo real, varreduras, exceções e demais funcionalidades do mesmo.
- Deverá ter os seguintes requisitos mínimos de sistema:
- Plataformas de Virtualização
- VMware vSphere ESX 5.0 ou superior;
- VMware vCenter Server 4.1 ou superior;
- Citrix XenDesktop 5.0 ou superior;
- Xen Server 5.5 ou superior;
- Citrix VDI-in-a-Box 5;
- Microsoft Hyper-V Server 2008 R2, 2012
- Oracle VM 3.0;
- Red Hat Enterprise Virtualization 3.0.

- Sistemas Operacionais para Desktops
- Windows 11 64Bits;
- Windows 10 64Bits;
- Windows 8.1 64Bits;
- Windows 8 64Bits;
- Windows 7 64Bits;
- Sistemas Operacionais para Servidores
- Windows Server 2025 ou superior;
- Windows Server 2019;
- Windows Server 2012R2;
- Windows Server 2012;
- Windows Server 2008 R2;
- Windows Server 2008 apenas os módulos de antivírus e Active Virus Control;
- Linux Red Hat Enterprise;
- CentOS 5.6 ou superior;
- Ubuntu 10.04 LTS ou superior;
- SUSE Linux Enterprise Server 11 ou superior;
- OpenSUSE 11 ou superior;
- Fedora 15 ou superior;
- Debian 5.0 ou superior.

Quarentena:

- Deverá permitir restauração remota, com configuração de localidade e deleção;
- Criação e exclusão para arquivos restaurados;
- Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;

- Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
- Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
- Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
- Deverá permitir escanear a quarentena após a atualização de assinaturas.

Controle do Dispositivo:

- Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
- Através do módulo de controle de dispositivo deverá ser possível controlar:
- Bluetooth;
- Unidades ópticas;
- Discos Externos;
- Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:
- Discos Externos;
- USB (Pendrives, armazenamentos removíveis);
- Área de transferência;
- Capturas de tela;
- Unidades mapeadas;
- Deverá permitir regras de definição de bloqueio/desbloqueio;
- Deverá permitir regras de exclusão.

Atualização:

- Após a atualização o administrador deverá ter a capacidade de configurar uma

reinicialização;

- Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
- Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando ela estiver sendo escaneada.

Proteção Avançada:

- Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.
- Detectar e parar, bloquear e interromper malwares sem arquivos.
- Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.
- Reparo e resposta automatizada a ameaças.
- Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal-intencionadas.
- Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.
- Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.
- Deverá ter um nível de proteção na fase de pré-execução com modelos locais de

aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web. Deverá permite que os administradores de segurança ajustem a proteção para combater os riscos.

- Proteção inteligente e em tempo real, verificando constantemente os arquivos e programas abertos, mesmo que para leitura.
- Prevenção de exploração através de recursos de proteção de memória, proteção contra programação orientada por retorno ou técnica ROP, proteção contra encaminhamento de privilégios ou injeção de códigos.
- Incluso funcionalidade EDR (Detecção e resposta do ponto de extremidade) nas licenças, para identificação, detectação e análise de incidentes e infecções da rede, com no mínimo: Coleta de dados forenses, monitoramento de eventos, correlação automatizada de eventos, priorização de atividades suspeitas, resumos de incidentes gerados por I.A, Visualização e interpretação automatizadas da cadeia de ataque MITRE ATT&CK®, resposta de incidentes com um clique, contenção total de ameaças e quarentena do endpoint como um todo, Pesquisa inteligente de IoCs, inclusive ameaças emergentes, Reversão específica de ataques.

Machine Learning

- As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.
- A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinarem continuamente com bilhões de amostras de arquivos legítimos e maliciosas devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.

Gerenciamento de ativos integrado na mesma console, que deverá prover:

- Agendamento de atualizações e execução de backups pré-atualização.

- A ferramenta devera desmobilizar dentro da mesma solução um painel para gestão das atualizações de aplicativos como java, adobe, office e outros, como também gerenciar paches de atualizações do Windows de forma individual, agrupada ou bloquear atualizações específicas;
- Listar atualizações de correção de vulnerabilidades listadas pelo MITRE.
- Gerenciar quais atualizações deverão ser realizadas (apenas importantes, recomendadas...)
- Inventário de Hardware e Software com relatório de registro de alterações, com no mínimo as especificações:
- Nome do Computador;
- Marca/modelo;
- Informações do CPU;
- Velocidade da CPU;
- RAM (Mb);
- Armazenamento total;
- Espaço livre;
- IP externo da máquina;
- Endereço de MAC;
- Endereço de IP;
- Máscara de sub-rede;
- Sistema Operacional instalado na máquina;
- Aplicativos e softwares instalados no computador, com fabricante e versão instalada.
- Controle de dispositivos, com bloqueio da área de transferência, impressoras, removíveis e portas USB.
- Verificação da integridade do HD, com dashard indicativo da “saúde” do componente.

- Solução de acesso remoto básico para quantidade ilimitada de computadores e avançado conforme licenças solicitadas no objeto.

- Possibilidade de execução de scripts em massa através das linguagens PowerShell e Bash para atualização, configuração, instalação ou remoção de softwares, por exemplo.

- Repositório de Scripts para armazenar o histórico de scripts criados pela equipe de TI.

- Biblioteca de scripts pré-configurados, como no mínimo 40 scripts já configurados para uso imediato.

- Permitir o gerenciamento dos dispositivos através de grupos, de forma que facilite a localização de um dispositivo na lista de computadores onde a solução for instalada.

- Opção para gerar alertas automáticos de integridade, com no mínimo as opções:
    - Alterações de hardware;
    - Espaço livre de unidades de disco;
    - Log de eventos do Windows;
    - Logons com falha;
    - Softwares instalados/desinstalados ou atualizados;
    - Status de atualização do S.O Windows;
    - Status do software antimalware;
    - Status do firewall;
    - Status do processo;
    - Status do AutoRun;
    - Status dos serviços do Windows;
    - Tamanho de pasta/arquivo;
    - Taxa de transferência de dados no disco;
    - Taxa de transferência de dados no disco por processo;
    - Temperatura da CPU;

- Temperatura da GPU;
- Uso de CPU por processo;
- Uso da memória RAM por processo;
- Uso da rede por processo;
- Uso geral da CPU;
- Uso geral da memória Ram;
- Uso geral da rede;
- Última reinicialização da estação de trabalho.

- Os alertas de alterações de hardware, espaço em disco, tamanho de pasta/arquivo e última reinicialização do sistema não deverão gerar custo adicional no licenciamento.
- Cada alerta deverá permitir uma personalização da sua severidade, no mínimo: Informativo, Aviso, Erro e Crítico.
- Permitir correção automática através de script remoto.
- Permitir reiniciar a máquina, interromper processo, interromper ou iniciar serviço do Windows automaticamente através do alerta gerado.
- Possuir opção de plano recomendado, já com pacote de alertas pré-configurado pra estações de trabalho.
- Avaliação e relatório de vulnerabilidades listados pela MITRE.

Possibilidade de contratação futura de Prevenção de Perda de Dados integrado na mesma console, que deverá prover:

- Permitir que seja configurado o modo de observação entre: permissão total das transferências de dados confidenciais; justificar tudo, onde aparecerá uma janela de pop-up para justificativa da transferência e misto, quando for um destino externo deverá ser justificado, já o que for interno irá permitir a transferência.

- Permitir que seja configurado o modo de imposição estrita, aplica conforme o fluxo de dados ou a imposição adaptativa com aprendizado.

• Possibilidade de ativar o reconhecimento óptico dos caracteres, através da tecnologia OCT, que permite extrair textos para inspeção de conteúdo de arquivos e imagens.

• Possibilidade de permitir ou bloquear a transferência de dados protegidos por senha.

• Possibilidade de impedir a transferência de dados em caso de erros.

• Possuir lista para permitir determinados dispositivos, independentemente da sensibilidade dos dados e da política de fluxo aplicada sendo eles: armazenamento removível; removível criptografado; unidades mapeadas; área de transferência redirecionada; impressores; MAPI (Outlook); Notas IBM; SMTP; Web Mail; ICQ; Jabber; Skype; Viber; Zoom; Serviços de compartilhamento de arquivos; Redes Sociais; FTP; HTTP; PME.

• Possibilidade de personalizar listas de permissões para hosts remotos e para aplicativos.

• Possuir relatório para análise da transferência dos dados que foram realizadas.

• Possuir relatório com as categorias de dados privados em saída.

• Possuir relatório com identificação dos principais remetentes de dados confidenciais de saída.

• Possuir relatório com identificação dos principais remetentes de dados confidenciais de saída bloqueados.

• Possuir relatório com os eventos recentes.

Recursos adicionais, sem vínculo ao licenciamento (poderão ser instalados em quantidade ilimitada de máquinas):

- Relatório de pontuação de segurança, com no mínimo os itens: Antimalware, backup, firewall, vpn, criptografia de disco e tráfego NTLM.
- Módulo de controle de dispositivo
- Inventário de Hardware com relatório de registro de alterações, com no mínimo as especificações:

- Nome do Computador;
- Marca/modelo;
- Informações do CPU;
- Velocidade da CPU;
- RAM (Mb);
- Armazenamento total;
- Espaço livre;
- IP externo da máquina;
- Endereço de MAC;
- Endereço de IP;
- Máscara de sub-rede;
- Funções padrões do antimalware (proteção de pastas, proteção antimalware, detecção de mineração e quarentena), sem proteção em tempo real, apenas agendada.
- Acesso remoto via RDP e HTML.
- Alertas automáticos de alteração do hardware, espaço em disco, tamanho de arquivos/pastas e última reinicialização da carga de trabalho.

ANDERSON ALVES RIBEIRO
Chefe do Serviço de Informática

JUSTIFICATIVA TÉCNICA DE READEQUAÇÃO DO OBJETO

Este serviço realizou uma prospecção de mercado mais abrangente, identificando soluções tecnológicas que entregam o mesmo nível de segurança exigido (Antivírus EDR, Anti-Ransomware e Backup em Nuvem para os 107 desktops e servidores citados no DFD) com maior eficiência de custo.

Ressaltamos que o contrato atual de antivírus expira em **09/05/2026**. O DFD apresentado assegura a proteção contra crimes cibernéticos e a conformidade com a LGPD dentro de uma realidade financeira responsável.

Ao optar pelo backup em "datacenter próprio da empresa", o objeto deixa de ser uma solução padronizada do fabricante e passa a depender da infraestrutura da contratada. No **Termo de Referência** é prudente exigir:

- **Localização dos Dados:** Onde fisicamente esse datacenter está localizado? (Isso é importante para conformidade com a LGPD).
- **Certificações:** Exigir que o datacenter da empresa possua certificações mínimas (como ISO 27001 ou Tier III) para garantir que os dados da Câmara não fiquem vulneráveis.
- **Disponibilidade (SLA):** Qual a garantia de tempo que o dado estará disponível para restauração? Precisa ter um mínimo de 10 dias de disponibilidade para baixar os arquivos.
- **Portabilidade dos dados (portabilidade e "Lock-in")** ao final do contrato, sem custos adicionais de "egress fees" (taxas de saída), para evitar que a Câmara fique refém de um único fornecedor pelo preço baixo inicial. Precisa ter um mínimo de 10 dias de disponibilidade para baixar os arquivos e a migração dos dados, em caso de troca de fornecedor.

A solução atual utiliza a tecnologia de Marca, mas com armazenamento em nuvem nacional/privada, o que reduz drasticamente o custo de transferência e custódia dos dados.

Observa-se que a solução continua sendo de alta performance (mantendo EDR e Antiransomware), mas que a mudança na arquitetura de armazenamento (de nuvem pública para nuvem privada de parceiro) foi o principal vetor de economicidade, sem piorar a segurança, mas otimizando a forma como o armazenamento é contratado.

Sugere-se que ocorra ampla divulgação do processo de contratação direta para que amplie a competitividade e as empresas orçamentistas e demais do ramo sejam notificadas para apresentação de propostas.

Conclusão:

Diante da reavaliação técnica do objeto e as especificações técnicas essenciais, solicitamos o imediato prosseguimento do processo para contratação.

Atenciosamente,

Anderson Alves Ribeiro
Chefe do Serviço de Informática / Autor do DFD

PROPOSTA COMERCIAL

Alta Floresta - MT, 23 de Abril de 2026

Prezados,

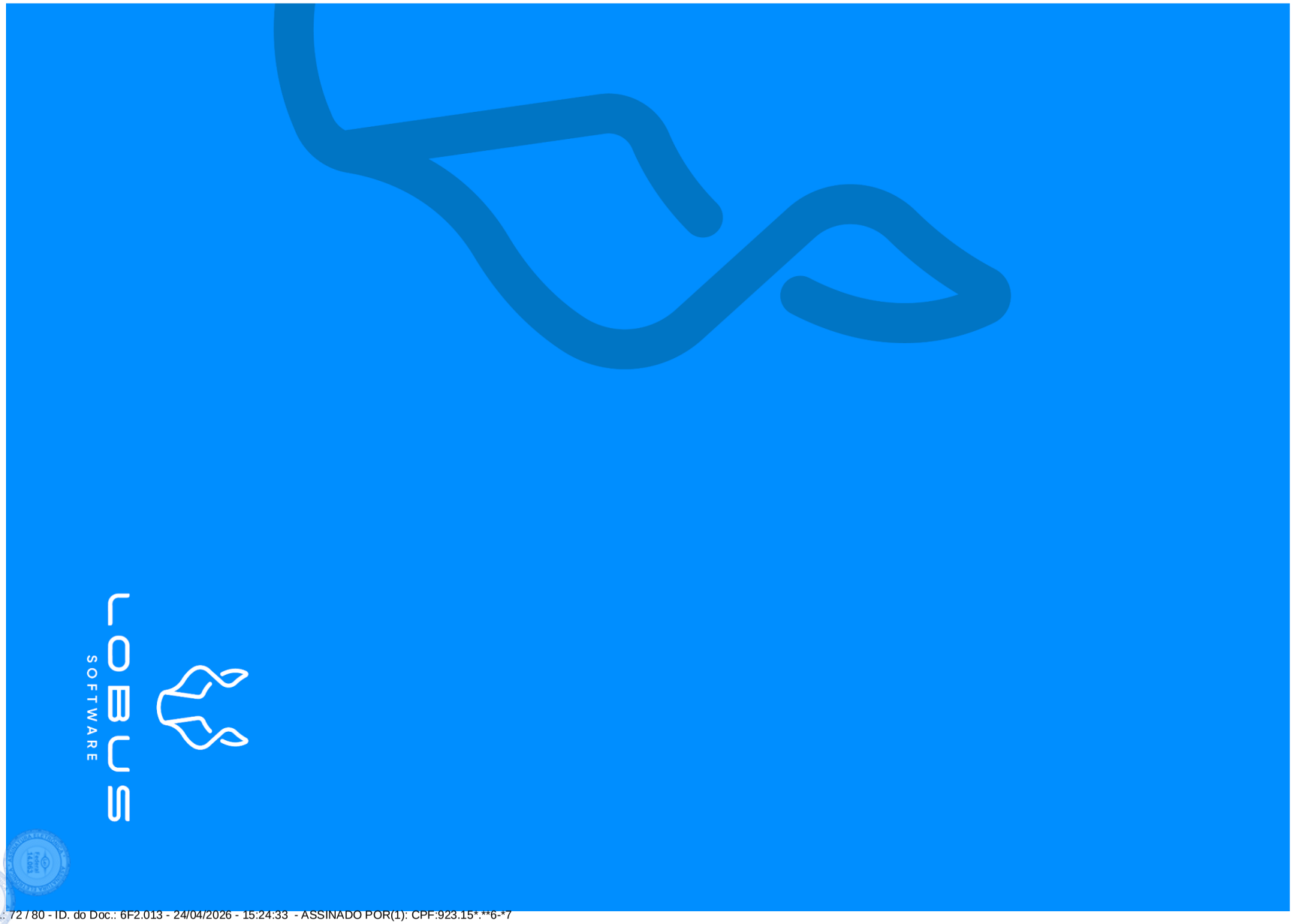
Apresentamos abaixo os valores referente soluções em tecnologia de Backup em nuvem para a Câmara de Unaí - MG.

ITEM	Quantidade GB	Vlr MENSAL	VLR ANUAL
ESPAÇO EM NUVEM	11000	R$ 1.870,00	R$ 22.440,00
SERVIDOR LOCAL	2	R$ 83,00	R$ 996,00
SERVIDOR VM	20	R$ 72,00	R$ 864,00
OFFICE 365	107	R$ 1.556,85	R$ 18.682,22
LICENÇA ANTIVIRUS	165	R$ 585,75	R$ 7.029,00
GERENCIAMENTO DE ATIVOS	165	R$ 1.287,00	R$ 15.444,00
VALOR GLOBAL PAGAMENTO Á VISTA:			**R$ 65.455,22**

Ressaltamos que nosso trabalho consiste também prestação de suporte técnico em informática e ERP em geral. Estamos à disposição para conversarmos mais sobre demais necessidades. **Valido por 60 dias. Pagamento a vista.**

Obrigado pela Oportunidade!

At.te;
Dirceu Henchen
vendashmcservicos@gmail.com
(66) 3521-4067



<Sobre nós/>

Somos uma empresa **nacional** de tecnologia da informação, focada em auxiliar **empresas e administração pública** com soluções de **cibersegurança e comunicação.**

Atuamos em todos os estados brasileiros e também Paraguay com mais de **4.000** usuários dentro das nossas soluções. Nos últimos anos conquistamos de forma muito **séria e comprometida** a autoridade no setor de backup em nuvem com as empresas Backup Dados e Nimbus Software, que hoje se tornaram nossa prestigiada **Lobus Software.**

Onde Estamos

Estamos presente em todo Brasil e também Paraguai

<Conheça nossas soluções/>

Backup

A Garantia dos seus dados armazenados com soluções robustas de backup automático e em nuvem para qualquer tipo de dados.

iopoint

Solução de ponto eletrônico móvel, com reconhecimento facial e gestão em tempo real do quadro de colaboradores.

Central by LogMeIn

Uma visão completa da integridade de cada computador, para detectar problemas críticos, inventário de hardware e atualizações importantes.

Rescue by LogMeIn

Uma solução de suporte remoto segura para seus dispotivos quando e onde quiser. O Rescue da LogMein foi feito para grandes demandas de suporte remoto.

LOBUS SOFTWARE

Mycena

Conecte os colaboradores sem abrir mão da visibilidade e do controle de cada acesso. Salve a senha uma vez, e ela estará protegida e disponivel.

VOIP

A plataforma que transforma a maneira como empresas se conectam com seus clientes. Proporcionando uma abordagem integrada e eficaz para interações comerciais.

PREFEITURA ZAP

Solução de comunicação especialista para órgãos públicos se comunicarem, interagir e ouvir os cidadãos.

CASCAVEL, 22 de abril de 2026.

Prezado Anderson,

Atendendo a sua solicitação, apresentamos uma proposta de solução integrada de tecnologia para atender as expectativas da **Câmara Municipal de Unai - MG** em relação **a contratação** dos serviços de edição e compartilhamento de arquivos.

Colocamos à vossa disposição toda experiência em prestação de serviços de CYBERSEGURANÇA EM NUVEM. Desenvolvemos esta Proposta com o compromisso de oferecer a solução mais aderente às suas necessidades de negócio.

Agradecemos a oportunidade e nos colocamos à sua inteira disposição para eventuais esclarecimentos que forem necessários.

Atenciosamente

Amanda Marcilio
CONSULTORA COMERCIAL

LOBUS SOFTWARE

Acronis

ITEM	QUANT/GB	VALOR MÊS	VALOR ANO
ESPAÇO EM NUVEM	11.000	R$ 1.430,00	R$ 17.160,00
SERVIDOR LOCAL	2	R$ 225,40	R$ 2.704,80
SERVIDOR VM	20	R$ 575,40	R$ 6.904,80
OFFICE 365	107	R$ 1.426,31	R$ 17.115,72
LICENÇA ANTIVIRUS	165	R$ 582,45	R$ 6.989,40
LECENÇA DE GESTÃO AVANÇADA	165	R$ 1.178,10	R$ 14.137,20

VALOR ANUAL Á VISTA APÓS IMPLANTAÇÃO	R$ 65.011,92

PAGAMENTO MENSAL SUJEITO A ACRÉSCIMO DE 10% SOBRE O VALOR DA TABELA Á CIMA, RESULTANDO EM 12 PARCELAS MENSAIS DE R$ 5.959,42 E TOTAL ANUAL DE R$71.513,11.

Validade da proposta: 60 dias.

****valor anual já incluso a implantação**.**

_____

JOCIMAR DA SILVA PEDROSO

<Clientes/>

EMPRESAS QUE CUIDAM DE SEUS DADOS COM ACRONIS

ÓRGÃO PÚBLICOS QUE PROTEGEM SEUS DADOS COM ACRONIS

ÓRGÃOS PÚBLICOS UTILIZANDO O PREFEITURAZAP

lobussoftwareoficial

@lobussoftwareoficial

45 3224 5603 | 0800 591 6677 **Whatsapp**

R. Paraná, 379 - Cascavel - PR
CEP 85813-010

www.**lobussoftware**.com.br

BACKUP JÁ
SEGURANÇA CIBERNÉTICA

Proposta Técnica/Comercial

SERVIÇO DE BACKUP ONLINE

Empresa: Câmara Municipal de Unaí/MG

24/04/2026

Prezado

Atendendo a sua solicitação de, apresentamos uma proposta de solução integrada de tecnologia para atender as expectativas da **Câmara Municipal de Unaí/MG** com relação aos serviços de backup online.

Colocamos à vossa disposição toda experiência de serviços de prestação de serviço de backup ao mercado corporativo. Desenvolvemos esta Proposta com o compromisso de oferecer a solução mais aderente às suas necessidades de negócio.

Agradecemos a oportunidade e nos colocamos à sua inteira disposição para eventuais esclarecimentos que forem necessários.

Atenciosamente,

Philip Obrien
65 99600-1301
philip@backupja.com.br

Proposta Comercial

Neste Capítulo são descritas as Condições Comerciais aplicáveis a esta Proposta. Estas condições serão transcritas para contrato a ser celebrado entre as partes.

Item	Descrição	Qtd	Und	Vlr mensal	Vlr Anual
1	Contratação de **SERVIÇOS TÉCNICOS DE SOLUÇÃO E SEGURANÇA DE PROTEÇÃO DE DADOS EM NUVEM** (cloud computing) com armazenamento em datacenter, incluindo suporte e treinamento e segurança. Composto por 20 servidores virtualizados, e também, 02 Servidores físicos, totalizando uma massa de 11TB.	1	Mês	R$ 2.004,62	R$ 24.055,44
2	Solução de proteção para servidores e estações de trabalho. Totalizando 165 licenças de antivírus, com Anti-Ransomware nativo.	1	Mês	R$ 595,17	R$ 7.142,04
3	Solução de gestão de ativos para estações de trabalhos, servidores e máquinas virtualizadas, totalizando 165 licenças.	1	Mês	R$ 1.287,00	R$ 15.444,00
4	Licença de backup do Office 365 Business em nuvem para 107 seats. **A solução deverá fazer backup dos serviços: (Exchange Online, Teams, Sharepoint e One Driver) de cada usuário sem restrição de espaço**.	1	Mês	R$ 1.562,20	R$ 18.746,40
VALOR GLOBAL ANUAL PAGAMENTO Á VISTA:					R$ 65.387,88

Condições Comerciais e Disposições Gerais

Esta proposta é válida por um período de 60 (trinta) dias contados a partir desta data e estará sujeita a revisão antecipada, caso ocorram mudanças relevantes na atual situação econômica do País, durante esse período, ou sendo adotada qualquer medida econômica que venha a causar desvalorização ou desatualização dos preços ora apresentados.

Philip Obrien

_____

Backup Já

CÂMARA MUNICIPAL DE UNAÍ-MG
Av. José Luiz Adjuto, nº 117, Centro, Unaí - MG, CEP: 38.610-066.
CNPJ:19.783.570/0001-23.

DECLARAÇÃO DE ADEQUAÇÃO ORÇAMENTÁRIA

UNAÍ/MG, 28 de abril de 2026.

Processo n.º 00023.01.01-2026 (ID: 64.1E4)

À Comissão de Apoio às contratações públicas

Declaro que o orçamento do exercício de 2026, conforme relatório anexo, contém saldo suficiente para a contratação de empresa de serviços de segurança cibernética, proteção de dados e gerenciamento de backup e armazenamento de arquivos em nuvem, incluindo implantação, configuração, treinamento e suporte contínuo, conforme especificações e quantidades descritas no termo de referência", com custo total anual estimado de R$65.387,88 (sessenta e cinco mil e trezentos e oitenta e sete reais e oitenta e oito centavos).

A presente despesa deve ser empenhada na seguinte dotação orçamentária: 01.01.00.01.031.1000.2002.3.3.90.40, ficha 15.

Declaro, ainda, que a despesa em questão é compatível com o Plano de Contratação Anual, especificamente com o item 234.

Declaro, por fim, que, após consulta no sistema, não foi localizada aquisição da mesma natureza em 2026, podendo a contratação em tela se dar por dispensa de licitação, sem caracterizar fracionamento de despesa.

Atenciosamente,

Unaí –MG, data da assinatura eletrônica.

_____
Eduardo Henrique Borges
Diretor do Departamento Financeiro
CRC/MG: 084709/0-2

Assinatura do Documento

Documento Assinado Eletronicamente por **EDUARDO HENRIQUE BORGES - DIRETOR DO DEPARTAMENTO FINANCEIRO** , **CPF:** 013.93*.**6-*0 em **28/04/2026 17:43:03**, Cód. Autenticidade da Assinatura: **17X8.6743.703W.X82U.4648**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Informações do Documento

ID do Documento: **6F8.B79** - Tipo de Documento: **DECLARAÇÃO DE ADEQUAÇÃO ORÇAMENTÁRIA**.

Elaborado por **EDUARDO HENRIQUE BORGES**, **CPF:** 013.93*.**6-*0 , em **28/04/2026 17:43:03**, contendo 178 palavras.

Código de Autenticidade deste Documento: 1745.5U43.8032.H134.7518

A autenticidade do documento pode ser conferida no site: **https://zeropapel.unai.mg.leg.br/verdocumento**

UF: MINAS GERAIS
MUNICIPIO: UNAI
28 abr 2026 17:39

ENTIDADE: CAMARA MUNICIPAL

SALDOS DE DOTAÇÃO

FOLHA: 1
Período
01/01/2026
até
28/04/2026

FICHA	NÚMERO DA CONTA	DESCRIÇÃO DA CONTA	FIXADA	CRÉDITOS	REDUÇÕES	RESERVADO	EMPENHADO	ANULADO	SALDO TOTAL
15	01.01.00.01.031.1000.2002.3.3.90.40.00	Serv. de TI e Comunicação - PJ	700.000,00	0,00	0,00	0,00	372.650,92	0,00	327.349,08
	1.500.000.0000	*Recursos não vinculados de Impostos*	*700.000,00*	*0,00*	*0,00*	*0,00*	*372.650,92*	*0,00*	*327.349,08*
		TOTAL GERAL.....:	**700.000,00**	**0,00**	**0,00**	**0,00**	**372.650,92**	**0,00**	**327.349,08**

Assinaturas do Documento

Documento Assinado Eletronicamente por **LAURA EDUARDA BUENO DA CRUZ - MEMBRO DA COMISSÃO PARA ADEQUAÇÃO DA LGPD**, **CPF:** 122.75*.**6-*8 em **29/04/2026 14:59:35**, Cód. Autenticidade da Assinatura: **1481.6X59.435R.2206.7338**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Documento Assinado Eletronicamente por **ANDERSON ALVES RIBEIRO - CHEFE DO SERVIÇO DE INFORMÁTICA**, **CPF:** 923.15*.**6-*7 em **29/04/2026 14:58:16**, Cód. Autenticidade da Assinatura: **1490.0A58.616R.H809.4786**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Documento Assinado Eletronicamente por **CLAUDIANE ALVES DE MELO - MEMBRO DA COMISSÃO DE APOIO ÀS CONTRATAÇÕES PÚBLICAS - CACP**, **CPF:** 083.28*.**6-*0 em **29/04/2026 14:53:31**, Cód. Autenticidade da Assinatura: **14K6.4253.7318.X284.1640**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Informações do Documento

ID do Documento: **6FB.49A** - Tipo de Documento: **ESTUDO TÉCNICO PRELIMINAR - ETP - Nº 6/CACP/2026**.

Elaborado por **CLAUDIANE ALVES DE MELO**, **CPF:** 083.28*.**6-*0 , em **29/04/2026 - 14:53:31**

Código de Autenticidade deste Documento: 14K7.4H53.731V.E642.0065

A autenticidade do documento pode ser conferida no site:
https://zeropapel.unai.mg.leg.br/verdocumento