DESPACHO

UNAÍ/MG, 24 de abril de 2026.

CONSIDERANDO o DFD de ID: Nº 2/SI/2026, bem como a ID: 6F2.013 (ZeroPapel);

CONSIDERANDO a necessidade de contratação de empresa especializada na prestação de serviços técnicos de solução e segurança para proteção de dados e gerenciamento de ativos de TI local e em nuvem adotados pela Câmara Municipal de Unaí, incluindo instalação, configuração, treinamento e suporte;

DEFIRO a inclusão da demanda no PCA 2026, conforme artigo 13 da Portaria 5.400/2024;

DEFIRO a tramitação do pedido constante no DFD de ID: Nº 2/SI/2026, conforme artigo 4º da Resolução nº 618/2024;

REMETO o pedido ao SECOMP para efetuar a inclusão da demanda no PCA 2026 e posteriormente;

DETERMINO a tramitação para a Equipe de Apoio às Contratações Públicas para fins de autuação e enumeração do processo administrativo preparatório, nos moldes da Resolução nº 618/2024.

VEREADOR CARLINHOS DEMOSTENES
Presidente da Câmara Municipal de Unaí

Assinatura do Documento

Documento Assinado Eletronicamente por **CARLOS LYSIAS MOREIRA DE SOUSA - PRESIDENTE - VEREADOR CARLINHOS DEMÓSTENES**, **CPF:** 547.89*.**6-*1 em **24/04/2026 16:17:18**, Cód. Autenticidade da Assinatura: **16W5.6717.7186.X55H.0381**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Informações do Documento

ID do Documento: **6F2.435** - Tipo de Documento: **DESPACHO**.

Elaborado por **BRUNO LEONARDO COSTA NEIVA BRANDÃO**, **CPF:** 012.46*.**6-*6 , em **24/04/2026 - 16:16:54**

Código de Autenticidade deste Documento: 1617.2H16.454K.V707.3677

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

DFD nº 02/2026/SI

Unaí (MG), 24 de abril de 2026.

À Sua Excelência o Senhor
VEREADOR CARLINHOS DEMÓSTENES (PL)
Presidente da Câmara Municipal de Unaí (MG)

DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA (DFD)

1 Fundamento
1.1 Lei Federal nº 14.133/2021.

2 Informações do Requisitante
2.1 Unidade administrativa:
2.2 Responsável pelo **DFD** e **ANEXO:**
Anderson Alves Ribeiro - Chefe do Serviço de Informática

3 Descrição suscinta do produto/serviço demandado
3.1 CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS TÉCNICOS DE SOLUÇÃO E SEGURANÇA DE PROTEÇÃO DE DADOS E GERENCIAMENTO DE ATIVOS DE TI LOCAL E EM NUVEM ADOTADA NA CÂMARA MUNICIPAL DE UNAÍ, INCLUINDO: INSTALAÇÃO, CONFIGURAÇÃO, TREINAMENTO E SUPORTE.

3.2 **TABELA DESCRITIVA E QUANTITATIVA:**

ITEM	DESCRIÇÃO	Qtd.	Und.
01	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 TB** de dados; - **02 Servidores físicos** de Virtualização Hyper-V com **150GB cada**; - **File server** com uma massa de dados de **10 TB**.	12	Mês
02	Solução de proteção para **servidores e estações de trabalho**. Totalizando uma massa de **165 licenças de antivírus**, com Anti-Ransomware nativo.	12	Mês
03	Solução de gestão avançada de ativos para **estações de trabalhos, servidores e máquinas virtualizadas**, totalizando uma massa de **165 licenças**.	12	Mês
04	**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**	12	Mês

AV. JOSÉ LUIZ ADJUTO nº 117 - FONE: (38) 3493-3260 - CEP 38.610-066 – UNAÍ - MG
HOME PAGE: http:// www.unai.mg.leg.br – E-MAIL: camara@unai.mg.leg.br

	espaço.		
05	Implantação, treinamento e suporte.	12	Mês

4 Justificativa e detalhamento da necessidade

4.1 Busca-se implementar serviços de proteção cibernética por meio de uma única plataforma e um único painel, provendo solução e segurança de proteção de dados local e em nuvem e gerenciamento de ativos de ti.

4.2 **Solução de Backup em nuvem:** 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.

4.3 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.

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

4.5 **Solução de Antivírus:** Atualmente 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 de que, o **contrato em vigor está vencendo dia 09/05/2026**.

4.6 **Solução de Gestão Avançada:** Além disso, 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. Solução voltada para departamentos de TI que busca monitorar, gerenciar e proteger endpoints remotamente. Ela utiliza IA para automatizar tarefas, garantindo maior visibilidade e controle sobre hardware e software.

Principais funcionalidades e benefícios:

- **Inventário Detalhado:** Descoberta automática de dispositivos e rastreamento de ativos de hardware e software.
- **Monitoramento Proativo:** Monitoramento em tempo real com alertas inteligentes baseados em autoaprendizagem, cobrindo 24 métricas essenciais.
- **Gestão de Patches e Software:** Automatiza a aplicação de patches e o deploy de softwares.
- **Scripts Automatizados:** Permite automação de tarefas rotineiras, como configuração e manutenção, usando scripts prontos e verificados.
- **Acesso Remoto Seguro:** Ferramentas para suporte remoto e análise de vulnerabilidades.
- **Geolocalização:** Rastreamento em tempo real de ativos.

4.7 Sendo assim, faz-se necessária a contratação de solução integrada que ofereça os serviços de

AV. JOSÉ LUIZ ADJUTO nº 117 - FONE: (38) 3493-3260 - CEP 38.610-066 – UNAÍ - MG
HOME PAGE: http:// www.unai.mg.leg.br – E-MAIL: camara@unai.mg.leg.br

proteção cibernética de segurança e backup em nuvem, com o objetivo de garantir a continuidade das atividades da Câmara, a proteção dos dados institucionais e a conformidade com as boas práticas de governança de tecnologia da informação, alcançando os seguintes objetivos:

- Flexibilidade da solução de backup;
- Armazenamento seguro em nuvem, em ambiente externo ao local físico da Câmara;
- Rapidez na implantação da solução;
- Facilidade e agilidade na recuperação dos dados;
- Ampla proteção contra crimes cibernéticos, incluindo ransomware e malwares avançados;
- Gerenciamento centralizado da segurança dos dispositivos;
- Manutenção, monitoramento e integridade dos equipamentos de informática;
- Garantia da continuidade dos serviços públicos prestados pela Câmara.

5 Resultados pretendidos com a contratação

5.1 A contratação de empresa especializada 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.

5.2 Os principais resultados esperados são:

5.3 **Resiliência e Continuidade do Negócio**

5.4 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.

5.5 **Resultado esperado:** 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.

5.6 **Fortalecimento da Cibersegurança e Defesa Ativa:**

5.7 Através da expansão do licenciamento (de 95 para 163 licenças) e da atualização tecnológica da solução de proteção.

5.8 **Proteção Multicamada:** Bloqueio eficiente contra *ransomware* (sequestro de dados), *malwares* e outras ameaças avançadas que podem paralisar o Legislativo.

5.9 **Controle de Perímetros:** Gestão rigorosa de dispositivos externos e periféricos, reduzindo as portas de entrada para infecções acidentais ou vazamento de informações.

5.10 **Eficiência Operacional e Gestão de Ativos**

5.11 A solução permitirá uma visão 360° do parque tecnológico da Câmara.

5.12 **Inventário Automatizado:** Monitoramento em tempo real do hardware e software, permitindo planejar manutenções preventivas e substituições de equipamentos de forma estratégica.

5.13 **Atualização Centralizada:** Garantir que todos os terminais estejam com as últimas correções de segurança aplicadas (patch management), eliminando vulnerabilidades críticas no sistema.

5.14 **Agilidade na Recuperação de Desastres (Disaster Recovery)**

5.15 A transição para uma solução moderna de backup em nuvem foca na redução do **RTO** (*Recovery Time Objective* - tempo necessário para recuperar um sistema) e do **RPO** (*Recovery Point Objective* - intervalo de dados perdidos).

5.16 **Flexibilidade e Rapidez:** A implantação deverá ser ágil, com configuração otimizada para o ambiente da Câmara, permitindo que a recuperação de arquivos específicos ou de servidores inteiros ocorra com poucos cliques.

5.17 **Transferência de Conhecimento e Capacitação**

5.18 Não basta deter a tecnologia; é preciso domínio sobre ela.

5.19 **Treinamento Técnico:** A contratação prevê o treinamento da TI da Câmara, assegurando que

AV. JOSÉ LUIZ ADJUTO nº 117 - FONE: (38) 3493-3260 - CEP 38.610-066 – UNAÍ - MG
HOME PAGE: http:// www.unai.mg.leg.br – E-MAIL: camara@unai.mg.leg.br

o servidor público esteja apto a operar as ferramentas, monitorar alertas de segurança e realizar restaurações de dados de forma autônoma e segura.

5.20 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.

6 Estimativa do valor e quantidade para aquisição

6.1 O valor estimado, em nível de DFD, deverá ser reavaliado, posteriormente, por meio de sites oficiais de pesquisas de preços e outras técnicas estimativas, para aumentar sua precisão e possibilitar servir como parâmetro ao termo de referência, considerando que, a **presente demanda fundamenta-se em pesquisa de preços composta por 03 (três) orçamentos (anexos) de fornecedores independentes.** Certifica-se que os preços coletados são reais e compatíveis com o mercado. O valor de referência adotado para a confecção do Documento de Formalização de Demanda (DFD) corresponde à proposta de menor montante, visando a otimização dos recursos disponíveis, e servirá apenas como base, como estimativa de preço real, encontrado em empresas especializadas no ramo de atividade específica.

7 Inclusão de itens ao PCA do ano de 2026

7.1 Requer a inclusão de novos itens e aumento de quantitativo de itens ao PCA do ano de 2026, levando em conta a identificação de novas demandas, conforme este Documento de Formalização de Demanda, nos termos da Lei Federal nº 14.133, de 01 de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios, e do art.13 da Portaria n.º 5.400/2024, de 13 de dezembro de 2024, que regulamenta no âmbito da Câmara Municipal de Unaí a elaboração do Plano de Contratações Anual - PCA da Câmara Municipal de Unaí, conforme os itens relacionados na tabela abaixo.

Observação: Há de se considerar que todos os itens abaixo devem ser de **PRIORIDADE ALTA**, sendo necessário a **compra até o dia 09/05/2026**, quando encerra o contrato vigente de antivírus, inclusive com entrega imediata.

OBJETO	JUSTIFICATIVA	UNIDADE	QUANTIDADE	VALOR MENSAL ESTIMADO	VALOR ANUAL ESTIMADO
1. ( ) Material ( ) Serviço ( ) obra (X) outros **Descrição:** Backup File Server em nuvem.	Atualmente a Câmara conta com solução de backup local, sendo necessário solução de backup em nuvem.	GB	11.000	R$ 1.430,00	R$ 17.160,00
2. ( ) Material ( ) Serviço ( ) obra (X) outros **Descrição:** Backup de Servidor Local em nuvem.	Atualmente a Câmara conta com solução de backup local, sendo necessário solução de backup em nuvem.	SERVIDOR	2	R$ 225,40	R$ 2.704,80
3. ( ) Material ( ) Serviço ( ) obra (X) outros **Descrição:**	Atualmente a Câmara conta com solução de backup local, sendo	SERVIDOR	20	R$ 575,40	R$ 6.904,80

AV. JOSÉ LUIZ ADJUTO nº 117 - FONE: (38) 3493-3260 - CEP 38.610-066 – UNAÍ - MG
HOME PAGE: http:// www.unai.mg.leg.br – E-MAIL: camara@unai.mg.leg.br

Backup de Servidor Virtual em nuvem.	necessário solução de backup em nuvem.					
4. ( ) Material ( ) Serviço ( ) obra (X) outros **Descrição:** Backup do OFFICE 365	Atualmente a Câmara conta com solução de backup local, sendo necessário solução de backup em nuvem.	CONTAS	107	R$ 1.426,31	R$ 17.115,72	
5. ( ) Material ( ) Serviço ( ) obra (X) outros **Descrição:** Proteção de Antivírus	Atualmente 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 aumento da quantidade de licenças de 95 para 165, além de que, o contrato em vigor está vencendo dia 09/05/2026.	LICENÇA	165	R$ 582,45	R$ 6.989,40	
6. ( ) Material ( ) Serviço ( ) obra (X) outros **Descrição:** Gestão avançada de ativos.	Justifica-se, pois, estende as capacidades de backup básico e proteção cibernética, focando no gerenciamento proativo, automação e visibilidade de endpoints.	LICENÇA	165	R$ 1.178,10	R$ 14.137,20	
7. ( ) Material (X) Serviço ( ) obra ( ) outros **Descrição:** Implantação, configuração, treinamento e suporte.	É fundamental para garantir a integridade, disponibilidade e segurança dos dados corporativos, alinhando a infraestrutura de TI às exigências atuais de conformidade (LGPD) e proteção contra ransomware.	SERVIÇO **Observação: O valor do serviço já incluso.**	1	R$ 0,00	R$ 0,00	

AV. JOSÉ LUIZ ADJUTO nº 117 - FONE: (38) 3493-3260 - CEP 38.610-066 – UNAÍ - MG
HOME PAGE: http:// www.unai.mg.leg.br – E-MAIL: camara@unai.mg.leg.br

8	**Dotação orçamentária**
8.1	O relatório de saldo de dotação deverá ser juntado ao processo posteriormente para comprovação de que o orçamento da Câmara possui envergadura suficiente para a execução da despesa.
8.2	Levando em consideração a natureza e o valor total estimado, a contratação pretendida será atendida pela seguinte dotação orçamentária: **Órgão:** 01- Câmara Municipal de Unaí **Unidade Orçamentária:** 01.02.00 – Gabinete e Secretaria **Programática:** 01.031.1000.2002 **Fonte de Recursos:** 1.500 **Elementos de despesa:** 3.3.90.40.00 **Ficha:** 15
8	**Requisitos necessários para contratação**
8.1	A contratada dever ser selecionada mediante processo licitatório na modalidade **pregão eletrônico ou compra direta**, considerando o objeto em tela. As soluções a serem ofertadas devem ter especificações técnicas idênticas às do Termo do Referência.
9	**Providências a serem adotas pela administração previamente à contratação**
9.1	Que o processo de contratação obedeça aos trâmites legais da Lei Federal n.º 14.133/2021.
10	**Prazo para vigência do contrato**
10.1	A demanda ora apresentada trata de prestação de serviço continuado, entretanto, a vigência de contratos de prestação de serviços continuados segue regras específicas para garantir a continuidade da atividade administrativa e a vantajosidade econômica.
10.2	Desse modo, levando em consideração a natureza dos serviços almejados, entende- se que o prazo do contrato deve ser celebrado por até 5 (cinco) anos, com possibilidade de prorrogação sucessiva até o limite de 10 (dez) anos, no entanto, para prorrogar, a Administração Pública deve demonstrar a vantajosidade econômica e técnica, além de verificar se os preços permanecem compatíveis com o mercado.
11	**Vinculação ou dependência com outro DFD**
11.1	Não se aplica.
12	**Anexos do DFD**
12.1	Anexo I - Especificações Técnicas e Quantitativos.
12.2	Termo de Referência
12.3	Estudo Técnico Preliminar
12.4	Oçamentos 1, 2 e 3
12	**Considerações finais**
12.1	Solicita-se o deferimento da tramitação do presente pedido por Vossa Excelência.
12.2	Por final, sendo autorizada a tramitação da presente demanda, pede-se o encaminhando deste DFD à Comissão de Apoio às Contratações Públicas para fins de autuação e enumeração do processo administrativo preparatório.
	ANDERSON ALVES RIBEIRO Chefe do Serviço de Informática

AV. JOSÉ LUIZ ADJUTO nº 117 - FONE: (38) 3493-3260 - CEP 38.610-066 – UNAÍ - MG
HOME PAGE: http:// www.unai.mg.leg.br – E-MAIL: camara@unai.mg.leg.br

Assinatura do Documento

Documento Assinado Eletronicamente por **ANDERSON ALVES RIBEIRO - CHEFE DO SERVIÇO DE INFORMÁTICA**, **CPF:** 923.15*.**6-*7 em **24/04/2026 15:24:33**, Cód. Autenticidade da Assinatura: **1564.5324.4339.W47E.7012**, Com fundamento na Lei Nº 14.063, de 23 de Setembro de 2020.

Informações do Documento

ID do Documento: **6F2.013** - Tipo de Documento: **DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA - DFD - Nº 2/SI/2026**.

Elaborado por **ANDERSON ALVES RIBEIRO**, **CPF:** 923.15*.**6-*7 , em **24/04/2026 - 15:24:33**

Código de Autenticidade deste Documento: 15V3.4924.0338.Z288.8352

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

ESPECIFICAÇÕES TÉCNICAS E QUANTITATIVO

OBJETO: Contratação de serviços de proteção cibernética por meio de uma única plataforma e um único painel, provendo solução e segurança de proteção de dados local e em nuvem e gerenciamento de ativos de ti.

1. DA QUANTIDADE

As quantidades a serem contratados seguem no quadro abaixo:

Item	Descrição	Qtd	Und
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 vitualizados totalizando uma massa de **1** TB de dados; - 02 Servidores físicos **de Virtualização Hyper-V com uma massa de 150GB cada**; - 01 File server com uma massa de dados de **10** TB.	12	Mês
2	Solução de proteção para servidores e estações de trabalho. Totalizando uma massa de 165 licenças de antivírus, com Anti-Ransomware nativo.	12	Mês
3	Solução de gestão avançada de ativos para estações de trabalhos, servidores e máquinas virtualizadas, totalizando uma massa de 165 licenças.	12	Mês
4	Licença do backup do Office 365 Business em nuvem com uma massa de 107 Licenças. Microsoft 365 Seats (**unlimited** Hosted Cloud Storage included). **A solução deverá fazer backup dos serviços: (Exchange Online, Teams, Sharepoint e One Driver) de cada usuário sem restrição de espaço**.	12	Mês
5	Implantação, treinamento e suporte.	12	Mês

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 TB de dados, e também, 02 Servidores Físicos de Virtualização Hyper-V com uma massa de 150GB cada, 01 File server com uma massa de dados de 10 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

TERMO DE REFERÊNCIA

A presente licitação tem por objeto a **: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM SERVIÇOS TÉCNICOS DE SOLUÇÃO E SEGURANÇA DE PROTEÇÃO DE DADOS E GERENCIAMENTO DE ATIVOS DE TI EM NUVEM ADOTADA NA CÂMARA MUNICIPAL DE UNAÍ, INCLUINDO: INSTALAÇÃO, CONFIGURAÇÃO E TREINAMENTO, CONFORME CONDIÇÕES E ESPECIFICAÇÕES DESTE TERMO DE REFERÊNCIA,** na modalidade de XXXXXXXXXXX, com o critério de JULGAMENTO das propostas **MENOR PREÇO GLOBAL.**

JUSTIFICATIVA PARA CONTRATAÇÃO

Atualmente a Câmara Municipal de Unaí já 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.

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.

Além disso, 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.

Sendo assim, faz-se necessária a contratação de solução integrada de segurança e backup em nuvem, com o objetivo de garantir a continuidade das atividades da Câmara, a proteção dos dados institucionais e a conformidade com as boas práticas de governança de tecnologia da informação, alcançando os seguintes objetivos:

→ Flexibilidade da solução de backup;
→ Armazenamento seguro em nuvem, em ambiente externo ao local físico da Câmara;
→ Rapidez na implantação da solução;
→ Facilidade e agilidade na recuperação dos dados;
→ Ampla proteção contra crimes cibernéticos, incluindo ransomware e malwares avançados;
→ Gerenciamento centralizado da segurança dos dispositivos;
→ Manutenção, monitoramento e integridade dos equipamentos de informática;
→ Garantia da continuidade dos serviços públicos prestados pela Câmara.

1. PRAZO, LOCAL E FORMA DE ENTREGA.

Os serviços serão executados no Predio da Câmara Municipal de Unaí – CMU, na Avenida José Luiz Adjuto, n.º 117, Centro, Unaí MG, CEP 38.610-066, o telefone para contato dos responsável da T.I da CMU(38) 3493-3260 no ramal 205.

A CONTRATADA deverá prover todo o suporte e gestão da solução ofertada.

É responsabilidade da CONTRATADA monitorar eletronicamente a solução 24x7x365 (vinte e quatro horas, sete dias por semana, 365 dias por ano) para garantia da disponibilidade da mesma.

A solução proposta deverá prever medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, segurança e integridade, prevenindo acesso não autorizado às informações;

Em casos de paralisações dos serviços deve a CONTRATADA iniciar a correção do problema em até 4 (quatro) horas corridas.

O sistema da CONTRATADA será responsável por operar as tarefas de backup de acordo com as solicitações realizadas pelo time da CÂMARA.

A CONTRATADA será responsável em verificar a execução das rotinas e tarefas de backup, rm casos de falha, a CONTRATADA deverá notificar eletronicamente o time da CÂMARA, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.

Em casos de impossibilidade técnica da resolução do erro, a CONTRATADA deve abrir chamado juntamente com o time de administração da CÂMARA para que o erro possa ser solucionado.

A CÂMARA terá direito a um número ilimitado de alterações mensais nas políticas e rotinas vigentes em seu cenário de backup ou proteção sem qualquer custo adicional.

A CONTRATADA deverá enviar semanalmente relatório estatístico das rotinas de backup, proteção e gestão.

A CONTRATA deverá fornecer suporte técnico 8x5 e um número de plantão fora do horário comercial, em língua portuguesa, para sanar dúvidas quanto à solução, sua configuração ou quaisquer outros assuntos relacionados à solução.
O suporte técnico deverá ter os seguintes canais de atendimento:

- Suporte Telefônico;
- E-mail;
- Sistema online de chamados.
- CHAT

O prazo para disponibilização dos serviços para a CÂMARA será de 30 (trinta) dias corridos após a assinatura do contrato.

Antes do início do projeto deverá ser convocada pela CONTRATADA reunião com a equipe técnica da CÂMARA. Serão apresentados os aspectos de concepção do projeto, incluindo rotinas, configurações, políticas, bem como plano de execução dos serviços, detalhando responsáveis, prazos e fases. Novas reuniões poderão ser convocadas por ambas as partes de modo a definir pormenores da solução e eliminar pendências;

Planejamento e descrição dos serviços (ETAPAS)

Planejamento dos serviços a serem executados, visando definir:

- escopo dos serviços
- Equipe envolvida na execução dos serviços
- Cronograma inicial de implementação da solução;
- Objetivo final dos serviços

Acompanhamento da execução dos serviços.

Execução dos serviços

Implementação da solução

- Um especialista da CONTRATADA deverá planejar todas as atividades necessárias e agendar a realização dos serviços em horários mutuamente acordados com a CÂMARA.
- Os serviços ocorrerão durante o horário comercial.

A CONTRATADA deverá disponibilizar checklist de backup, para que CÂMARA preencha o mesmo com os servidores, serviços, bancos, diretórios, storages, agendamentos, prioridades e outras informações pertinentes à configuração das tarefas e rotinas de backup.

Implantação do Serviço

Testes de verificação da instalação, conectividade e redundância de conectividade

Documentação da instalação em relatório de instalação

Configuração das tarefas e rotinas de backup e proteção

A CONTRATADA deverá realizar reunião para demonstração do mapa de rotinas que foi criado a partir do checklist gerado pela CÂMARA.

Em casos de alteração das rotinas ou divergência de entendimentos, o mapa de rotinas será alterado.

Implementação do mapa de rotinas na solução

Execução inicial, de cada tarefa, acompanhada por técnico responsável da CONTRATADA.

Ao término da execução inicial, a CONTRATADA deve submeter seu resultado à aprovação do time da CÂMARA

Sessão de orientação ao cliente

Fornecer orientação à equipe técnica da CÂMARA , em horário combinado, antes da conclusão do serviço, durante o horário de expediente;

Analisar o Relatório de instalação

Aprovação por parte da CÂMARA do relatório final de execução dos serviços.

O prazo de recebimento provisório será de até 1 (dia) dia útil e do recebimento provisório será de até 05 (cinco) dia corrido;

O prazo de entrega será de no máximo 05 (cinco) dias úteis contado a partir da solicitação da câmara, através de empenho ou ordem de compra, encaminhado sempre via e-mail da empresa a qual deverá responder o recebimento do mesmo.

2. VIGÊNCIA

O prazo de vigência da contratação será de 12 (doze) meses, após a data de assinatura da mesma. Podendo ser prorrogado por igual período até o limite de 10 (dez) anos, após a verificação da real necessidade e vantagens para a CÂMARA na continuidade do Contrato, com fundamento no Artigo 105, inciso I, da Lei nº. 14.133/2021.

3. DA QUANTIDADE E VALOR ESTIMADO

As quantidades e valores estimados a serem contratados seguem no quadro abaixo:

Item	Descrição	Qtd	Und	Unitário	Total
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 vitualizados, também 02 Servidores físico File server, totalizando uma massa de dados de 11 TB.	12	Mês	R$ XXX,XX	R$ XXX,XX
2	Solução de proteção para servidores e estações de trabalho. Totalizando uma massa de 165 licenças de antivírus, com antiransomware nativo.	12	Mês	R$ XXX,XX	R$ XXX,XX
3	Solução de gestão de ativos para estações de trabalhos, servidores e máquinas vistualizadas, totalizando uma massa de 165 licenças	12	Mês	R$ XXX,XX	R$ XXX,XX
4	Licença do backup do Office 365 Business em nuvem com uma massa de 107 Licenças	12	Mês	R$ XXX,XX	R$ XXX,XX
5	Implantação, treinamento e suporte.	12	Mês	R$ XXX,XX	R$ XXX,XX

Conforme descrito no quadro acima, o valor estimado será de ***R$ XXX,XX*** (VALOR POR EXTENSO).

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 150GB

cada, 01 File server com uma massa de dados de 11 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.

5. HABILITAÇÃO TÉCNICA

A solução proposta deverá hospedar os dados em datacenter que possua a certificação da NBR ISO/IEC 27001:2013 e classificado no mínimo como TIER III a ser consultada no site da Uptime Institute, além de estar localizado em território nacional, sendo que a comprovação deverá ser apresentada na habilitação;

Após a implantação deverá comprovar mensalmente, atráves de relatório ou outro meio que esta utilizando o datacenter informado na habilitação, ou no mínimo com as certificações exigidas em edital durante toda a vigência do contrato, sob pena de rescisão em caso de uso de datacenter ou armazenamento diferente do informado em sua habilitação.

Deverá ser apresentada quais fabricantes com seus Modelos compõem a solução ofertada.

A CONTRATADA deverá fornecer declação de aptidão técnica de outros órgãos públicos que já atendam com o mesmo serviço, objeto do contrato.

6. OBRIGAÇÕES DA CONTRATADA

Além daquelas determinadas em Leis, Decretos, regulamento e demais dispositivos legais, nas obrigações do fornecedor, também incluem:

a) comunicar a CÂMARA por escrito, no prazo de 48 (quarenta e oito) horas, quaisquer alterações, acontecimentos ou motivos de força maior que impeçam, mesmo que temporariamente, de garantir o fornecimento total ou parcial;

b) cumprir rigorosamente as solicitações e os prazos de entrega descrito neste termo;

c) assumir, os riscos e as despesas decorrentes da prestação dos serviços, bem como, os encargos sociais e trabalhistas necessários à perfeita execução do objeto do contrato;

d) responsabilizar-se por quaisquer acidentes que venham a ser vítimas seus empregados e/ou terceiros, decorrentes do fornecimento;

e) manter, durante todo o período de execução do contrato, as condições de habilitação jurídica, qualificação técnica, qualificação econômico-financeira e regularidade fiscal exigidas para a contratação, sob pena de suspensão do pagamento e/ou rescisão contratual;

f) apresentar na data de assinatura do contrato, nome, endereço e telefone de profissional da empresa para responder pela execução dos serviços;

g) não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o presente contrato, nem subcontratar a prestação a que esta obrigada;

h) utilizar pessoal uniformizado e identificado com crachá, para entrega do material contratado, sendo este de bom comportamento, podendo ser exigida a substituição, cujo comportamento ou capacidade a CONTRATANTE julgue impróprio ao desempenho dos serviços contratados;

i) não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, o presente contrato.

j) manter uma cópia dos dados em um local remoto visando a segurança dos dados em caso de desatre;

k) assegurar a restauração dos dados de forma rápiada e segura;

l) melhoria na qualidade do backup dos dados;

m) replicação do backup em ambiente seguro;

n) ampliação da disponibilidade do backup dos dados (quando necessitar).

m) Deverá apresentar mensalmente, relatório da conta criada para CONTRATANTE que COMPROVE utilização do datacenter apresentado na habilitação ou com as certificações equivalentes, sendo que, se a qualquer momento for constatado uso de datacenter sem as certificações exigidas poderá a CONTRATANTE realizar rescisão unilateral do contrato com direto as multas e penalizações previstas.

7. DO FATURAMENTO E PAGAMENTO

Deverão ser apresentadas nas dependências de cada CÂMARA, as notas fiscais/faturamentos, devendo conter no corpo da nota fiscal as informações a seguir:

a.1) descrição dos materiais, **O NÚMERO DO EMPENHO**, o nome do banco, a agência bancária e o número da conta corrente para depósito do pagamento;

b.2) Juntamente com a Nota Fiscal de Serviço, deverão ser apresentadas as cópias dos seguintes documentos de suporte:

b.2.1 certidão Negativa de Débito – CND do Instituto Nacional de Seguridade Social conjunta com a Certidão Federal -PGFN ;

b.2.2 certificado de Regularidade do FGTS;

b.2.3 certificado de Regularidade dos Débitos Trabalhistas (CNDT);

b.2.4 certificado de Regularidade do Município (se a empresa vencedora for do Município);

b.2.5 cópia do empenho encaminhado para a empresa para agilizar o recebimento.

c) O pagamento será efetuado no 15º (décimo quinto) dia, contado a partir da entrada da Nota Fiscal de Serviços, nas dependências de cada CÂMARA;

d) Quando a documentação para cobrança estiver incompleta e/ou apresentar elementos que a invalide, deverá ser substituída pela CONTRATADA, dispondo a CÂMARA de 08 (oito) dias corridos a partir do recebimento da documentação correta, para análise e pagamento.

8. DAS OBRIGAÇÕES DA CONTRATANTE

a) Efetuar regularmente o pagamento, desde que obedecida às cláusulas e condições estabelecidas;

b) Acompanhar a entrega, podendo recusar qualquer entrega, que não esteja de acordo com as normas ou descrições e/ou verificar se a água nele contido apresente dúvidas quanto a sua pureza;

c) Sustar a execução de qualquer fornecimento que esteja sendo feito em desacordo com o Contrato, normas ou orientação formal.

9. PENALIDADES E RESCISÃO

Conforme determina a Lei. 14.133/21, no caso de atraso na entrega dos produtos parcial ou total conforme as condições fixadas em contratos, salvo se ensejada por motivo de força maior ou caso fortuito, a: CONTRATANTE poderá garantida a prévia defesa, aplicar multa de 1% (um por cento) por dia de atraso, limitado a 10% (dez por cento) do valor da fatura, a ser deduzida do valor a ser pago pela CONTRATANTE, sem prejuízo das demais penalidades contratuais e legais.

10. FISCALIZAÇÃO E ACOMPANHAMENTO

A CONTRATANTE designará para função de gestor do contrato será o Diretor Administrativo, o senhor José Geraldo Ramos e o servidor Anderson Alves Ribeiro, Chefe do Serviço de Informática, designado para acompanhar e fiscalizar a execução do objeto, observando a entrega dos objetos e se as demais obrigações estão sendo cumpridas em conformidades com as condições estabelecidas no contrato, fazendo registro de todas as ocorrências, determinando os representante da CONTRATADA o que for necessário para a reparação de todas as ocorrências ou descumprimento de clausulas observadas, sendo que as decisões e providencias que ultrapassarem o limite de sua competência deverão ser comunicadas ao Departamento de licitação em tempo hábil para a adoção das medidas necessárias.

11. DOTAÇÕES A SEREM UTILIZADAS

O código reduzido para suportar esta despesa é: XXX – Serviços de Informática - RECURSOS LIVRES.

Unaí MG, 06 de abril de 2026.

Quem elaborou o Termo de Referência:

_____
Departamento de Compras

Autorização e ciência do conteúdo deste Termo de Referência:

_____
Diretor Geral

ESTUDO TÉCNICO PRELIMINAR

OBJETO

4.1 Análise da viabilidade técnica e econômica para contratação de serviços de proteção cibernética por meio de uma única plataforma e um único painel, provendo solução e segurança e proteção de dados local e em nuvem e gerenciamento de ativos de ti.

Serviço de backup e armazenamento de arquivos, segurança e proteção de dados para atendimento à Câmara Municipal de Unaí - CMU.

LEGISLAÇÃO

Lei nº 14.133/2021 e a **Instrução Normativa SEGES/ME nº 58/2022**, que dispõe sobre a elaboração do ETP no âmbito da administração pública federal direta, autárquica e fundacional (utilizada como parâmetro de boas práticas para municípios).

I – Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público.

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

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

Atualmente a Câmara possui apenas quatro equipamentos Datacenter que se encontra no mesmo prédio da Câmara, onde os dados estão armazenados, não havendo cópias ou backups dos mesmos. Possui solução de antivírus e proteção contra sequestros de dados e malwares em geral, no entanto, não possui solução para gerenciamento das atualizações e inventário de hardware e software. 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 poder legislativo municipal.

Sendo assim, faz-se necessária a aquisição dos serviços para garantir a continuidade do negócio, alcançando os seguintes objetivos:

a) Flexibilidade da solução de backup;
b) Rapidez na implantação da solução;
c) Facilidade na recuperação dos dados.
d) Ampla proteção contra crimes cibernéticos;

e) Controle dos endereços eletrônicos (sites) acessados pelos servidores.
f) Manutenção e monitoramento da integridade dos equipamentos de informática.

II - Descrição dos requisitos necessários e suficientes à escolha da solução, prevendo critérios e práticas de sustentabilidade.

a) Todas as aplicações e licenças e necessárias à execução do objeto serão fornecidas juntas à solução, devendo ser legítimas. Será inadmissível a utilização de licenças e aplicações pirateadas/craqueadas;

b) A solução deverá estar consoante aos conceitos normativos ISO/IEC 9126 (NBR 13596) quanto à sua Qualidade, mantendo níveis aceitáveis de funcionalidade, confiabilidade, usabilidade, eficiência, manutenibilidade e portabilidade, pelo Setor de TI da Câmara Municipal de Unaí;

c) A execução dos serviços deverá ser feita em paralelo ao funcionamento dos equipamentos que serão atendidos com a solução;

d) Não possuir restrição de uso, estando a solução disponível 24h por dia, 7 dias/semana;

e) Cordialidade durante todo e qualquer atendimento técnico e suporte perante os servidores públicos da instituição;

f) A solução deverá estar disponível 24x7x365 (vinte e quatro horas, sete dias por semana, 365 dias por ano);

g) 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.

2.1. Especificação (detalhamento)

a) A Solução deve proteger o ambiente atual da CÂMARA que é composto por 20 servidores virtualizados totalizando uma massa de 1 TB de dados, 02 Servidores Físicos de Virtualização Hyper-V com uma massa de dados de 150GB cada, e um Servidor de Arquivos com 10 TB de massa de dados. Além de 165 estações de trabalho.

b) O serviço compreende a realização e gerenciamento de backup e armazenamento de arquivos, segurança e proteção de dados, conforme especificações deste documento, incluindo instalação, configuração, treinamento e suporte.

c) A solução proposta deverá prever medidas para garantir a proteção dos dados, antecipando ameaças à privacidade, segurança e integridade, prevenindo acesso não autorizado às informações;

d) A solução deverá contar com sistema responsável por operar as tarefas de backup de acordo com as solicitações realizadas pelo Setor de TI da Câmara Municipal de Unaí-

MG, o qual poderá solicitar e/ou realizar alterações mensais ilimitadas nas políticas e rotinas vigentes em seu cenário de backup ou proteção sem qualquer custo adicional.

e) A solução deverá contar com meios eletrônicos ou humanos de verificação da execução das rotinas e tarefas de backup, em casos de falha, o mesmo deverá notificar eletronicamente o time da Câmara, verificar a causa raiz da falha, e sendo possível a correção, corrigir e executar novamente a tarefa.

f) A solução deverá disponibilizar relatórios periódicos com informações completas sobre os jobs executados e porcentagem de sucesso de backups e restaurações, estatística das rotinas de backup, proteção e gestão.

g) A solução deverá ser entregue como serviço e todos os dados deverão ser armazenados em datacenter externo ao ambiente da Câmara Municipal de Unaí-MG.

h) A solução proposta deverá dispor de console/portal para gerência e execução de backup e restauração de dados em nuvem, com suporte a visualização de todas as rotinas de backup, com opção de gerar relatórios online ou enviar os mesmo por e-mail, bem como funcionalidade completa de backup e restauração através de gerência centralizada;

i) O sistema deve prover quantidade ilimitada de restaurações dos backups efetuados por ele.

j) O tráfego de dados de internet deve ser ilimitado, permitindo a transferência, via funcionalidades de backup e restauração, de volume ilimitado de dados, a criptografia dos dados na armazenagem e na transmissão dos dados, possibilitando a comunicação criptografada e protegida para transferência de dados (HTTPS, VPN ou outros).

k) 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. Deverá, ainda, otimizar a restauração de arquivos individuais.

l) Dos recursos da solução:

i. Permitir replicação de um mesmo dado da origem para vários destinos.

ii. Permitir replicação criptografada.

iii. Possuir proteção Antimalware contra-ataques de Ransomware nativa na ferramenta, com configurações para alertar, bloquear ou até mesmo reverter um ataque de Ransomware utilizando cache da máquina.

iv. Possuir tecnologia de desduplicação de dados, ou seja, não armazenar mais de uma vez dados que sejam duplicados.

v. Deverá possuir backup sintético, ou seja, criar uma imagem a partir dos backups incrementais já armazenados no backup.

vi. Deverá suportar política de disasterrecovery para prevenir perda de dados e uma restauração mais rápida e segura.

vii. Deverá possuir mecanismos que não permitam a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental, por meio de memória não-volátil dedicada a operações de escrita (NVS/NVRAM) ou recurso similar.

viii. A solução deverá validar continuamente de forma automática a integridade lógica dos dados, "ponteiros" e índices armazenados no hardware com correção automática das falhas encontradas, de forma a garantir a consistência de todo o conteúdo em sua total capacidade.

ix. Possibilitar predefinir arquivos, pastas ou tipos de arquivos que não devem fazer parte dos backups mesmo quando backup da máquina toda;

x. Deverá possuir interface de administração GUI.

xi. O sistema de armazenamento de backup deverá ser escalável conforme a necessidade da Administração.

xii. Backup sintético otimizado (funcionalidade que permite criar uma imagem full, a partir dos backups incrementais, sem movimentação de dados);

xiii. Deverá prover o envio de alertas e relatórios através de e-mail, de modo automático, manual ou programado.

xiv. 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 prefencialmente sem necessidade de instalação de agentes na máquina virtual. Para Banco de Dados sendo eles Oracle, SQL Server, MySQL, com instalação de agente.

xv. A solução de backup a ser ofertada deverá atender integralmente os requisitos especificados neste Estudo, 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.

xvi. Deverá permitir o backup e restore de arquivos abertos, garantindo a integridade do backup.

xvii. Deverá ter compatibilidade com aplicações, bancos de dados e sistemas de arquivos (File System).

xviii. Deverá possuir capacidade de estabelecer níveis de acesso diferenciados e configuráveis para atividades de administração e operação do software de backup.

xix. Deverá permitir:

a. a programação de tarefas de backup automatizadas em que sejam definidos prazos de retenção dos arquivos personalizáveis.

b. a programação de jobs de backup automatizadas em que sejam definidos prazos de retenção das imagens.

c. a realização do backup completo de servidor para recuperação de desastres.

d. restaurar o backup de recuperação de desastres para hardware diferente do original.

xx. Deverá ser capaz de recuperar dados individuais ou em lote para servidores diferentes do equipamento de origem.

xxi. Deverá possuir a função de Disk Staging, ou seja, que permita o envio dos dados para disco e posteriormente do disco para outro tipo de mídia (disco ou fita).

xxii. Deverá permitir integração do controle de acesso com sistemas de diretório Active Directory.

xxiii. 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.

xxiv. Para servidores Windows, deverá ser possível a recuperação das imagens de recuperação de desastres em um hardware ou em ambiente virtual.

xxv. Deverá permitir a verificação da integridade dos dados armazenados através de algoritmos de checksum e/ou autocorreção.

xxvi. 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.

xxvii. Deverá possuir mecanismo de auditoria, permitindo a emissão de relatórios.

xxviii. Deverá possuir capacidade de resumo de tarefas de backup com falha, e de reiniciar os backups a partir do ponto de falha, após a ocorrência da mesma.

xxix. Relatórios para verificar o nível de serviço, ou seja, visualização de que aplicações estão com políticas de backup ativadas e executadas periodicamente.

xxx. Base de dados de relatórios para suportar armazenamento de dados históricos superior a 30 dias.

xxxi. Deverá suportar o uso da funcionalidade CBT (ChangeBlockTracking) para as operações de backup.

xxxii. Máquinas Virtuais:

a. Deverá permitir o descobrimento automático das máquinas virtuais nos ambientes VMWare e Hyper-V, XenServer.

b. 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.

c. Deverá prover otimização do backup e recursos, permitindo que somente blocos utilizados sejam copiados no processo de backup.

d. Deverá possuir capacidade de realizar backup de maneira off-host, sem a necessidade de instalação de agentes nas máquinas virtuais.

e. Deverá possuir capacidade de realizar backup de máquinas virtuais em estado online ou off-line.

f. Deverá possuir a capacidade de realizar backup On-Host e Off-host das máquinas virtuais Windows.

xxxiii. Deverá possuir a capacidade de realizar backup de maneira Full, Incremental ou Diferencial.

xxxiv. Deverá suportar ambientes configurados com Cluster Shared Volumes.

xxxv. Deve implementar backup utilizando Microsoft Volume Shadow Copy Service (VSS).

xxxvi. A solução deverá possuir recursos básicos de segurança como ant-malware e avaliação de vulnerabilidade sistemas operacionais e aplicativos visto que 60% dos vazamentos de dados estão relacionados a falhas em aplicativos;

xxxvii. O acesso ao portal de gestão deverá possibilitar acesso com autenticação múltiplofator via aplicativos de autenticação, sms ou e-mail.

m) Do Agente (Aplicação cliente)

i. A solução deverá contar com aplicação que será instalada nas máquinas para que possa ser realizada a coleta de dados, denominada “Agente”.

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

a. MySQL

b. Microsoft SQL Server

c. ORACLE

d. PostgreSQL

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

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

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

a. VMware,

b. Hyper-V,

c. XenServer,

d. Windows Server

e. Linux

vi. Os mesmos Agentes de backup deverão possuir recurso de acesso remoto aos computadores permitindo assim uma maior facilidade ao suporte;

vii. Os mesmos Agentes de backup deverão realizar inventário de hardware que serão acessados e auditados pela equipe técnica da Câmara, sem custo adicional.

2.2. Vigência contratual

A demanda ora apresentada trata de prestação de serviço continuado, como backup e armazenamento em nuvem, a Lei nº 14.133/2021 permite, no Art. 106, impõe regras específicas para garantir a continuidade da atividade administrativa e a vantajosidade econômica.

Desse modo, levando em consideração a natureza dos serviços almejados, entende- se que o prazo do contrato deve ser celebrado por até 5 (cinco) anos, com possibilidade de prorrogação sucessiva até o limite de 10 (dez) anos, no entanto, para prorrogar, a Administração Pública deve demonstrar a vantajosidade econômica e técnica, além de verificar se os preços permanecem compatíveis com o mercado.

2.3. Necessidade de treinamento de pessoal

Compreende a realização de capacitação do profissional da área de Tecnologia da Informação.

Esta capacitação visa o repasse de conhecimento prático da utilização do sistema de acordo com a realidade do departamento, com demonstrações efetivas e didática simplificada, de forma a demonstrar todas as funcionalidades que a solução possui, até mesmo as que não tiverem sido solicitadas ou especificadas no item II deste estudo, sanando todas as dúvidas dos colaboradores usuários do software.

O conteúdo programático dos treinamentos ou cursos de capacitação deve prever todas as funções necessárias para a correta operação, utilização, implantação, configuração, parametrização, gerenciamento e administração das funções e acessos. O treinamento deverá ocorrer no setor de TI localizado na Sede do Legislativo Municipal de Unaí e deverá ser pré-agendado com o responsável do departamento.

III - Levantamento de mercado, que consiste na prospecção e análise das alternativas possíveis de soluções, podendo, entre outras opções:

a) ser consideradas contratações similares feitas por outros órgãos e entidades, com objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendam às necessidades da administração; e

b) ser realizada consulta audiência pública ou diálogo transparente com potenciais contratadas, para coleta de contribuições.

Em minuciosa busca às alternativas diversas existentes no mercado, foram consideradas as seguintes alternativas:

> **1.** Treinamento dos Servidores do Município que atuam na área de Tecnologia da Informação, no sentido de que se capacitem, para que criem o software objeto da necessidade apresentada. A opção apresentada é uma boa medida, no entanto, esbarra na dificuldade temporal, pois o processo de capacitação é lento, e não tem garantia do retorno imediato, por ser uma atividade cientifica e intelectual. Ademais, o espaço para o armazenamento dos dados em nuvem precisaria ser adquirido por terceirização;
>
> **2.** Contratação de empresa com know how para criação de softwares que atendam às necessidades elencadas no objeto, a contratação é eficaz no que diz respeito a qualidade, pois, os softwares serão criados exclusivamente para o Município, no entanto essa contratação deixa de ser vantajosa devido ao alto custo para sua criação e desenvolvimento;
>
> **3.** Contratação de empresa que locará os softwares que atenderão as necessidades colocadas no objeto, a contratação é eficaz e vantajosa, devido a experiência da empresa adquirida por meio de contratações feitas por outros órgãos públicos e privados, e também pelo valor pois a locação se mostra menos custosa.

IV - Descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso, acompanhada das justificativas técnica e econômica da escolha do tipo de solução

Em minuciosa busca às alternativas diversas existentes no mercado, não fora identificado melhor solução para que atenda aos interesses e necessidades da Administração senão a contratação de empresa especializada na prestação de serviços de locação de programa para backup e armazenamento de arquivos, segurança e proteção de dados,

mediante a realização de procedimento competitivo pela modalidade Pregão Eletrônico, considerando os itens apontados em tópico específico deste relatório de viabilidade.

A solução como um todo contempla a realização de procedimento licitatório na modalidade Pregão Eletrônico, para a contratação de serviços de backup e armazenamento de arquivos, segurança e proteção de dados, contando com software gerenciador de backups, recursos de acesso remoto, realização de inventário de hardware, 150 licenças de software antivírus e 3,5TB de armazenamento em nuvem, com suporte técnico durante os dias úteis e em horário comercial e telefone de plantão para os demais dias e horários, implantação, treinamento e migração dos dados já armazenados no DATACENTER. Toda a solução operará 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, para atender às necessidades da Câmara Municipal de Unaí, mormente ao Setor de TI do município, aperfeiçoando as práticas de Segurança da Informação, contribuindo com o cumprimento à LGPD, com a gestão do parque tecnológico e na proteção contra crimes cibernéticos.

V - Estimativa das quantidades a serem contratadas, acompanhada das memórias de cálculo e dos documentos que lhe dão suporte, considerando a interdependência com outras contratações, de modo a possibilitar economia de escala

A estimativa das necessidades programadas para a atual contratação levou em consideração a análise de espaço utilizado do atual servidor de dados DATACENTER, já prevendo a otimização e a inclusão de novos dados no servidor, visto que este será o local mais seguro para manter as informações da Câmara Municipal de Unaí, suas Secretarias e Unidades Administrativas.

Assim, o Setor de TI avaliou que a solução deverá ter capacidade de armazenamento de 3,5TB (três terabytes e meio), com 1 (uma) licença de Servidor e 150 (cento e cinquenta) licenças de segurança (antivírus).

VI - Estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a administração optar por preservar o seu sigilo até a conclusão da licitação.

A pesquisa de mercado será obtida pelo Setor de Compras posteriormente à elaboração do Termo de Referência.

A estimativa do valor da contratação está fundamentada através de contratações similares realizadas por outras entidades públicas que se encontram anexo a este Estudo. Os custos expressos foram devidamente aprovados pela autoridade superior.

VII - justificativas para o parcelamento ou não da solução, se aplicável

O processo será realizado através de julgamento global, por ser a melhor forma de atendimento às necessidades do município e a forma economicamente mais viável, tendo em vista que se tratando de um conjunto o valor dos serviços tende a ser menor. Desta forma, a contratação em estudo caracteriza-se por um sistema único e integrado.

VIII - contratações correlatas e/ou interdependentes

Não há contratações correlatas ou interdependentes.

IX - demonstração do alinhamento entre a contratação e o planejamento do órgão ou entidade, identificando a previsão no Plano Anual de Contratações ou, se for o caso, justificando a ausência de previsão.

A futura contratação está devidamente alinhada com o Plano Plurianual do Município. O Município encontra-se em fase de elaboração do Plano de Contratações Anual para o exercício de 2026, de acordo com a Lei Federal nº 14.133/2021, a qual o Município já está utilizando.

X - resultados pretendidos, em termos de efetividade e de desenvolvimento nacional sustentável.

Espera-se que a presente contratação supra as necessidades da Câmara Municipal de Unaí, suas Unidades Administrativas e as Secretarias Municipais no que tange à realização de backup e armazenamento de arquivos, segurança e proteção de dados, gerenciamento dos recursos de tecnologia do munícipio, visto que a contratação apresentada no presente documento de análise de viabilidade é serviço fundamental para a segurança das informações do município e a perca ou vazamento dos mesmo geraria enormes prejuízos e transtornos à Administração.

Por fim, com a utilização do Pregão Eletrônico para presente aquisição, espera-se que a disputa de preço entre as licitantes proporcione uma aquisição de qualidade pelo custo mais vantajoso à Administração.

XI - providências a serem adotadas pela administração previamente à celebração do contrato, inclusive quanto à capacitação de servidores ou de empregados para fiscalização e gestão contratual ou adequação do ambiente da organização

Não há necessidade de adequações na estrutura do órgão.

XII - possíveis impactos ambientais e respectivas medidas de tratamento

Certo é que o planejamento e execução dos procedimentos licitatórios devem sempre ser motivados com vistas à redução do consumo, análise da produção, distribuição, uso e disposição, o que determinará a vantajosidade econômica da proposta, estimulando assim os fornecedores a proporcionarem ao mercado produtos e serviços sustentáveis e que, de certa forma, fomentem a inovação com o uso racional de produtos com menor impacto ambiental negativo.

Neste sentido, analisando o objeto da presente demanda para esta perspectiva, não vislumbramos a possibilidade de impactos ambientais negativos em decorrência da aquisição desta solução.

XIII – Gerenciamento de risco **AÇÕES MITIGADORAS**

PLANEJAMENTO

Instrução Processual Deficitária	Disseminação e Uso das boas práticas de Seleção do Fornecedor

PRODUÇÃO

Pedidos de esclarecimentos/impugnações ao Edital que alterem o Instrumento Convocatório	Ajuste e republicação do Edital
Apresentação de Recurso	Reabertura do certame, com aproveitamento de todos os atos não comprometidos.
Empresa recusar a assinar o Instrumento Contratual	Abertura de processo de sanção

Instauração de novo procedimento para os serviços.

EXECUÇÃO TÉCNICA DO CONTRATO

Descumprimento de cláusulas contratuais	Fiscalização preventiva e ostensiva da entrega dos materiais

Abertura de Processo de Sanção

No caso de atraso superior ao aceitável conforme definição contratual, Rescisão.

PROPOSTA COMERCIAL

Alta Floresta - MT, 23 de Abril de 2026

Prezados,

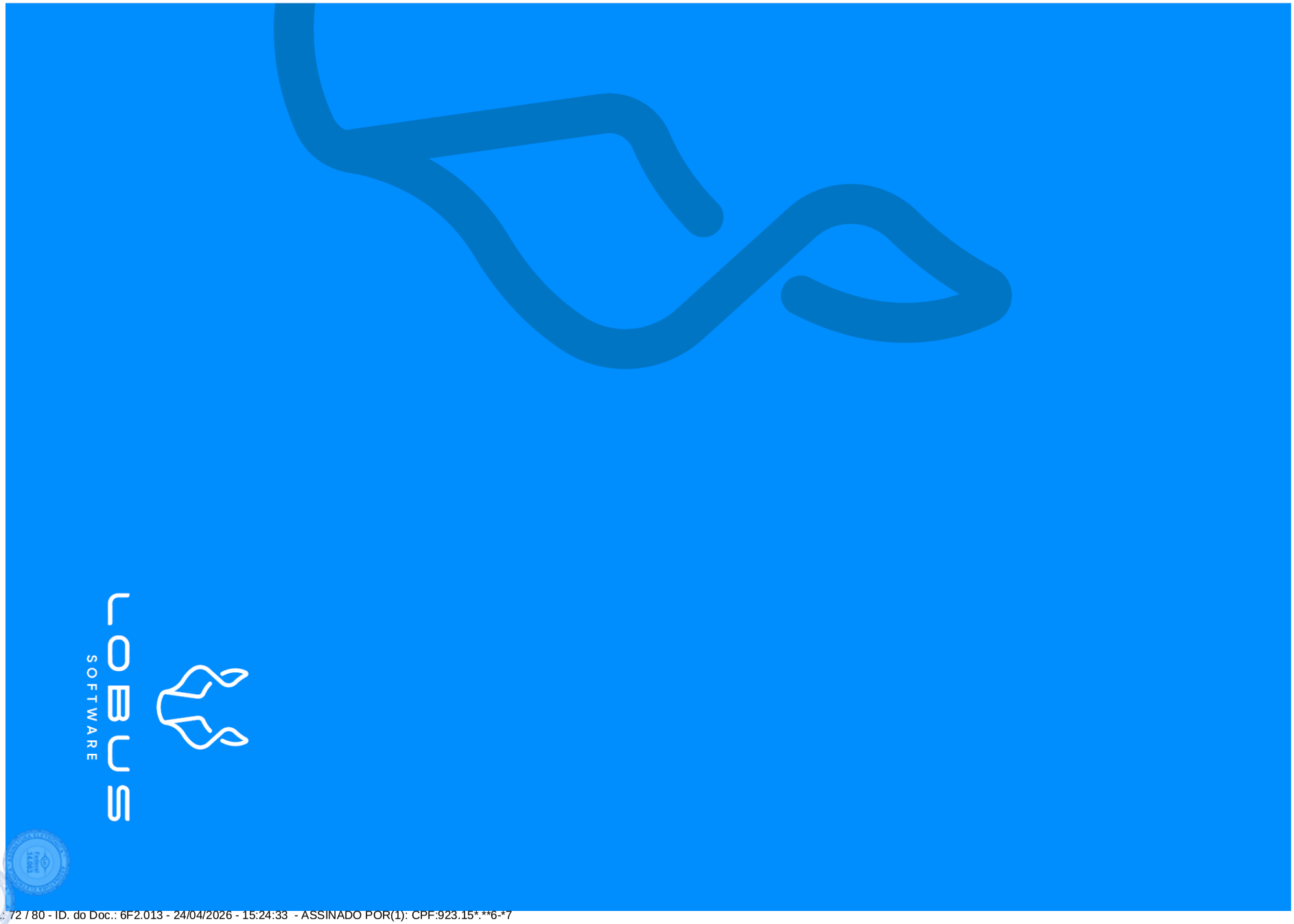
Apresentamos abaixo os valores referente soluções em tecnologia de Backup em nuvem para a Câmara de Unaí - MG.

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


LOBUS
SOFTWARE

<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

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

Consultoria Contábil RIR · CONSTRUCAL Acabamento & Construção · ATACADO · Lanali · ArtPedra
Pallus · ESTRADA · ESTERICAP · Geriba Alimentos · Anjos Colchões & Sofás
BIONOVA Energia Solar · INDEPENDÊNCIA · PLUMA · FAS Gestão Empresarial · PLUSMAQ
TM Balanças · STÜRMER · gênesis · CONSTRUCERTO Materiais de Construção · Clube FM

ÓRGÃO PÚBLICOS QUE PROTEGEM SEUS DADOS COM ACRONIS

PREFEITURA DE CIANORTE · Prefeitura Municipal de FIGUEIRÃO · Prefeitura Municipal de CARDOSO Cardoso não pode parar · Câmara Municipal de LUCAS DO RIO VERDE · CÂMARA MUNICIPAL DE SÃO GABRIEL DA PALHA ESPÍRITO SANTO
PREFEITURA OURO PRETO O futuro é feito agora · PREFEITURA DE ITARIRI · PREFEITURA MUNICIPAL DE CORDEIRÓPOLIS · PREFEITURA MUNICIPAL DE OSVALDO CRUZ · AREAL PREFEITURA
CÂMARA MUNICIPAL de Mogi Guaçu · Prefeitura Municipal de Horizontina · CÂMARA MUNICIPAL DE CRISTALINA · CÂMARA MUNICIPAL DE TAQUARITINGA · CÂMARA MUNICIPAL DE PAULÍNIA
ALTO PARAÍSO DE GOIÁS CÂMARA MUNICIPAL · Fontoura Xavier · PREFEITURA DE NOVA CANTU · PREFEITURA DE CAPITÃO · NOVA MUTUM PREFEITURA

ÓRGÃOS PÚBLICOS UTILIZANDO O PREFEITURAZAP

SEMUT NATAL · PREFEITURA DE STO ANTONIO DO MONTE · PREFEITURA DE NOVA PETRÓPOLIS · Prefeitura de Brochier · PREFEITURA DE MATÃO
SEDEC BLUMENAU · PREFEITURA DE JACAREZINHO · SEMMACC GOIATUBA · Município de CAMPO MOURÃO · PREFEITURA DE ITAQUIRAÍ cuidando da nossa Gente
PREFEITURA DE CAMANDUCAIA · PREFEITURA DE NOVA AURORA · PREFEITURA MUNICIPAL DE MACATUBA · PREFEITURA DE ITAPUÍ · PREFEITURA DE ILHOTA
PREFEITURA MUNICIPAL DE VERA CRUZ/RS · PREFEITURA DE SÃO GABRIEL DA PALHA · PREFEITURA DE CHAPADÃO DO SUL UMA CIDADE BEM MELHOR · Prefeitura de DUMONT - SP · PREFEITURA DE IPORÃ DO OESTE

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