AVISO DE DISPENSA DE LICITAÇÃO 028/2025

O MUNICÍPIO DE CACIQUE DOBLE - RS, torna pública a abertura da Dispensa de Licitação nº 009/2025, de acordo com o Art. 75, inciso II, da Lei nº 14.133/2021 objetivando a **contratação de uma solução de Licença de Proteção de EndPoint (Antivírus), incluindo os serviços de instalação, configuração e suporte técnico presencial, visando proteger os dispositivos da Prefeitura Municipal de Cacique Doble/RS,** de acordo com o Termo de Referência, disponível no site oficial: https://caciquedoble.rs.gov.br.

Interessados podem apresentar propostas até às 17h do dia 03 de Junho de 2025, através do e-mail adm@caciquedoble.rs.gov.br ou entregar em mãos no setor de Licitações do Município, até as 17h.

Mais informações: fone (54) 3552 - 1244, e-mail: adm@caciquedoble.rs.gov.br

Cacique Doble/RS, 29 de maio de 2025.

Márcio Caprini
Prefeito Municipal

Processo Geral nº056/2025

DISPENSA DE LICITAÇÃO Nº 028.2025

TERMO DE REFERÊNCIA

1. DEFINIÇÃO DO OBJETO E VALORES DE REFERÊNCIA

1.1. Contratação de uma solução de Proteção de EndPoint (Antivírus), visa proteger dispositivos da Prefeitura municipal de Cacique Doble/RS. As soluções devem proporcionar segurança, desempenho e escalabilidade adequados às necessidades da administração pública, com foco em proteção contra uma ampla gama de ameaças avançadas bem como o gerenciamento centralizado e alta disponibilidade.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. A contratação que ora se pretende realizar está integralmente fundamentada no Estudo Técnico Preliminar – ETP em anexo, o qual detalhou minuciosamente os requisitos necessários e outros elementos pertinentes ao objeto, fazendo-se integral referência ao mesmo.

2.2. Fundamenta-se também na lei 14.133/2021, art. 75, II.

3. REQUISITOS DA CONTRATAÇÃO

3.1. A contratação será realizada por meio de dispensa de licitação, com critério de julgamento por menor preço global.

3.2. Para o fornecimento o município estará aberto ao recebimento de propostas adicionais.

3.3. A empresa deverá fornecer os seguintes serviços:

3.3.1. A instalação, configuração, manutenção e suporte técnico deverá se iniciar a partir da assinatura do contrato. Os serviços deverão ser prestados exclusivamente pela contratada, (ficando vedado a subcontratação de outra prestadora de serviço),

na modalidade on-site (presencial) em todos os setores da Prefeitura Municipal de Cacique Doble/RS devendo ser realizada exclusivamente por técnicos especialistas.

3.3.2. Chamados técnicos poderão ser abertos em regime 8x5, via internet, chamada telefônica local ou discagem direta, caracterizando a abertura do chamado. Este momento será considerado o início para a contagem dos prazos estabelecidos;

3.3.3. Os chamados serão registrados pela Contratada e deverão estar disponíveis para acompanhamento pela equipe da Administração Municipal, contendo data e hora da chamada, o problema ocorrido, a solução, data e hora de conclusão;

3.3.4. Os atendimentos aos chamados obrigatoriamente deverão ser realizados por profissionais certificados e deverão ser realizados presencialmente sempre que solicitado pela Administração pública, sendo que a solução para o problema, caso seja atribuída aos equipamentos descritos, deverá ser alcançada em no máximo 24 (vinte e quatro) horas corridas após a abertura do chamado técnico;

3.3.5. Deverá a contratada apresentar ao CONTRATANTE a certificação do profissional que irá prestar o suporte, certificação esta que deverá estar vigente durante a vigência do contrato.

3.3.6. É vedado a subcontratação de outra empresa para realização dos trabalhos.

Item 1: Solução de Antivirus

Especificações Técnicas Mínimas

Requisitos Gerais

- Tipo de Solução: Software de proteção de endpoints com capacidades de proteção contra ameaças cibernéticas e gerenciamento de segurança.
- Tipo de Licenciamento: Licença por usuário/dispositivo ou baseado em subscrição, conforme o número de endpoints a serem protegidos.
- Modelo de Implementação: Solução baseada em nuvem com gerenciamento centralizado e possibilidade de integração com infraestrutura local se necessário.
- Parceria com o Fabricante: A contratada deve ser parceira do fabricante da solução, o que indica que a contratada possui habilidades comprovadas com a

solução.

3. Certificações Requeridas

A contratada deve possuir em seu quadro de funcionários, no mínimo um profissional com as seguintes certificações:

- Fortinet NSE 4 Network Security Professional: Exigida para assegurar que o fornecedor possui conhecimento e habilidades para integrar a solução proposta com produtos da Fortinet, garantindo uma proteção abrangente e eficaz da rede.
- FCA - Fortinet Certified Associate in Cybersecurity: Necessária para confirmar que o fornecedor possui uma base sólida em segurança cibernética, essencial para a integração e suporte da solução de proteção com a infraestrutura de segurança existente da Fortinet.
- Certificação de Produtos Kaspersky Next: Exigida para garantir que o fornecedor tem a habilidade para analisar as configurações atuais do produto Kaspersky Next, que é a solução atual da prefeitura, e realizar a remoção adequada do produto, se necessário.
- Cloud Tech Professional: Exigida para garantir que o fornecedor tenha uma compreensão avançada das soluções de backup e recuperação em nuvem, essenciais para a proteção e recuperação de dados.
- Cloud Tech Associate Disaster Recovery: Necessária para assegurar que o fornecedor pode implementar e gerenciar eficazmente as soluções de recuperação de desastres, garantindo a continuidade dos negócios em caso de falhas ou incidentes críticos.
- Cloud Tech XDR: A certificação em XDR é fundamental para o profissional responsável pela contratação de soluções de antivírus, pois garante expertise em integrar e analisar dados de diversas fontes, como endpoints, redes, e-mails, servidores e aplicativos em nuvem. Essas integrações permitem uma resposta mais rápida e eficaz contra ameaças cibernéticas, assegurando a melhor escolha para proteger a administração pública.

4. Funcionalidades Principais

1. Proteção Contra Ameaças:

o Antivírus e Antimalware: Detecção e remoção de vírus, malware,

ransomware e outras ameaças cibernéticas.

o Proteção em Tempo Real: Monitoramento contínuo de atividades suspeitas e bloqueio automático de ameaças.

o Filtragem de Conteúdo Web: Bloqueio de sites maliciosos e controle de acesso à internet.

o XDR (Extended Detection and Response): Capacidade de fornecer uma visão integrada de eventos de segurança e resposta a ameaças, correlacionando dados de múltiplas fontes (endpoints, rede, e-mail, etc.) para detectar e mitigar ameaças complexas e persistentes.

2. Detecção Comportamental Avançada:

o Mecanismo de Detecção Baseado em Inteligência Artificial: Tecnologia que utiliza IA para identificar e prevenir malware, ransomware e ataques de dia zero através da análise comportamental dos endpoints e sistemas.

o Prevenção de Ameaças Desconhecidas: Capacidade de detectar e bloquear ameaças que não são identificadas por assinaturas tradicionais, usando análise comportamental e heurística.

3. Gerenciamento de Patches:

o Atualização Automática de Patches: Implementação automática de atualizações e patches de segurança para sistemas operacionais e aplicativos, garantindo que as vulnerabilidades sejam corrigidas prontamente.

4. Controle de Dispositivos:

o Gerenciamento de Dispositivos Externos: Controle e monitoramento de dispositivos externos conectados aos endpoints, como USBs e dispositivos de armazenamento, para prevenir vazamentos de dados e introdução de malware.

5. Prevenção Contra Vazamento de Dados (DLP):

o Recursos de DLP: Capacidade de implementar políticas de prevenção contra vazamento de dados para proteger informações sensíveis e evitar o envio não autorizado de dados fora da organização.

6. Isolamento de Endpoints:

o Mecanismo de Isolamento: Possibilidade de configurar o isolamento dos endpoints na rede de forma manual ou automática. Isso inclui a capacidade de

colocar um endpoint em quarentena ou restringir seu acesso à rede em resposta a comportamentos suspeitos ou confirmações de infecção, garantindo uma resposta rápida a incidentes e minimizando a propagação de ameaças.

7. Gerenciamento e Relatórios:

o Console de Gerenciamento Centralizado: Interface intuitiva para administração e configuração de políticas de proteção em todos os endpoints.

o Relatórios e Alertas: Geração de relatórios detalhados sobre status de proteção, eventos de segurança e atividades de segurança. Configuração de alertas para atividades suspeitas e falhas de segurança.

8. Integração com Ferramentas de Segurança Adicionais:

o Integração com Perception-Point: Possibilidade de integrar a solução com a ferramenta de proteção de e-mail da Perception-Point (Advanced Email Security) para fornecer uma camada adicional de proteção contra ameaças de e-mail, como phishing e malware.

9. Conformidade e Segurança:

o Gerenciamento de Patches: Reiterado, confirmando sua importância.

o Conformidade com Regulamentações: Suporte a regulamentações de proteção de dados, como LGPD, GDPR, entre outros.

10. Suporte aos Sistemas/Aplicativos/Virtualizadores:

o Compatibilidade: A solução deve suportar uma ampla gama de sistemas operacionais, aplicativos e hipervisores, garantindo que se adapte ao ambiente tecnológico existente.

11. Recuperação de Arquivos e Notificações de Ameaças:

o Resposta a Incidentes de Antimalware: O software deve ser capaz de gerar alertas em tempo real quando um arquivo suspeito for detectado. Além disso, deve interromper imediatamente o processo relacionado ao arquivo malicioso e reverter quaisquer alterações feitas pelo arquivo utilizando o cache de serviços. Isso garante que o sistema seja restaurado ao seu estado seguro anterior à infecção.

12. Suporte e Atendimento:

o Suporte Técnico: Disponibilidade de suporte técnico 24/7 para resolução de problemas e assistência técnica durante todo o período da licença da solução. Com

tempo máximo admitido para atendimento presencial de 1 (uma) hora.

o A contratada deverá auxiliar a equipe de TI da prefeitura na investigação, resolução e documentação de eventuais incidentes relacionados à solução, incluindo assistência na análise e resolução de problemas e na elaboração de relatórios sobre incidentes e ações corretivas.

o Canais de Contato: A contratada deverá oferecer vários canais de contato com a equipe de TI da prefeitura, incluindo um portal de chamados (helpdesk), e-mail e telefones. Esses canais devem estar disponíveis para garantir uma comunicação eficiente e rápida resolução de problemas.

13. Tempo do atendimento presencial: A empresa contratada deverá prestar suporte técnico de forma presencial, sempre que solicitada, em um prazo máximo de 1 hora, contados a abertura do chamado, sem custos adicionais a contratante. Esta exigência visa assegurar a eficiência e a qualidade do atendimento

• O fornecedor deve realizar a instalação, configuração e teste do equipamento na sede da Prefeitura no máximo em 24horas após a assinatura do contrato, de forma presencial e sem custos adicionais para administração pública.

• Treinamento para a equipe técnica da Prefeitura sobre as funcionalidades e administração da solução.

• Equipe Certificada: A contratada deve possuir em seu quadro de funcionários, no mínimo um profissional certificado pelo fabricante na categoria "Professional" para gerenciar e operar o equipamento.

• Suporte às Demandas de Configuração: A contratada deverá atender todas as demandas de configuração relacionadas ao equipamento solicitadas pelo profissional de TI da Prefeitura.

4. MODELO DE GESTÃO DO CONTRATO

4.1. A gestão do contrato será feita pelo Secretário da Administração, e a fiscalização do objeto pela servidora Janaina Reginato.

5. CRITÉRIOS DE ENTREGA E DE PAGAMENTO

5.1. A entrega dos serviços deverá se dar de forma gradativa, a iniciar em até 05

dias da assinatura do contrato.

5.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser ajustados imediatamente quando evidenciadas as falhas pela fiscal do contrato, às custas da contratada, sem prejuízo da aplicação das penalidades.

5.3. A nota fiscal/fatura emitida pelo fornecedor deverá conter, em local de fácil visualização, a indicação do número do processo, número do processo de dispensa e do contrato, a fim de se acelerar o trâmite de recebimento do material e posterior liberação do documento fiscal para pagamento.

5.4. O pagamento deverá ser efetuado, em uma única vez, após a instalação dos antivirus, mediante apresentação de nota fiscal.

5.5 O prazo de vigência da presente **contratação será de 12 meses**, tendo em vista o periodo de licenciamento do antivirus.

6. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR/PRESTADOR DE SERVIÇO

6.1. Será adquirido do fornecedor apresentar a proposta com menor valor, desde que detenha os seguintes documentos de habilitação:

Habilitação Jurídica:

a.1) No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.

a.2) Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br.

a.3) No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores.

a.4) Inscrição no Registro Público de Empresas Mercantis onde opera com

averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência.

a.5) No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores.

a.6) No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei no 5.764, de 1971.

a.7) No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização.

b) Regularidade Fiscal:

b.1) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ);

b.2) Cédula de identidade do(s) diretor(es)ou proprietário(s);

b.3) Certidão Negativa ou Positiva com efeitos de negativa, de Débitos Relativos aos Tributos Federais e a Dívida Ativa da União, emitida pela Receita federal do Brasil;

b.4) Certidão que prove a regularidade para com a Fazenda Estadual, relativa ao domicílio ou sede do licitante;

b.5) Certidão que prove a regularidade para com a Fazenda Municipal da jurisdição fiscal do estabelecimento licitante; e,

b.6) Certificado de Regularidade do FGTS (CRF) perante o Fundo de Garantia do Tempo de Serviço.

c) Regularidade Trabalhista:

c.1) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei no 5.452, de 1° de maio de 1943 (Certidão Negativa de Débitos Trabalhistas), em seu prazo de validade.

d) Qualificação Econômico-Financeira:

d.1) Certidão Negativa de Falência ou Recuperação Judicial expedida pelo

Distribuidor da sede da pessoa jurídica, com data de expedição não superior a 60 (sessenta) dias da data designada para a apresentação do documento.

e) Qualificação Técnica:

e.1) Atestado de Capacidade Técnica emitida por pessoa jurídica de direito público, firmando que o licitante prestou ou presta serviços de Locação de Firewall e Serviço de licenciamento de antivírus, e que cumpriu/cumpre com as obrigações assumidas, fornecido por no mínimo 02 (duas) instituições;

e.2) A empresa licitante deverá possui em seu quadro funcional no mínimo 1 (um) profissional com formação em Segurança da Informação (junto com comprovante de especialização de nível superior na área - no mínimo pós-graduação), que será o responsável técnico pelos serviços contratados;

e.3) 1 (um) profissional com formação em CyberSecurity (junto com comprovante de especialização de nível superior na área - no mínimo pós-graduação);

e.4) Prova de vínculo dos profissionais, com a empresa licitante, caso não possua vínculo societário, deverá apresentar a Carteira de Trabalho e Previdência Social (CTPS) com o devido registro do empregado.

e.5) A licitante deverá indicar um responsável técnico dos serviços, de segurança virtual, devendo conter no mínimo: treinamentos em: CompTIA Security + 2, CCNA Cisco Cyberops 2, Gestão de Identidade e Acesso, Sistemas de Detecção e Prevenção de Intrusão, comprovando sua qualificação através de Certificado e/ou atestado de conclusão de cursos relacionados acima.

f) Demais Documentos:

e.1.) Declaração Conjunta, assinada pelo proprietário ou representante legal, dando ciência de que cumpre plenamente os requisitos de habilitação; que não está impedida de licitar e contratar com a Administração Pública; que atende ao disposto no artigo 7°, inciso XXXIII, da Constituição Federal, e inciso VI do art. 68 da Lei nº 14.133, de 2021; que não possui em seu quadro societário servidor público da ativa ou empregada de empresa pública ou de sociedade de economia mista; que são verdadeiras as informações, estando ciente das sanções impostas, conforme disposto neste Edital e no art. 299 do Código Penal, na

hipótese de falsidade da presente declaração; e, que se vencedora do processo licitatório, possui disponibilidade para realizar a entrega dos produtos no prazo previsto).

6.2. A documentação citada no item 7 deverá ser enviada juntamente com a proposta até o dia 03/06/2025 para o email adm@caciquedoble.rs.gov.br ou entregue pessoalmente no Setor de Licitações do Município.

7. PROPOSTA DE PREÇO/COTAÇÃO:

7.1. As propostas de preço que não estiverem em consonância com as exigências deste certame serão desconsideradas, julgando-se pela desclassificação.

7.2. O preço ofertado não poderão exceder o constantes neste Aviso, devendo obedecer ao valor estipulado pela Administração.

7.3. No valor da proposta deverão estar inclusos todo e qualquer custo extra oriundo da contratação, inclusive tributos, impostos e valores para deslocamento para prestação do serviço.

7.4. Caso o Município não receba nenhuma proposta adicional após transcorrido o prazo previsto neste Aviso de Dispensa, o mesmo poderá contratar com o orçamento de menor valor apurado na fase inicial do processso, desde que a empresa apresente toda documentação de habilitação exigida neste aviso.

8. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

8.1. O valor máximo total aceito é de R$ 11.830,00.

9. OBRIGAÇÕES DO CONTRATADO

9.1. São obrigações da empresa contratada:

9.1.1. Fornecer licenças de antivírus compatíveis com as necessidades da Administração;

9.1.2. Realizar a instalação e configuração da solução em todos os dispositivos indicados;

9.1.3. Disponibilizar suporte técnico presencial e remoto durante a vigência do contrato;

9.1.4. Entregar relatório de ativação, cobertura, desempenho e conformidade;

9.1.5. Garantir alta disponibilidade e gerenciamento centralizado da solução;

9.1.6. Treinar, quando solicitado, equipe técnica da Prefeitura para uso básico da ferramenta;

9.1.7. Manter confidencialidade sobre as informações institucionais acessadas;

9.1.8. Atender a todas as obrigações trabalhistas, fiscais e previdenciárias incidentes sobre sua equipe.

10. DAS OBRIGAÇÕES DO CONTRATANTE

10.1. São Obrigações do Município:

10.1.1. Disponibilizar os dispositivos e ambientes para instalação do software;

10.1.2. Acompanhar tecnicamente a execução dos serviços;

10.1.3. Realizar os pagamentos conforme condições pactuadas;

10.1.4. Designar servidor responsável pelo acompanhamento e fiscalização: Joceli Paim Zorzan.

11. DAS SANÇÕES ADMINSITRATIVAS

11.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

11.1.1. Dar causa à inexecução parcial do contrato;

11.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

11.1.3. Dar causa à inexecução total do contrato;

11.1.4. Deixar de entregar a documentação exigida para a contratação direta;

11.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

11.1.7. ensejar o retardamento da execução ou da entrega do objeto da contratação direta sem motivo justificado;

11.1.8. apresentar declaração ou documentação falsa exigida para a contratação direta ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

11.1.9. fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

11.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

11.1.10.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

11.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste para a contrataçãodireta. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

11.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 11.1.1 e seguintes deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

b) Multa de até 30% (trinta por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor, por qualquer das infrações supracitadas;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 11.1.1 e seguintes deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 11.1.1 e seguintes, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

11.3. Na aplicação das sanções serão considerados:

11.3.1. a natureza e a gravidade da infração cometida;

11.3.2. as peculiaridades do caso concreto;

11.3.3. as circunstâncias agravantes ou atenuantes;

11.3.4. os danos que dela provierem para a Administração Pública;

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

11.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

11.5. A aplicação das sanções previstas neste Aviso de Contratação Direta, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

11.6. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

11.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133, de 2021, e subsidiariamente na Lei nº 9.784, de 1999.

12. CLÁUSULA DÉCIMA TERCEIRA – DAS OBRIGAÇÕES PERTINENTES Á LGPD.

12.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

12.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

12.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei. 9.4 É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

13. DOTAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Municipal, decorrente da seguinte dotação:

03-01 – Secretaria da Administração
2009 – Manutenção secretaria administração
339040- Serviço tecnologia informação
77 redu.

Conforme a demanda apresentada pelas secretarias as dotações deverão ser retiradas, considerando elas alternarem pelos locais escolhidos.

Cacique Doble-RS, 29 de Maio de 2025.

Joceli Paim Zorzan
Secretária Municipal de Administração