

**ESTUDO TÉCNICO PRELIMINAR – ETP.****1.DA INTRODUÇÃO E DO OBJETO SUGERIDO NO DFD**

1.1. O presente documento constitui a primeira etapa da fase de planejamento da contratação, em conformidade com o disposto no art. 18 e art. 40 da Lei nº 14.133/2021, e apresenta os estudos técnicos preliminares necessários para a contratação de solução que atenderá à necessidade especificada a seguir. O objetivo principal do estudo técnico preliminar é analisar, de forma detalhada, a necessidade a ser suprida, avaliar as alternativas disponíveis no mercado e identificar a solução mais eficiente, econômica e vantajosa para a Administração Pública.

1.2. O presente estudo visa subsidiar a tomada de decisão e demonstrar a viabilidade técnica, econômica e ambiental da contratação, considerando ainda os riscos envolvidos, os resultados esperados e os impactos decorrentes da contratação. Tais elementos são essenciais para a elaboração adequada do Termo de Referência e para a garantia da eficiência do processo licitatório.

**1.3. DO OBJETO SUGERIDO NO DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA-DFD:** CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE CIBERSEGURANÇA, INCLUINDO A REALIZAÇÃO DE TESTES DE INTRUSÃO (PENTEST) E DEMAIS SERVIÇOS TÉCNICOS ESPECIALIZADOS VOLTADOS À IDENTIFICAÇÃO, ANÁLISE E MITIGAÇÃO DE VULNERABILIDADES, VISANDO GARANTIR A SEGURANÇA DOS SISTEMAS, DADOS E INFRAESTRUTURA TECNOLÓGICA DAS DIVERSAS SECRETARIA DO MUNICIPIO DE FRECHEIRINHA/CE.

**2. DA LEGISLAÇÃO APLICÁVEL E DA PREVISÃO NO PLANO DE CONTRATAÇÃO ANUAL**

2.1. As disposições legais que nortearão este documento serão detalhadas na fundamentação legal a seguir e orientarão a aplicação das seguintes premissas:

- a) Lei Nº 14.133, de 1º de abril de 2021 - Normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;
- b) DECRETO MUNICIPAL Nº 002/2024, DE 02 DE JANEIRO DE 2024, que regulamenta a Nova Lei de Licitações no âmbito Municipal;
- c) Lei Complementar 123/06, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte e suas alterações;
- d) Lei 12.846/2013, que dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências;
- e) Lei nº 8.078, de 1990 – Código de defesa do Consumidor;
- f) Demais legislação aplicável ao objeto.

2.2. A presente contratação não está prevista no Plano de Contratações Anual formalmente estabelecido para o ano de 2025, em face de sua ausência. A ausência deste plano, entretanto, não impede o avanço de projetos essenciais que se alinham com os objetivos estratégicos de longo prazo da Administração. A contratação tem previsão na Lei Orçamentária Anual Vigente para o exercício financeiro de 2025.

### **3. DA(S) UNIDADE ADMINISTRATIVA(S) DEMANDANTE(S) E DA EQUIPE DE PLANEJAMENTO DESIGNADA:**

3.1. SECRETARIA DE ADMINISTRAÇÃO

3.2. SECRETARIA DE EDUCAÇÃO

3.3. SECRETARIA DE SAÚDE

3.4. SECRETARIA DO TRABALHO E ASSISTÊNCIA SOCIAL.

3.5. A equipe de planejamento responsável pela presente contratação é composta pelos seguintes agentes públicos, designados conforme portaria anexada aos autos do processo: **Sr. Pedro Tiago Ximenes da Silva**, matrícula nº 61419; **Sra. Antônio Maicon Serafim da Silva**, matrícula nº 61519.

### **4. DA DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO, CONSIDERADO O PROBLEMA A SER RESOLVIDO SOB A PERSPECTIVA DO INTERESSE PÚBLICO (art.6º, INC. I do anexo II do decreto municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024)**

4.1. A transformação digital e a ampliação do uso de tecnologias da informação no âmbito das diversas secretarias do Município de Frecheirinha/CE têm proporcionado avanços significativos na eficiência da gestão pública e na qualidade dos serviços oferecidos à população. No entanto, esse progresso tecnológico também acarreta um aumento exponencial dos riscos relacionados à segurança da informação, dada a crescente complexidade e sofisticação dos ataques cibernéticos, que podem comprometer sistemas críticos, dados sensíveis e a infraestrutura tecnológica municipal.

4.2. Neste contexto, torna-se imprescindível a adoção de medidas robustas e especializadas para garantir a proteção dos ativos digitais do município. A contratação de empresa especializada em serviços de cibersegurança, incluindo a execução de testes de intrusão (PENTEST) e outras atividades técnicas voltadas à identificação, análise e mitigação de vulnerabilidades, é essencial para fortalecer a defesa contra ameaças internas e externas, assegurando a confidencialidade, integridade e disponibilidade das informações governamentais.

4.3. Os testes de intrusão, conhecidos como PENTESTS, constituem uma prática consolidada e reconhecida internacionalmente, que consiste na simulação controlada de ataques cibernéticos visando detectar brechas e falhas de segurança nos sistemas, redes e aplicações utilizadas pela administração pública. Por meio desses testes, é possível antecipar possíveis pontos de exploração por agentes mal-intencionados, o que permite a correção tempestiva das vulnerabilidades antes que sejam efetivamente exploradas, reduzindo o risco de incidentes

graves que possam comprometer a continuidade dos serviços públicos, a imagem institucional e a segurança dos dados dos cidadãos.

4.4. Além disso, a legislação brasileira, incluindo a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD), impõe obrigações claras às entidades públicas para a proteção dos dados pessoais e sensíveis sob sua guarda, exigindo a implementação de medidas técnicas e administrativas eficazes contra acessos não autorizados e incidentes de segurança. A contratação dos serviços especializados está alinhada a essas exigências legais, evidenciando o compromisso do Município de Frecheirinha com a governança digital responsável e a proteção dos direitos dos cidadãos.

4.5. Outro aspecto relevante é a constante evolução das ameaças cibernéticas, que demanda a atualização contínua dos conhecimentos técnicos e a utilização de metodologias avançadas para a identificação das vulnerabilidades. Empresas especializadas possuem expertise, ferramentas e processos certificados que garantem a qualidade, eficiência e segurança das análises e intervenções, aspectos que dificilmente poderiam ser assegurados com a estrutura interna do município, que geralmente conta com recursos limitados para a área de segurança da informação.

4.6. Por fim, a contratação dos serviços de cibersegurança reforça o compromisso da gestão municipal com a modernização tecnológica, a segurança dos sistemas públicos e a proteção das informações, promovendo um ambiente digital confiável, resiliente e apto a atender às demandas da população de forma segura e eficiente.

4.7. Diante do exposto, conclui-se que a contratação de empresa especializada em cibersegurança, com foco em testes de intrusão e demais serviços técnicos para identificação e mitigação de vulnerabilidades, é medida imprescindível para garantir a segurança dos sistemas, dados e infraestrutura tecnológica das diversas secretarias do Município de Frecheirinha/CE, alinhando-se às melhores práticas do setor e às exigências legais vigentes.

## **5. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO (Art.6º, Inc. II do Anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024)**

5.1. Para atender às necessidades das diversas secretarias do Município de Frecheirinha/CE na proteção dos sistemas, dados e infraestrutura tecnológica, a contratação deverá contemplar serviços especializados em cibersegurança, com foco na realização de testes de intrusão (pentest) e avaliação abrangente das vulnerabilidades presentes no ambiente tecnológico.

### **REQUISITOS FUNCIONAIS DA SOLUÇÃO:**

- Execução de testes de penetração (pentest) nas modalidades externa (redes e sistemas acessíveis pela internet) e interna (rede corporativa), com possibilidade de acesso remoto via VPN, contemplando as abordagens black-box, Gray-box e White-box;
- Análise detalhada dos processos de gestão de tecnologia da informação, incluindo gestão de mudanças, incidentes, identidade e acessos, e controle de ativos;
- Revisão das configurações de segurança de sistemas operacionais, servidores (WEB, DNS, arquivos, domínio), equipamentos de rede (firewalls, switches, roteadores, access points), bancos de dados e serviços associados;

- Auditoria de logs, registros de eventos e controle de acesso para detecção de atividades suspeitas ou não autorizadas;
- Avaliação da segurança física das instalações, com análise dos controles de acesso, monitoramento por vídeo e segurança do data center;
- Verificação da segurança das comunicações, incluindo protocolos SSL/TLS, criptografia, certificados digitais, APIs e mecanismos de integração;
- Identificação de riscos relacionados a ataques do tipo DoS e DDoS, com recomendações para mitigação;
- Produção de relatórios técnicos detalhados contendo vulnerabilidades encontradas, classificação de riscos, probabilidade de exploração e sugestões de controles mitigatórios.

#### **REQUISITOS TÉCNICOS E DE SEGURANÇA:**

- Capacidade para execução das diferentes modalidades de pentest (black-box, Gray-box, White-box), conforme necessidade do Município;
- Utilização de metodologias atualizadas e reconhecidas internacionalmente para avaliação de vulnerabilidades e testes de intrusão;
- Conformidade rigorosa com a Lei Geral de Proteção de Dados (LGPD) e demais legislações aplicáveis;
- Garantia de sigilo e confidencialidade das informações acessadas durante os serviços;
- Emissão de documentação técnica clara e precisa, que permita a tomada de decisão para a mitigação de riscos.

#### **REQUISITOS OPERACIONAIS E DE SUPORTE:**

- Disponibilização de suporte técnico durante e após a execução dos serviços;
- Definição e cumprimento de cronograma detalhado para realização dos testes e análises;
- Flexibilidade para atuação nos ambientes tecnológicos das diversas secretarias, incluindo acessos remotos autorizados;
- Monitoramento contínuo e acompanhamento das ações corretivas recomendadas.

#### **REQUISITOS LEGAIS E DE CONFORMIDADE:**

- Comprovação de experiência técnica através de atestados emitidos por entidades públicas ou privadas, preferencialmente com atuação no setor público;
- Disponibilidade de equipe técnica certificada nas áreas de segurança da informação, testes de intrusão e gestão de vulnerabilidades;
- Atendimento às normas vigentes relacionadas à segurança cibernética e proteção de dados;
- Capacidade técnica e operacional para garantir a segurança, integridade e disponibilidade dos sistemas do Município.

5.2. Os serviços objeto desta contratação são classificados como serviços técnicos especializados, conforme o art. 6º, inciso XIII, da Lei Federal nº 14.133/2021, por envolverem a prestação de atividades específicas voltadas à identificação, análise e mitigação de vulnerabilidades em sistemas, redes e infraestrutura tecnológica, com desempenho mensurável por meio de relatórios técnicos e laudos.



5.2.1. Embora baseados em metodologias padronizadas para testes de intrusão (pentest) e avaliação de segurança, a correta execução dos serviços exige capacidade técnica qualificada por parte da empresa contratada, devido à complexidade e abrangência dos sistemas tecnológicos das diversas secretarias municipais. Por isso, a Administração exigirá que a contratada mantenha equipe técnica especializada, com profissionais certificados em segurança da informação, além de preposto formalmente designado e responsável técnico com formação superior na área de Tecnologia da Informação ou correlatas, garantindo a qualidade, segurança e continuidade dos serviços.

5.2.2. A exigência de experiência comprovada mínima de dois anos em execução contínua de serviços de cibersegurança, incluindo testes de penetração e gestão de vulnerabilidades, fundamenta-se nos princípios da eficiência administrativa (arts. 5º e 11 da Lei nº 14.133/2021), mitigação de riscos contratuais e seleção da proposta mais vantajosa para a Administração Pública (Decreto Municipal nº 002/2024). Essa qualificação técnica objetiva assegurar a execução satisfatória dos serviços, conforme previsto no art. 67 da Lei nº 14.133/2021.

5.2.3. Considerando que o objeto desta contratação é a prestação de serviços de pentest (testes de intrusão) e demais avaliações técnicas especializadas voltadas à identificação, análise e mitigação de vulnerabilidades, a exigência de manutenção de estrutura técnica contínua será avaliada conforme o escopo previsto no contrato. Para os serviços pontuais de pentest, a contratada deverá dispor de equipe técnica qualificada e capacitada para a execução dos testes e elaboração dos relatórios, garantindo o cumprimento dos prazos e a qualidade dos serviços prestados. Caso o contrato contemple serviços adicionais de suporte, monitoramento ou gestão contínua de vulnerabilidades, será exigida estrutura técnica adequada para atendimento e supervisão durante toda a vigência contratual, assegurando a continuidade e eficiência das ações de segurança da informação.

### **5.3.1. COMPROVAÇÃO DE CAPACIDADE TÉCNICA OPERACIONAL:**

5.3.1.1. A comprovação da aptidão técnica da licitante deverá ocorrer mediante a apresentação de atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) de forma inequívoca a execução prévia de serviços compatíveis em natureza, complexidade e vulto com o objeto licitado, especialmente relacionados à prestação de serviços de cibersegurança, testes de intrusão (pentest), análise e mitigação de vulnerabilidades em sistemas e infraestrutura tecnológica.

Em todos os casos, o(s) atestado(s) apresentado(s) deverá(ão) conter, no mínimo:

- Razão social, CNPJ e identificação da entidade emitente;
- Identificação do serviço executado, com descrição clara e objetiva compatível com o item correspondente da licitação;
- Período de execução e local de realização dos serviços;
- Declaração de que os serviços foram prestados a contento, de forma satisfatória;
- Assinatura e identificação do responsável pela emissão.

5.3.1.2. Em relação ao atestado de capacidade técnica emitido por pessoa jurídica de direito Privado, o agente de contratação só aceitará os atestados/declarações emitida por empresas públicas, sociedades de economia mista e fundações público e/ou privadas, as quais se

qualificam notoriamente como pessoas jurídicas de Direito Privado, ou seja, que possuem compatibilidade com o objeto da licitação (Projeto Básico/Termo de Referência).

5.3.1.3. Por tratar-se de serviços técnicos especializados que podem ser executados em caráter pontual ou periódico, os atestados de capacidade técnica referidos no item 5.3.1.1 deverão comprovar que a licitante realizou serviços similares no mínimo nos últimos 12 (doze) meses, comprovando sua experiência, capacidade técnica e conhecimento atualizado na área de segurança da informação e testes de intrusão. Essa exigência visa assegurar a idoneidade e expertise da licitante na prestação de serviços compatíveis com o objeto da contratação, conforme previsto no art. 67 da Lei nº 14.133/2021.

### **5.3.2. COMPROVAÇÃO DE CAPACIDADE TÉCNICA PROFISSIONAL**

5.3.2.1. A licitante deverá apresentar a identificação da equipe técnica pertencente ao seu quadro permanente, composta por profissionais devidamente qualificados e com disponibilidade para a execução do objeto contratual. A equipe mínima exigida será composta por:

**a.1) 01 (um) Analista de Segurança da Informação**, com certificações reconhecidas (CEH, CISSP, CISM) e comprovada experiência em testes de intrusão (pentest), análise e mitigação de vulnerabilidades, alinhado às melhores práticas de segurança da informação

**a.2) 01 (um) profissional certificado em Governança e Conformidade em Segurança da Informação**, com conhecimento atualizado da Lei Geral de Proteção de Dados (LGPD), assegurando a conformidade legal e a proteção dos dados do município.

**a.3) 01 (um) Especialista em Infraestrutura de TI**, com experiência comprovada em auditoria de segurança, análise de redes, servidores, sistemas operacionais e equipamentos de rede, responsável pelo suporte técnico e pela operacionalização das ações de segurança.

**b)** Para os fins desta exigência, conforme previsto no art. 67, inciso I, da Lei nº 14.133/2021, consideram-se pertencentes ao quadro permanente da empresa os profissionais que mantenham vínculo com a licitante na condição de sócio, diretor, responsável técnico ou empregado. A comprovação do vínculo dar-se-á por meio de:

**I – Para sócio:** apresentação do contrato social ou estatuto atualizado, devidamente registrado no órgão competente;

**II – Para diretor:** apresentação da ata de eleição e posse da atual diretoria, também registrada no órgão competente;

**III – Para responsável técnico ou empregado com vínculo empregatício:** apresentação da ficha ou livro de registro de empregados, contendo os campos de admissão ou rescisão e o termo de abertura do livro, ou, alternativamente, declaração de vínculo firmada pela licitante e pelo profissional, acompanhada de documentação complementar que comprove a relação de trabalho;

**IV – Nos casos em que o vínculo se der por contrato de prestação de serviços contínuos:** será admitida a apresentação de contrato vigente devidamente formalizado, com cláusula expressa de responsabilidade técnica do profissional em relação ao objeto do certame, observando-se as disposições da Lei nº 14.133/2021 e do Código Civil. Como medida

alternativa, poderá ser aceita declaração de disponibilidade assinada pelo profissional, comprometendo-se a integrar a equipe técnica da licitante, desde que acompanhada da documentação que comprove sua qualificação profissional e capacidade técnica compatível com as exigências do edital.

### **Justificativa da exigência dos profissionais**

A exigência de profissionais qualificados e vinculados ao quadro permanente da licitante, com formações e certificações específicas, justifica-se pela natureza técnica, estratégica e sensível da contratação, que envolve a prestação de serviços especializados de cibersegurança, testes de intrusão (pentest) e gestão de vulnerabilidades nos sistemas, dados e infraestrutura tecnológica das diversas secretarias do Município de Frecheirinha/CE.

A complexidade dos serviços e os riscos associados à segurança da informação exigem que a empresa contratada demonstre capacidade técnica efetiva e estrutura compatível com o objeto, o que só é possível com a presença de equipe mínima previamente estruturada, estável e experiente, composta por:

#### **1. Analista de Segurança da Informação com certificações reconhecidas**

Este profissional é indispensável para garantir a identificação, análise e mitigação de vulnerabilidades, execução dos testes de intrusão, e a proteção da integridade, confidencialidade e disponibilidade dos dados e sistemas. Além disso, atua na implementação de boas práticas e conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais normas aplicáveis à segurança cibernética.

#### **2. Profissional certificado em Governança e Conformidade em Segurança da Informação e LGPD**

A exigência desse profissional visa assegurar que a empresa possua expertise para interpretar e aplicar corretamente os requisitos legais relacionados à proteção de dados pessoais, atuando como elo entre o município, os titulares dos dados e os órgãos reguladores, prevenindo incidentes e garantindo a conformidade normativa durante a execução dos serviços.

#### **3. Especialista em Infraestrutura de TI com experiência em auditoria e análise de redes e sistemas**

Responsável pela avaliação técnica detalhada da infraestrutura tecnológica, suporte à operação dos testes de segurança, revisão de configurações e monitoramento de ativos críticos, garantindo a eficácia das medidas adotadas e a continuidade segura dos serviços.

#### **5.3.3. REQUISITOS DE QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:**

**5.3.3.1.** Apresentação de Certidão Negativa de Falência, Recuperação Judicial ou Extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica ou, no caso de pessoa física, Certidão Negativa de Execução Patrimonial, emitida no domicílio do proponente, conforme disposto na legislação aplicável.

**5.3.3.2.** No caso de cooperativas, estará dispensada a exigência constante do subitem acima.



**5.3.3.3.** Apresentação do Balanço Patrimonial, Demonstração do Resultado do Exercício (DRE) e demais demonstrações contábeis relativas aos dois (02) últimos exercícios sociais.

**5.3.3.4.** O julgamento da capacidade econômico-financeira será feito separadamente para cada exercício, de forma independente, com base no Balanço Patrimonial de cada ano.

**5.3.3.5.** Caso a pessoa jurídica tenha sido constituída há menos de dois (02) anos, os documentos mencionados no item 5.3.3.3 serão limitados ao último exercício encerrado, sendo admitido o balanço de abertura, conforme o caso.

**5.3.3.6.** O Balanço Patrimonial e as demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, deverão estar:

Registrados na Junta Comercial competente (ou em cartório, conforme o tipo societário);
Assinados por contador legalmente habilitado no Conselho Regional de Contabilidade (CRC);
Assinados pelo titular ou representante legal da empresa;
Vedada sua substituição por balancetes ou balanços provisórios, salvo se atualizados por índices oficiais quando encerrados há mais de três (03) meses da data de apresentação da proposta.

**5.3.3.7.** Serão aceitos o Balanço Patrimonial e demais demonstrações contábeis transmitidas via SPED (Escrituração Contábil Digital), desde que acompanhadas do recibo oficial de entrega, observadas as Instruções Normativas da Receita Federal vigentes.

**5.3.3.8.** Para sociedades por ações, será exigida a apresentação do Balanço Patrimonial publicado em jornal de grande circulação da localidade onde está situada a sede da companhia, acompanhado de seu respectivo registro na Junta Comercial.

**5.3.3.9.** As empresas deverão observar, conforme o seu porte e regime jurídico, as disposições constantes nos arts. 289, 294, 294-A e 294-B da Lei nº 6.404/1976 (Lei das Sociedades por Ações).

**5.3.3.10.** Para empresas recém-constituídas (com menos de 01 ano de atividade), deverá ser apresentado o Balanço de Abertura, acompanhado dos termos de abertura e encerramento, devidamente registrados na Junta Comercial, constando o número do Livro Diário e das folhas em que o balanço está transcrito, ou com a devida autenticação pela Junta. O documento deverá estar assinado por contador habilitado no CRC e pelo representante legal da empresa.

**5.3.3.11.** No caso de sociedades simples, o Balanço Patrimonial deverá estar inscrito no Cartório de Registro Civil de Pessoas Jurídicas, com a assinatura do contador habilitado e do representante legal da instituição, e deverá atender aos índices financeiros mínimos definidos neste instrumento convocatório.

**5.3.3.12.** Quando a empresa apresentar Índice de Liquidez Geral (LG) inferior a 1,0 (um), será exigida a comprovação de Patrimônio Líquido Mínimo ou Capital Mínimo correspondente a pelo menos 10% (dez por cento) do valor estimado da contratação, por meio do Balanço Patrimonial, como forma de compensação da capacidade econômico-financeira.

**5.3.3.13.** A comprovação da boa situação financeira da licitante deverá ser feita mediante documento assinado por profissional legalmente habilitado junto ao Conselho Regional de



Contabilidade da sede ou filial da empresa, comprovando que a mesma apresenta Índice de Liquidez Geral (LG) igual ou superior a 1,0 (um), calculado pela seguinte fórmula:

$$\text{LG} = \frac{\text{AC} + \text{ARLP}}{\text{PC} + \text{PELP}} \geq 1,0$$

**Onde:**

AC: Ativo Circulante;

ARLP: Ativo Realizável a Longo Prazo; PC: Passivo Circulante;

PELP: Passivo Exigível a Longo Prazo.

**Justificativa e Fundamentação da Exigência do Balanço Patrimonial e Demonstrações Contábeis**

A exigência de Balanço Patrimonial, Demonstração do Resultado do Exercício (DRE) e demais demonstrações contábeis visa assegurar à Administração Pública que a empresa contratada possui capacidade econômico-financeira suficiente para suportar as obrigações decorrentes da contratação, garantindo a continuidade e qualidade dos serviços prestados durante toda a vigência contratual. Conforme dispõe o art. 69 da Lei Federal nº 14.133/2021, a Administração poderá exigir, como requisito de habilitação, a apresentação de documentação contábil e indicadores financeiros, com o objetivo de verificar a situação financeira da licitante e sua aptidão para assumir obrigações contratuais.

A exigência de demonstrações contábeis dos dois últimos exercícios sociais, devidamente registradas na Junta Comercial ou cartório competente (conforme o tipo jurídico), assinadas por contador habilitado no Conselho Regional de Contabilidade (CRC) e pelo representante legal da empresa, visa garantir a confiabilidade e autenticidade das informações contábeis, conforme previsto no Código Civil Brasileiro, na Lei nº 6.404/1976 (Lei das S.A.) e nas Normas Brasileiras de Contabilidade (NBC).

A possibilidade de análise do Índice de Liquidez Geral (LG) ou a exigência de Patrimônio Líquido Mínimo ou Capital Social compatível com o objeto da contratação também está amparada pelo §1º do art. 69 da Lei nº 14.133/2021, que autoriza a fixação de critérios objetivos para aferir a boa saúde financeira da empresa, desde que justificados tecnicamente, como é o caso deste ETP.

Além disso, a Administração Pública tem o dever de mitigar riscos contratuais relacionados à inexecução parcial, total ou de baixa qualidade, especialmente em contratações que envolvem prestação contínua de serviços com suporte logístico relevante — como é o caso da locação de veículos com e sem motorista, onde há expectativa de manutenção da frota, substituições imediatas, seguro total e eventuais responsabilidades trabalhistas, no caso da prestação com condutor.

A apresentação do balanço patrimonial de abertura (para empresas recém-constituídas) ou a demonstração da situação financeira por meio do SPED Contábil com recibo de entrega oficial são alternativas legalmente aceitas, conforme orientações da Receita Federal do Brasil e da NBC TG 1000 – Contabilidade para Pequenas e Médias Empresas.

Por fim, tal exigência não restringe indevidamente a competitividade, pois é proporcional ao valor e à complexidade da contratação, sendo aplicada de forma uniforme e objetiva a todos os licitantes, em estrita observância ao princípio da isonomia (art. 5º, da Lei nº 14.133/2021), bem como aos princípios da vantajosidade, planejamento, transparência e segurança jurídica

**5.4. DA PRESTAÇÃO DOS SERVIÇOS.** A prestação dos serviços contratados será conforme solicitação da Secretaria requisitante com antecedência de 05 (Cinco) dias úteis, em locais a serem definidos e informados previamente pela administração;

**5.5. EXECUÇÃO.** Prazo para recebimento dos serviços, bem como critérios de pagamento serão detalhados no Termo de Referência.

#### **DA NATUREZA CONTINUADA OU NÃO (SERVIÇOS)**

**5.6.** Os presentes requisitos de contratação foram elencados levando-se em consideração as peculiaridades do serviço a ser prestado. Trata-se de **serviço continuado**, sem ou com fornecimento de mão de obra em regime de dedicação exclusiva;

**5.7.** Os serviços objeto desta contratação possuem natureza continuada, nos termos do art. 6º, incisos XIII e XV, da Lei nº 14.133/2021, tendo em vista sua essencialidade para a manutenção da integridade, disponibilidade e confidencialidade dos sistemas e dados institucionais. A continuidade contratual é necessária para assegurar a realização periódica de testes de intrusão (Pentest), a correção de vulnerabilidades identificadas e a manutenção ativa da estrutura de segurança da informação, prevenindo incidentes cibernéticos e garantindo conformidade com a Lei Geral de Proteção de Dados (LGPD). Trata-se de um serviço que não se limita a uma execução pontual, mas que exige monitoramento contínuo, atualizações frequentes, suporte técnico especializado e integração permanente com os demais sistemas institucionais, podendo se estender por mais de um exercício financeiro.

#### **5.8. Critérios e práticas de sustentabilidade e governança:**

**5.8.1.** A presente contratação observará os critérios de sustentabilidade e governança previstos nos arts. 5º, 20 e 23 da Lei nº 14.133/2021, priorizando a eficiência administrativa, inovação tecnológica, economicidade, responsabilidade socioambiental e integridade na gestão pública.

No tocante à sustentabilidade, os serviços de cibersegurança a serem contratados deverão:

Ser realizados em modelo híbrido, priorizando o atendimento remoto, porém assegurando a presença física de profissionais especializados sempre que a complexidade das atividades exigir intervenção direta;

Utilizar tecnologias avançadas de automação e monitoramento contínuo para identificação proativa, mitigação e resposta a incidentes de segurança;

Garantir a conformidade rigorosa com a Lei Geral de Proteção de Dados Pessoais (Lei nº

13.709/2018), assegurando a confidencialidade, integridade e disponibilidade das informações sensíveis do Município;

Adotar procedimentos rigorosos para armazenamento seguro, gerenciamento adequado e descarte responsável de dados, prevenindo riscos de vazamentos e acessos não autorizados.

**Quanto à governança, a contratação deverá atender aos seguintes princípios**

Assegurar transparência total nos registros e relatórios produzidos, possibilitando auditoria detalhada, rastreabilidade e fiscalização por parte da Administração Pública;

Garantir a prestação contínua de contas, por meio de painéis gerenciais (dashboards), indicadores de desempenho e relatórios regulares que evidenciem o cumprimento das obrigações contratuais;

Estabelecer cláusulas contratuais que definam níveis mínimos de serviço (SLA) e instrumentos eficazes de acompanhamento e fiscalização digital por parte da Secretaria responsável;

Promover o compromisso ético e o combate a práticas ilícitas, mediante a inclusão de cláusulas contratuais que responsabilizem a contratada, assegurem a integridade empresarial e regulamentem o controle de acessos e dados sensíveis.

5.8.1.1. Essas práticas serão analisadas tanto na fase de habilitação quanto durante a execução contratual, podendo ser exigida documentação comprobatória, certificações pertinentes ou relatórios de conformidade periódicos, conforme definido no Termo de Referência e no edital.

5.8.2. Estímulo à adoção de soluções digitais e tecnológicas que elevem a eficiência operacional, minimizando intervenções manuais e aumentando a segurança dos processos;

5.8.3. Implantação de medidas que garantam a continuidade operacional e a resiliência dos serviços, mitigando impactos decorrentes de incidentes de segurança cibernética;

5.8.4. Observância de critérios de acessibilidade digital e usabilidade para garantir que as ferramentas disponibilizadas sejam inclusivas e de fácil operação pelos usuários envolvidos;

5.8.5. Incentivo à participação de fornecedores locais e microempresas que demonstrem qualificação técnica compatível, promovendo o desenvolvimento regional e a competitividade no processo licitatório.

5.9. Este estudo foi elaborado com base no objeto informado pelas Secretarias Municipais em seus Documentos de Formalização de Demanda (DFD), tendo como objeto sugerido a seguinte contratação: **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE CIBERSEGURANÇA, INCLUINDO A REALIZAÇÃO DE TESTES DE INTRUSÃO (PENTEST) E DEMAIS SERVIÇOS TÉCNICOS ESPECIALIZADOS VOLTADOS À IDENTIFICAÇÃO, ANÁLISE E MITIGAÇÃO DE VULNERABILIDADES, VISANDO GARANTIR A SEGURANÇA DOS SISTEMAS, DADOS E INFRAESTRUTURA**

**TECNOLÓGICA DA PREFEITURA MUNICIPAL DE FRECHEIRINHA/CE.**, visando atender as necessidades administrativas da Secretaria demandante. Essa contratação tem como objetivo suprir as demandas administrativas da Secretaria solicitante, garantindo o cumprimento das exigências legais.

5.10. Isso posto, a melhor estratégia para atender à demanda seria a **CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS DE CIBERSEGURANÇA, INCLUINDO A REALIZAÇÃO DE TESTES DE INTRUSÃO (PENTEST) E DEMAIS SERVIÇOS TÉCNICOS ESPECIALIZADOS VOLTADOS À IDENTIFICAÇÃO, ANÁLISE E MITIGAÇÃO DE VULNERABILIDADES, VISANDO GARANTIR A SEGURANÇA DOS SISTEMAS, DADOS E INFRAESTRUTURA TECNOLÓGICA DAS DIVERSAS SECRETARIA DO MUNICÍPIO DE FRECHEIRINHA/CE**, de natureza continuada, para não comprometer a continuidade das atividades Administrativas.

5.11. A vigência inicial do contrato será de **01 (UM) ano**, com possibilidade de prorrogação nos termos e prazos dos artigos 106 e 107 da Lei 14.133/2021, desde que seja comprovado a sua vantajosidade e que os serviços tenham sido prestados com eficiência e qualidade.

5.12. Necessidade de garantia de execução: **NÃO**.

5.13. As autorizações de serviços contendo as notas de empenho serão enviadas da seguinte na Forma Prevista no **TERMO DE REFERÊNCIA**.

5.14. execução contratual dos serviços será organizada conforme a natureza específica da solução tecnológica contratada, respeitando os princípios da eficiência, do controle, da economicidade e da continuidade administrativa. A contratada deverá seguir rotinas operacionais e técnicas previamente definidas pelos órgãos do Município de Frecheirinha/CE, compreendendo a implantação, suporte, atualização e integração dos sistemas de segurança da informação, testes de intrusão (pentest) e mitigação de vulnerabilidades na infraestrutura tecnológica.

#### **5.15. DAS ESPECIFICAÇÕES E EXECUÇÃO DOS SERVIÇOS/OBJETO**

5.15.1. O objetivo desta contratação é identificar e explorar vulnerabilidades, simulando ataques reais que serão realizados por profissionais identificados, certificados e capacitados, devendo incluir a elaboração e apresentação de relatórios detalhados contendo os métodos, técnicas e ferramentas utilizadas, bem como avaliação, diagnóstico e recomendações de correção das vulnerabilidades porventura encontradas.

5.15.2. Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, nem do ativo porventura relacionado, sem explícita e prévia autorização e monitoração pela equipe técnica responsável da DAE S/A.

5.15.3. Caso o DAE S/A entenda haver algum risco na execução do Pentest que possa comprometer, em qualquer grau, o funcionamento de sistema, ativo ou processo da DAE S/A, poderá solicitar a mudança de metodologia e/ou do cronograma, inclusive podendo requerer a execução dos testes em finais de semana, feriados ou fora do horário comercial.



5.15.4. Durante os testes, não poderão ser executados quaisquer variações dos seguintes ataques sem explícita autorização prévia e monitoração pela equipe técnica responsável da DAE S/A:

5.15.4.1. Ataques de negação de serviços e flooding;

5.15.4.2. Engenharia social, por exemplo, phishing, vishing, pharming, personificação, roubo de identidade e outros;

5.15.4.3. Ataques que possam causar danos físicos, por exemplo, arrombamentos, danos a fechaduras eletrônicas, ativação de sistemas de alarme.

5.15.4.4. Todos os testes deverão ser acompanhados e supervisionados pela equipe de TI da DAE.

5.15.5. A empresa CONTRATADA deverá ser capaz de aplicar, no mínimo, os seguintes tipos de ataques, quando aplicáveis:

5.15.5.1. Violações do protocolo HTTP;

5.15.5.2. SQL Injection;

5.15.5.3. LDAP Injection;

5.15.5.4. Cookie Tampering;

5.15.5.5. Cross-Site Scripting (XSS);

5.15.5.6. Directory Transversal;

5.15.5.7. Buffer Overflow;

5.15.5.8. OS Command Execution;

5.15.5.9. Command Injection;

5.15.5.10. Remote Code Inclusion;

5.15.5.11. Server Side Includes (SSI) Injection;

5.15.5.12. File disclosure;

5.15.5.13. Information Leak;

5.15.5.14. Ataques contra protocolo TCP:

5.15.5.14.1. Sequestro de conexões;

5.15.5.14.2. Prognóstico de número de sequência do protocolo TCP;

5.15.5.14.3. Source routing.

5.15.5.15. Ataques em nível da aplicação:

5.15.5.15.1. Buffer Overflow;

5.15.5.15.2. Problemas com o SNMP;

5.15.6. Para testes de invasão direcionados, especificamente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, no mínimo, os testes

baseados na publicação OWASP TESTING GUIDE (The Open Web Application Security Project) em sua versão mais recente.

#### **5.16. TESTES A SEREM REALIZADOS**

5.16.1. A CONTRATADA realizará testes de intrusão (pentest) sob demanda nos ativos do ambiente de TI da CONTRATANTE, com objetivo de identificar e explorar vulnerabilidades de forma controlada, simulando ataques reais por profissionais certificados. Deverá apresentar relatórios detalhados com métodos, técnicas, ferramentas, avaliação e recomendações para correção.

5.16.2. O serviço será prestado por 12 meses, contados a partir do Termo de Aceite Técnico, podendo ser prorrogado conforme legislação.

5.16.3. Em até 60 dias após a assinatura, a CONTRATADA deverá apresentar o planejamento da execução, equipe, canais de comunicação e demais requisitos.

5.16.4. A CONTRATANTE terá 10 dias para validar a documentação e emitir o Termo de Aceite Técnico, com até 5 dias para nova validação após ajustes, se necessário.

5.16.5. As horas utilizadas serão deduzidas do total contratado, podendo o saldo remanescente ser utilizado durante a vigência.

5.16.6. Escopo e horas dos testes devem ser alinhados previamente com gestores da CONTRATANTE e formalizados por Ordem de Serviço.

5.16.7. Testes poderão ser realizados fora do horário comercial e em dias não úteis, conforme critério da CONTRATANTE.

5.16.8. Consideram-se ATIVO qualquer item de TI, como hosts, dispositivos de rede, interfaces de aplicação ou sistemas internos.

5.16.9. Pentests podem abranger infraestrutura de TI, aplicações web e nuvem, APIs, bancos de dados e outros alvos definidos pela CONTRATANTE.

5.16.10. Serviços poderão incluir engenharia social, com usuários definidos pela CONTRATANTE, como:

- Phishing/spear phishing com controle de rastreamento;
- Smishing via apps, SMS e voz em smartphones corporativos;
- Dumpster diving para coleta de material descartado;
- Tailgating em áreas restritas autorizadas;
- Quid pro quo, pendrive “esquecido” e sondagem em mídias sociais;
- Scareware ou ransomware falso com rastreamento;
- Outras técnicas de engenharia social.

5.16.11. Testes só serão realizados com autorização formal da CONTRATANTE, podendo ser black-box, gray-box ou white-box, internos, externos ou específicos.

5.16.12. Os formatos incluem:

- Ataques a redes e protocolos com varreduras automatizadas em infraestrutura (firewall, IPS, WAF, bancos de dados, sistemas operacionais);
- Varreduras em aplicações web contra vulnerabilidades OWASP Top 10;
- Varreduras em APIs conforme OWASP API Security e linguagens web (.Net, Java, PHP, Python, etc.).

5.16.13. Avaliação técnica do hardening dos ativos segundo padrões NIST/CIS/FIRST, incluindo:

- Autenticação: controles para proteção de credenciais;
- Autorização: permissões e grupos de privilégios;
- Auditoria: eventos importantes para registro e investigação;
- Serviços: identificação de serviços/protocolos desnecessários;
- Checklist personalizado para implantação ou entrada do ativo na rede.

5.16.14. Técnicas deverão focar na integridade, confidencialidade e disponibilidade dos recursos conforme características indicadas pela CONTRATANTE.

5.16.15. Exploração de vulnerabilidades ocorrerá apenas após autorização formal, em datas e horários acordados com profissionais indicados pela CONTRATANTE.

5.16.16. Resultados das explorações deverão ser documentados com evidências suficientes para comprovar o sucesso.

5.16.17. Vulnerabilidades serão classificadas conforme metodologia CVSS (Common Vulnerability Scoring System) do FIRST, contendo:

**- Análise das métricas bases:**

- Vetor de ataque;
- Complexidade do ataque;
- Privilégios requeridos;
- Interação com usuário
- Impacto em confidencialidade, integridade e disponibilidade.

**- Análise das métricas temporais:**

- Maturidade do exploit;
- Nível de remediação.

## **5.17. ENTREGA DOS TESTES**

5.17.1. Os resultados deverão ser entregues em relatório descritivo e planilha eletrônica, podendo também ser disponibilizados em plataforma para gestão centralizada da correção das vulnerabilidades e comprovação para auditorias futuras.

5.17.2. A documentação deverá relacionar endereços com falhas e vulnerabilidades, além de recomendar plano de ação para proteger a infraestrutura da CONTRATANTE.

5.17.3. Deverá ser entregue apresentação técnica segmentada por ambiente, camada ou tecnologia, conforme escopo alinhado com a CONTRATANTE.

5.17.4. Também deverá ser entregue apresentação executiva.

5.17.5. Será entregue um Sumário Executivo.

5.17.6. A CONTRATADA participará de reuniões com equipes técnicas da CONTRATANTE para detalhar resultados e repassar recomendações.

5.17.7. Todas as atividades deverão seguir boas práticas nacionais e internacionais de gestão e governança de TI, como ITIL, ISO 20000, Cobit, PMBOK e ISO 27000, além das metodologias específicas para pentest, obrigatoriamente uma das seguintes:

- OSSTMM 3;
- OWASP Testing Guide (última versão);
- NIST SP 800-115;
- PTES.

5.17.8. As ferramentas utilizadas são de responsabilidade da CONTRATADA, não devem ser instaladas na infraestrutura da CONTRATANTE e o impacto na rede deve ser mínimo. Ferramentas são auxiliares e não substituem a análise manual.

5.17.9. As ferramentas devem ser modernas e utilizadas no mercado, com as seguintes características mínimas:

- Atualização constante com as últimas ameaças e vulnerabilidades;
- Avaliação de riscos com score CVSS;
- Apresentação de soluções ou mitigação detalhadas;
- Uso de identificadores CVE para vulnerabilidades;
- Aprovação prévia das ferramentas e metodologia pela CONTRATANTE;
- Armazenamento seguro de credenciais para varreduras autenticadas em sistemas e dispositivos;
- Capacidade de detectar vulnerabilidades OWASP Top 10 atualizadas;
- Realizar escaneamento ativo e passivo;
- Executar crawling/spidering para descoberta de URLs, links e páginas.

5.17.10. Ao final de cada Ordem de Serviço, deverá ser preenchido o “Registro de Atendimento - Ordem de Serviço”, assinado por representante da Fazenda ou colaborador designado.

5.17.11. O pagamento será mensal, proporcional às horas utilizadas, mediante emissão de relatório mensal pela CONTRATADA e comprovação das atividades.



5.17.12. O relatório mensal deverá incluir os formulários “Registro de Atendimento - Ordem de Serviço” assinados para cada atividade.

5.17.13. Todos os custos relacionados aos serviços, incluindo hardware e software necessários não especificados, serão de responsabilidade da CONTRATADA.

#### **5.18. GESTÃO DE VULNERABILIDADE**

5.18.1. Os serviços de Gestão de Vulnerabilidades terão duração inicial de 15 meses a partir do Termo de Aceite Técnico, podendo ser prorrogados até 60 meses, conforme a lei.

5.18.2. A CONTRATADA deve apresentar em até 60 dias, após assinatura do contrato, o planejamento da execução, composição da equipe, canais de comunicação e demais requisitos.

5.18.3. A CONTRATANTE terá 10 dias para validar a documentação, emitindo o Termo de Aceite Técnico; em caso de inconsistências, a CONTRATADA terá 5 dias para correções e nova validação.

5.18.4. O serviço será executado em regime 8x5, ou seja, 8 horas diárias, 5 dias por semana, entre 7h e 19h em dias úteis.

5.18.5. A CONTRATADA deverá identificar proativamente vulnerabilidades na infraestrutura da CONTRATANTE para mitigar riscos de ataques cibernéticos, entregando relatório com as 5 principais recomendações detalhadas para execução pela equipe da CONTRATANTE.

5.18.6. Semestralmente, a CONTRATADA realizará, em conjunto com a CONTRATANTE, hardening em até 5 ativos, fundamentado tecnicamente e adaptado ao ambiente, considerando cerca de 40 horas por ativo.

5.18.7. A CONTRATADA deverá monitorar fontes públicas de vulnerabilidades, analisá-las para o ambiente da CONTRATANTE e recomendar correções nos relatórios mensais. Para vulnerabilidades com CVSS v3.1  $\geq 9.0$ , deverá emitir relatório imediato contendo descrição, impacto, probabilidade, mitigação, riscos e alternativas.

5.18.8. A gestão atuará em parceria com o CSIRT para sugerir ações frente a novas vulnerabilidades.

5.18.9. As análises e recomendações considerarão escopo, relevância e criticidade dos ativos da CONTRATANTE.

5.18.10. Falsos positivos e vulnerabilidades não aplicáveis deverão ser eliminados dos relatórios.

5.18.11. A CONTRATADA deverá evitar causar indisponibilidades ou alterações no ambiente da CONTRATANTE durante as análises.

5.18.12. O registro das vulnerabilidades será feito em plataforma da CONTRATANTE, com participação da CONTRATADA na customização e evolução, incluindo dashboards para acompanhamento dinâmico.

5.18.13. O CONTRATANTE poderá solicitar detalhamento adicional dos relatórios.

5.18.14. Todos os relatórios serão em português.

5.18.15. A CONTRATANTE validará os relatórios em até 5 dias úteis, solicitando correções se necessário.

5.18.16. Os relatórios serão considerados entregues após revisão e correções aprovadas pela CONTRATANTE.

5.18.17. A CONTRATADA deverá cumprir os níveis de SLA definidos, com penalidades por atraso na entrega de relatórios: 5% do valor da fatura (VF) por ocorrência, aumentando até 15% por atraso prolongado.

5.18.18. A CONTRATADA deverá executar o serviço dentro dos níveis de acordo de serviço (SLA) explicitados abaixo, incorrendo em glosas sobre o valor da fatura (VF) conforme a tabela a seguir:

Indicador	Objetivo	Fórmula de Cálculo	Resultado Aceitável	Redutor
Entrega dos relatórios	Entregar os relatórios exigidos no prazo acordado.	Por dia de atraso	Atraso = 0 dias	5% do VF por ocorrência (+5% por semana extra de atraso, limitado a 15%, por relatório)

5.18.19. As seguintes ocorrências também serão objeto de glosa no valor da fatura (VF), limitados até 40%, no caso da CONTRATADA:

Descrição	Referência	Redutor
Causar qualquer indisponibilidade dos serviços da contratante por motivo de imperícia ou imprudência na execução das atividades contratuais	Por ocorrência	10% do VF
Suspender, colocar como pendente ou interromper, salvo por motivo justificado, a execução dos serviços.	Por ocorrência	5% do VF
Realizar mudanças de configuração nos ativos de Cybersegurança sem autorização da CONTRATANTE.	Por ocorrência	10% do VF
Fraudar, manipular ou descaracterizar indicadores de níveis de serviço e de desempenho por quaisquer subterfúgios	Por ocorrência	20% do VF
Recusar-se a executar serviço relacionado às atividades deste ITEM solicitado pela CONTRATANTE.	Por ocorrência	10% do VF

5.18.20. O pagamento ocorrerá de forma mensal, após a avaliação do nível de serviço conforme relatórios elencados no item anterior e computadas às eventuais glosas do mês de referência.

5.18.21. No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso fundamentado que será analisado pela área administrativa da CONTRATANTE. Se a

decisão da Administração for favorável ao recurso da CONTRATADA, o valor glosado será novamente considerado no faturamento mensal.

**6. LEVANTAMENTO DE MERCADO (§ 2º do art. 18 da Lei nº 14.133/2021 e art.6º, Inc. III do Anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024).**

6.1. Considerando a necessidade apresentada, o levantamento de mercado demonstra que existem diversas soluções especializadas capazes de atender, de forma individual ou integrada, à demanda por serviços de cibersegurança, abrangendo a execução de testes de intrusão (Pentest) e demais serviços técnicos voltados à identificação, análise e mitigação de vulnerabilidades. As principais soluções ofertadas pelo mercado incluem ferramentas e metodologias avançadas para avaliação da segurança de sistemas, redes e aplicações, serviços gerenciados de monitoramento contínuo, auditorias técnicas com emissão de relatórios detalhados, suporte especializado para correção de falhas, capacitação de equipes internas e conformidade com as normas e legislações aplicáveis, especialmente a Lei Geral de Proteção de Dados (LGPD).

**Soluções Disponíveis de Mercado:**

SOLUÇÕES ENCONTRADAS	DETALHAMENTO DA SOLUÇÃO
Contratação de empresa especializada em serviços de cibersegurança, incluindo testes de intrusão (pentest) e gestão de vulnerabilidades, por meio de processo licitatório.	1) Oferece serviços técnicos especializados para identificação, análise e mitigação de vulnerabilidades em sistemas, redes, aplicações e infraestrutura tecnológica. 2) Profissionais certificados e atualizados em metodologias reconhecidas (OSSTMM, PTES, OWASP, NIST) capazes de realizar testes controlados e seguros. 3) Uso de ferramentas avançadas e relatórios detalhados que fornecem diagnóstico preciso e recomendações práticas para correção das falhas detectadas.
Execução dos serviços de pentest e gestão de vulnerabilidades pela equipe interna da Administração.	1) Aproveita o conhecimento e experiência dos servidores sobre o ambiente tecnológico local. 2) Permite maior controle sobre os dados e processos sensíveis. 3) Pode reduzir custos com contratação externa.

6.2. A seguir, apresenta-se a análise das soluções identificadas para atender à necessidade de contratação, conforme as informações contidas nos documentos apresentados até aqui:

COMPARATIVO DE SOLUÇÕES PARA TESTES DE INTRUSÃO E GESTÃO DE VULNERABILIDADES		
Contratação de empresa especializada em pentest e gestão de vulnerabilidades	-Equipes com certificações e experiência específica em testes de intrusão.	- Investimento financeiro maior devido à contratação externa.

	<ul style="list-style-type: none"> <li>-Utilização de metodologias e ferramentas atualizadas, garantindo cobertura e profundidade nas análises.</li> <li>-Emissão de relatórios técnicos e executivos que subsidiam tomadas de decisão e planejamento de segurança.</li> <li>- Maior segurança no ambiente por simulação realista de ataques.</li> </ul>	<ul style="list-style-type: none"> <li>- Dependência do fornecedor para cumprimento das atividades críticas.</li> <li>- Necessidade de acompanhamento rigoroso para garantir qualidade e cumprimento dos prazos.</li> </ul>
Execução interna dos testes e gestão pela equipe de TI da Administração	<ul style="list-style-type: none"> <li>- Conhecimento aprofundado do ambiente interno e seus sistemas.</li> <li>- Controle direto e imediato sobre dados sensíveis.</li> <li>- Potencial redução de custos com terceiros.</li> </ul>	<ul style="list-style-type: none"> <li>- Limitações técnicas da equipe interna frente a ameaças cada vez mais complexas.</li> <li>- Necessidade constante de atualização e capacitação.</li> <li>- Investimentos adicionais em ferramentas e infraestrutura de segurança.</li> <li>- Maior risco de falhas e vulnerabilidades não detectadas.</li> </ul>

#### 6.2.1. Soluções possíveis oferecidas pelo mercado:

<b>1. Serviços de Testes de Intrusão (Pentest) Internos e Externos</b>	<ul style="list-style-type: none"> <li>- Simulação controlada de ataques para identificar vulnerabilidades em redes, servidores, aplicações e dispositivos.</li> <li>- Abrange testes em ambiente interno (intranet) e externo (exposição na internet), com relatórios técnicos e executivos.</li> </ul>
<b>2. Varredura e Análise de Vulnerabilidades (Vulnerability Assessment)</b>	<ul style="list-style-type: none"> <li>- Ferramentas e métodos para destacar e classificar falhas de segurança em ativos tecnológicos</li> <li>- Priorização de riscos e recomendações de mitigação.</li> </ul>
<b>3. Monitoramento Contínuo de Segurança (SOC – Security Operations Center)</b>	<ul style="list-style-type: none"> <li>- Serviços de acompanhamento 24/7 de eventos de segurança</li> <li>- Detecção e resposta a incidentes de forma proativa</li> </ul>
<b>4. Análise e Fortalecimento da Infraestrutura de Rede e Servidores</b>	<ul style="list-style-type: none"> <li>- Avaliação de configuração e hardening de equipamentos e sistemas.</li> <li>- Implementação de controles de segurança para prevenir acessos não autorizados</li> </ul>



<b>5. Testes de Segurança em Aplicações Web e Móveis</b>	<ul style="list-style-type: none"><li>- Identificação de falhas com injeção de código, quebras de autenticação, exposição de dados e vulnerabilidade OWASP Top 10.</li></ul>
<b>6. Serviços de Simulação de Engenharia Social (Phishing, Pretexting e Vishing)</b>	<ul style="list-style-type: none"><li>- Testes voltados à avaliação da conscientização dos usuários frente a tentativas de fraude.</li><li>- Inclusão de campanhas educativas pós-teste</li></ul>
<b>7. Consultoria em Conformidade com LGPD e Normas de Segurança da Informação</b>	<ul style="list-style-type: none"><li>- Adequação de processos e sistemas à Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e demais normas aplicáveis.</li><li>- Elaboração de políticas e procedimentos de segurança.</li></ul>
<b>8. Serviços de Resposta a Incidentes e Recuperação Pós-Invasão</b>	<ul style="list-style-type: none"><li>- Investigação, contenção e erradicação de incidentes de segurança.</li><li>- Análise forense e recomendações para evitar reincidência.</li></ul>
<b>9. Treinamento e Capacitação de Equipes Internas</b>	<ul style="list-style-type: none"><li>- Programas de formação técnica para servidores da área de TI e conscientização para todos os usuários.</li><li>- Simulações práticas e cursos de atualização em cibersegurança.</li></ul>
<b>10. Modelos de Contratação por Projeto, Assinatura ou Pacotes Personalizados</b>	<ul style="list-style-type: none"><li>- Prestação de serviços pontuais (projetos específicos) ou contínuos (assinatura mensal).</li><li>- Possibilidade de personalização de acordo com o porte e necessidade da Administração.</li></ul>

### 6.2.3. A análise das soluções identificadas:

SOLUÇÃO	PONTOS POSITIVOS	PONTOS NEGATIVOS
<b>Serviços de Testes de Intrusão (Pentest) Internos e Externos</b>	<ul style="list-style-type: none"><li>- Identifica vulnerabilidades reais antes que sejam exploradas.</li><li>- Reproduzir cenários de ataque real.</li><li>- Gera relatórios técnicos e executivos para diferentes públicos.</li></ul>	<ul style="list-style-type: none"><li>- Pode Exigir Janelas de manutenção para evitar impactos nos serviços.</li><li>- Alto custo se executado com frequência.</li></ul>

<b>Varredura e Análise de Vulnerabilidades (Vulnerability Assessment)</b>	<ul style="list-style-type: none"><li>- Detecta e classifica falhas de forma ampla e sistemática.</li><li>- Permite priorização de risco para ações rápidas</li><li>- Facilita a mitigação preventiva.</li></ul>	<ul style="list-style-type: none"><li>- Não simula ataques reais como Pentest.</li><li>- Pode gerar falso positivos que exigem validação.</li></ul>
<b>Monitoramento Contínuo de Segurança (SOC – Security Operations Center)</b>	<ul style="list-style-type: none"><li>- Garantia de acompanhamento 24/7.</li><li>- Detecção e resposta rápida a incidente.</li><li>- Aumento significativo na postura de segurança.</li></ul>	<ul style="list-style-type: none"><li>- Custo recorrente elevado.</li><li>- Dependência de equipe especializada terceirizada.</li></ul>
<b>Análise e Fortalecimento da Infraestrutura de Rede e Servidores</b>	<ul style="list-style-type: none"><li>- Melhora a resiliência contra ataques.</li><li>- Reduz riscos de acesso não autorizados.</li><li>- Segue boas práticas de Hardening.</li></ul>	<ul style="list-style-type: none"><li>- Pode demandar reconfiguração de sistemas críticos.</li><li>- Implementações mal planejadas podem gerar indisponibilidade temporária.</li></ul>
<b>Testes de Segurança em Aplicações Web e Móveis</b>	<ul style="list-style-type: none"><li>- Identifica vulnerabilidade específicas da aplicação.</li><li>- Abrange OWASP Top 10, aumentando a segurança contra ataques comuns.</li><li>- Melhora a confiança do usuário final.</li></ul>	<ul style="list-style-type: none"><li>- Exige conhecimento especializado.</li><li>- Testes mal conduzidos podem afetar o funcionamento temporário da aplicação.</li></ul>
<b>Serviços de Simulação de Engenharia Social (Phishing, Pretexting e Vishing)</b>	<ul style="list-style-type: none"><li>- Mede a conscientização real dos usuários.</li><li>- Auxilia na prevenção de ataques baseados em manipulação humana.</li><li>- Inclui ações educativas corretivas.</li></ul>	<ul style="list-style-type: none"><li>- Pode Gerar desconforto nos colaboradores.</li><li>- Requer comunicação clara para evitar mal-entendido.</li></ul>
<b>Consultoria em Conformidade com LGPD e Normas de Segurança da Informação</b>	<ul style="list-style-type: none"><li>- Adequação à legislação vigente.</li><li>- Melhora a governança e transparência.</li><li>- Evita multas e sanções legais.</li></ul>	<ul style="list-style-type: none"><li>- Processo pode ser demorado.</li><li>- Requer envolvimento ativo de várias áreas da organização.</li></ul>

<b>Serviços de Resposta a Incidentes e Recuperação Pós-Invasão</b>	<ul style="list-style-type: none"><li>- Minimiza danos após incidentes.</li><li>- Possibilita rápida retomada das operações.</li><li>- Fornece análise forense para evitar recorrência.</li></ul>	<ul style="list-style-type: none"><li>- Atuação geralmente reativa.</li><li>- Custo elevado em casos críticos.</li></ul>
<b>Treinamento e Capacitação de Equipes Internas</b>	<ul style="list-style-type: none"><li>- Aumenta o nível de preparo e conscientização.</li><li>- Reduz riscos humanos.</li><li>- Pode ser adaptado ao público-alvo.</li></ul>	<ul style="list-style-type: none"><li>- Pode gerar custo de deslocamento ou hora-parada.</li><li>- Exige atualização constante dos conteúdos.</li></ul>
<b>Modelos de Contratação por Projeto, Assinatura ou Pacotes Personalizados</b>	<ul style="list-style-type: none"><li>- Flexibilidade para atender diferentes necessidades.</li><li>- Possibilidade de ajuste ao orçamento disponível.</li><li>- Opção de serviços pontuais ou contínuos.</li></ul>	<ul style="list-style-type: none"><li>- Projetos pontuais podem não garantir segurança contínua.</li><li>- Assinaturas podem gerar custos fixos elevados se subutilizadas.</li></ul>

**SOLUÇÃO:** A escolha da solução pela contratação de empresa especializada em serviços de cibersegurança, incluindo testes de intrusão (pentest) e gestão de vulnerabilidades, com o objetivo de fortalecer a segurança dos sistemas, dados e infraestrutura tecnológica do Município. Essa abordagem visa garantir a identificação, análise e mitigação proativa de riscos cibernéticos, assegurando a integridade, confidencialidade e disponibilidade dos ativos de TI, em conformidade com as melhores práticas e normativas vigentes.

### **6.3. JUSTIFICATIVA TÉCNICA, ECONÔMICA E SUSTENTÁVEL PARA A ESCOLHA DA SOLUÇÃO**

Considerando a necessidade de fortalecer a segurança dos sistemas, dados e infraestrutura tecnológica do Município de Frecheirinha/CE, justifica-se a contratação de empresa especializada para a prestação de serviços de cibersegurança, abrangendo testes de intrusão (pentest) e demais ações técnicas voltadas à identificação, análise e mitigação de vulnerabilidades, conforme detalhado neste Estudo Técnico Preliminar.

#### **1. Justificativa Técnica**

A opção pela contratação de empresa especializada em serviços de pentest e gestão de vulnerabilidades atende de forma ampla e eficiente às necessidades de segurança da informação do Município, priorizando soluções que possibilitem:

Execução de testes de intrusão externos e internos, simulando vetores de ataque reais e
---

controlados, visando a identificação de vulnerabilidades críticas em redes, sistemas operacionais, aplicações web e móveis, dispositivos de rede e demais ativos tecnológicos;

Uso de metodologias reconhecidas internacionalmente (OSSTMM, PTES, OWASP, NIST), assegurando cobertura completa e abordagem sistemática na avaliação de riscos;

Geração de relatórios técnicos detalhados, com evidências, análise de impacto, classificação de riscos e recomendações estruturadas para mitigação, além de relatórios executivos para suporte à governança e tomada de decisão estratégica;

Monitoramento contínuo e análise proativa das ameaças e vulnerabilidades, com utilização de ferramentas avançadas de escaneamento autenticado e análise baseada em métricas CVSS v3.1, incluindo detecção das vulnerabilidades listadas no OWASP Top 10 e outras ameaças emergentes;

Suporte técnico permanente para assessoramento na remediação e hardening da infraestrutura, assegurando a governança dos processos de segurança e a conformidade com normativas vigentes, como a Lei Geral de Proteção de Dados (LGPD).

Essa solução técnica é fundamental para mitigar riscos cibernéticos, preservar a integridade, confidencialidade e disponibilidade dos ativos de TI, garantindo resiliência operacional e alinhamento com as melhores práticas de segurança da informação.

#### **Justificativa Econômica:**

A opção pela contratação de serviços especializados, seja na modalidade contínua ou por demanda, apresenta vantagens econômicas significativas, tais como:

Eliminação de investimentos elevados em aquisição, licenciamento e atualização de ferramentas proprietárias de segurança, além de capacitação técnica especializada interna;

Redução de custos operacionais relacionados a correções emergenciais, respostas a incidentes e paralisações decorrentes de vulnerabilidades exploradas;

Previsibilidade financeira com pagamentos estruturados conforme entregas mensais, indicadores de nível de serviço (SLAs) e resultados efetivos, facilitando o planejamento orçamentário;

Desoneramento da administração pública quanto à manutenção de equipe interna altamente especializada, que demanda altos custos em recrutamento, treinamento e retenção.

6.3.1. Adicionalmente, a contratação de empresa com comprovada expertise reduz o risco de incidentes graves que impactem a continuidade dos serviços públicos, protegendo o patrimônio digital e evitando custos decorrentes de falhas de segurança.

#### **Justificativa Sustentável**

A solução técnica contratada contribui para a sustentabilidade administrativa, tecnológica e ambiental do Município, por meio de:

Minimização dos impactos financeiros e operacionais causados por incidentes de segurança, prevenindo danos, perdas de dados e interrupções nos serviços essenciais;



Incentivo à digitalização segura de processos, com redução do uso de documentos físicos, mitigando riscos de vazamento e retrabalho;

Garantia de conformidade rigorosa com a LGPD, promovendo a governança e o controle adequado dos dados pessoais e sensíveis de servidores, alunos e cidadãos;

Uso de tecnologias escaláveis e ambientes de hospedagem certificados e seguros, que evitam o descarte prematuro de equipamentos físicos e contribuem para a redução da pegada ambiental.

6.4. Assim, a solução contratada assegura o atendimento aos princípios da economicidade, eficiência, inovação e responsabilidade socioambiental previstos na Lei nº 14.133/2021, estando alinhada às melhores práticas de governança e segurança da informação no setor público.

## **7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO (inciso VII do § 1º do art. 18 da Lei 14.133/21)**

7.1. A presente solução compreende a contratação de empresa especializada em tecnologia da informação para a execução contínua de serviços avançados de cibersegurança, englobando a realização de testes de intrusão (pentest), a gestão proativa e integrada de vulnerabilidades, bem como o monitoramento e a resposta a incidentes de segurança digital. O objetivo central é assegurar, de forma ininterrupta, a proteção, a integridade, a confidencialidade e a alta disponibilidade dos sistemas, dados e de toda a infraestrutura tecnológica do Município de Frecheirinha/CE, preservando a continuidade dos serviços públicos e a resiliência operacional diante de ameaças cibernéticas.

7.2. Os serviços deverão abranger integralmente a infraestrutura de TI do Município, incluindo redes físicas e virtuais, servidores físicos e em nuvem, estações de trabalho, dispositivos móveis, aplicações internas e externas, além de perímetros de segurança lógica, contemplando os seguintes componentes essenciais:

**Testes de Intrusão (Pentest):** execução de simulações controladas e autorizadas de ataques cibernéticos externos e internos, utilizando metodologias reconhecidas internacionalmente (ex: OSSTMM, PTES, OWASP), para identificação de vulnerabilidades críticas, análise de vetores de ataque e avaliação da resistência da infraestrutura a ameaças reais e persistentes.

**Gestão Integrada de Vulnerabilidades:** realização de varreduras contínuas, catalogação e priorização das vulnerabilidades conforme métricas padrão (CVSS v3.1), análise de impacto e risco, com elaboração de planos detalhados de mitigação, correção e monitoramento evolutivo das falhas identificadas.

**Monitoramento e Resposta a Incidentes:** operação de centro de operações de segurança (SOC) com monitoramento 24/7 dos eventos e logs de segurança, detecção em tempo real de ameaças e anomalias, emissão de alertas imediatos para vulnerabilidades críticas, suporte ágil na contenção, investigação forense e remediação de incidentes.

**Hardening e Fortalecimento da Infraestrutura:** avaliação técnica e implementação de

práticas avançadas de segurança, incluindo configurações seguras (hardening) em sistemas operacionais, bancos de dados, dispositivos de rede e aplicações, minimizando a superfície de ataque e garantindo a conformidade com padrões de segurança reconhecidos.

**Relatórios Dinâmicos e Dashboards Interativos:** fornecimento de relatórios detalhados e painéis gerenciais customizados, atualizados periodicamente, que permitam o acompanhamento da evolução das vulnerabilidades, status das ações corretivas, análise de tendências e suporte para tomada de decisões estratégicas.

**Conformidade Regulatória e Governança:** alinhamento integral às exigências da Lei Geral de Proteção de Dados (LGPD) e às melhores práticas internacionais de segurança da informação (ISO/IEC 27001, NIST Cybersecurity Framework), promovendo governança robusta e proteção dos dados sensíveis da Administração Pública.

**Suporte Técnico Especializado e Capacitação Contínua:** disponibilização de suporte técnico dedicado, consultoria especializada e treinamentos regulares para a equipe de TI municipal, visando o fortalecimento contínuo da postura de segurança organizacional e capacitação para resposta eficaz a incidentes.

7.3. A execução contratual será acompanhada pela equipe técnica da área de tecnologia da informação do Município, com fiscalização contínua das entregas, avaliações periódicas dos indicadores de desempenho, análise dos relatórios e verificação do cumprimento dos níveis de serviço pactuados (SLA). A adoção desta solução tem como objetivo mitigar riscos cibernéticos, garantir a disponibilidade e integridade dos sistemas municipais, fortalecer a governança de segurança da informação e assegurar a continuidade dos serviços públicos essenciais com alta confiabilidade e transparência.

## **8. DA 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 (art.6º, Inc. IX do Anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024)**

8.1. A estimativa das quantidades de serviços a serem contratados foi elaborada com base nas necessidades levantadas junto ao setor responsável e às diversas secretarias do Município de Frecheirinha/CE, considerando a imprescindibilidade de contar com suporte técnico especializado em cibersegurança. O cálculo foi fundamentado em dados históricos de demandas e incidentes registrados, bem como nas diretrizes do planejamento estratégico municipal para a área de segurança da informação, conforme exposto abaixo:

ESPECIFICAÇÃO	UND.	QUANT.
TESTE DE INTRUSÃO (PENTEST).	HORAS	200
GESTÃO DE VULNERABILIDADES SISTEMAS DA SECRETARIA DE ADMINISTRAÇÃO	MÊS	12
GESTÃO DE VULNERABILIDADES SISTEMAS DA SECRETARIA DE EDUCAÇÃO	MÊS	12

GESTÃO DE VULNERABILIDADES SISTEMAS DA SECRETARIA DE SAÚDE	MÊS	12
GESTÃO DE VULNERABILIDADES SISTEMAS DA SECRETARIA DO TRABALHO E ASSISTÊNCIA SOCIAL.	MÊS	12

## 8.2. DA ESTIMATIVA DO VALOR (art.6º, Inc. X do Anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024)

8.2.1. A estimativa do valor da contratação foi realizada com base em pesquisa de preços praticados por outros entes públicos em processos licitatórios voltados à **prestação de serviços especializados em segurança da informação**, compreendendo a execução de análise de vulnerabilidades e testes de invasão (pentest) no ambiente externo de tecnologia da informação, incluindo a emissão de relatórios técnicos com recomendações corretivas e acompanhamento das medidas de mitigação. Foram analisados contratos e registros de preços firmados por órgãos públicos e municípios de porte semelhante ao de Frecheirinha/CE, tais como:

8.2.2. Tabela com quantitativo e demais informações:

DESCRIÇÃO	UND	QUANT	VL. MENSAL
contratação de empresa especializada na prestação de serviços técnicos em segurança da informação, compreendendo os serviços de análise de vulnerabilidades e teste de invasão (pentest) no ambiente externo de tecnologia da informação da controladoria e ouvidoria geral do estado do Ceará – cge sede e suas unidades remotas(central_155 e colocattion), emissão de relatórios e apresentação dos resultados, conforme condições, quantidades e exigências estabelecidas neste termo de referência e seus anexos.	serv	01	R\$ 116.309,52
Contratação de empresa para a execução de serviços técnicos especializados em segurança da informação, para atender as necessidades da câmara municipal de forquilha/ce	mês	05	R\$ 52.650,00

Links consultados:

Licitações | TCE Ceará – Prefeitura Municipal de Fortaleza/CE.

<https://pncp.gov.br/app/editais/07954480000179/2024/24831>

Licitações | TCE Ceará – Prefeitura Municipal de Forquilha/CE.

<https://pncp.gov.br/app/editais/10379642000105/2025/20>

8.3. O custo estimado médio da contratação é de **R\$ 84.479,76 (oitenta e quatro mil, quatrocentos e setenta e nove reais e setenta e seis centavos)**, tomando-se como base os valores praticados em contratações anteriores e similares, bem como em contratações equivalentes realizadas por outros municípios, em conformidade com o Decreto Municipal nº 002/2024.

**9. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO (art.6º, Inc. XI do anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024).**

9.1. Após análise técnica da natureza do objeto e do mercado, foram avaliadas as opções de contratação com parcelamento ou de forma unificada. O parcelamento poderia permitir fornecedores distintos, mas traz riscos de inconsistência, dificuldades de coordenação e exposição de informações sensíveis. A contratação unificada garante responsabilidade técnica completa, integração, confiabilidade e eficácia dos serviços. Portanto, conclui-se que a contratação não será parcelada, por se tratar de solução integrada e indivisível, essencial para a execução eficiente dos serviços de segurança da informação, incluindo análise de vulnerabilidades e testes de intrusão (pentest).

**9.2. Avaliação da Possibilidade de Parcelamento da Solução:**

CRITÉRIO DE AVALIAÇÃO	APLICABILIDADE À CONTRATAÇÃO
A divisão em 's ou fases proporciona maior competitividade no mercado	Pouco aplicável – empresas especializadas em segurança da informação geralmente oferecem o conjunto completo de serviços.
O fracionamento não compromete a funcionalidade do objeto contratado	Não aplicável – a fragmentação comprometeria a integração entre análise de vulnerabilidade e teste de invasão (Pentest)
A segmentação permite maior especialização na prestação dos serviços	Não aplicável – os serviços requerem atuação unificada e contínua.
Existe disponibilidade de fornecedores distintos para cada parcela do serviço	Baixa – fornecedores atuam de forma integrada, prestando todos os serviços em um único pacote.

**9.3. Justificativa para a contratação de forma global (SEM PARCELAMENTO):**

FATOR	DESCRIÇÃO
Natureza Integrada da Solução	Os serviços de segurança da informação englobam ações interligadas, como análise de vulnerabilidades, execução de testes de invasão (pentest), emissão de relatórios técnicos e recomendações de mitigação. A divisão entre prestadores distintos comprometeria a uniformidade e a integração técnica.
Necessidade de Gestão Técnica Unificada	A execução demanda padrões únicos de metodologia, ferramentas, atualização de ameaças cibernéticas e critérios de avaliação de riscos. Um único fornecedor garante consistência e continuidade nas ações.
Economia de Escala e Redução de Custos	A contratação única reduz custos administrativos e operacionais, otimiza fiscalização e garante maior previsibilidade de despesas.



Viabilidade Técnica e Operacional	Empresas especializadas já oferecem soluções completas, evitando a limitação da competitividade e garantindo maior qualidade técnica.
-----------------------------------	---

#### 9.4. Impactos negativos do parcelamento:

RISCOS	IMPACTO POTENCIAL
Incompatibilidade de metodologias	Empresas distintas podem adotar padrões divergentes de análise e teste, gerando inconsistências técnicas.
Dificuldade de Responsabilização	Fragmentação da execução dificulta a apuração de falhas e a responsabilização.
Aumento dos Custos Administrativos	Mais processos licitatórios, contratos e atividades de fiscalização.
Perda de Eficiência e Padronização	A ausência de metodologia única compromete a eficácia das ações de segurança e a mitigação de vulnerabilidades.

9.5. Após análise técnica, operacional e econômica, **não se recomenda o parcelamento** da contratação dos serviços de **segurança da informação**, compreendendo análise de vulnerabilidades e teste de invasão (pentest) no ambiente externo de tecnologia da informação. A contratação de forma unificada garante padronização, eficiência, economia de escala, segurança operacional e jurídica, atendendo aos princípios da Lei nº 14.133/2021 e do Decreto Municipal nº 002/2024.

#### 10. CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES (Lei Federal 14.133/2021, art. 18, § 1º, X e art.6º, Inc. XII do Anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024)

10.1. Conforme o disposto no artigo 18, § 1º, inciso X, da Lei Federal nº 14.133/2021 e no artigo 6º, inciso XII, do Anexo II do Decreto Municipal nº 002/2024, a presente contratação de empresa especializada em serviços de cibersegurança, incluindo testes de intrusão (pentest) e gestão de vulnerabilidades, está diretamente interligada a outras contratações e rotinas de tecnologia da informação correlatas e interdependentes, essenciais para garantir a eficiência, confiabilidade e a segurança da infraestrutura tecnológica do Município de Frecheirinha/CE.

10.2. A atuação da empresa especializada impacta diretamente diversas áreas da administração municipal, abrangendo redes, servidores, estações de trabalho, dispositivos móveis, sistemas internos e externos, exigindo integração com sistemas de gestão pública (ERP municipal) e constante alinhamento às normas de segurança, LGPD e melhores práticas de governança de TI. Dessa forma, a contratação deve estar coordenada com a manutenção, suporte e futuras aquisições de soluções de segurança da informação.

10.3. A prestação dos serviços também está interligada à adoção de ferramentas complementares, como monitoramento contínuo (SOC), sistemas de backup seguro, controle

de acessos, políticas de criptografia, resposta a incidentes e planos de continuidade de negócios, que demandam informações técnicas padronizadas e relatórios especializados oriundos da empresa contratada. Outro ponto de interdependência é a necessidade de capacitação continuada da equipe de TI do Município, garantindo correta interpretação, aplicação das recomendações de segurança e mitigação de vulnerabilidades.

10.4. Portanto, a contratação planejada e integrada dos serviços de cibersegurança contribui para a proteção dos ativos de informação, evita duplicidade de esforços, reduz riscos operacionais e fortalece a segurança jurídica na gestão de dados e sistemas. Além disso, essa medida assegura maior eficiência, controle e transparência, em conformidade com os princípios da Lei nº 14.133/2021 e com o Decreto Municipal nº 002/2024, promovendo uma gestão pública mais segura, moderna e aderente às boas práticas de tecnologia da informação

## **11. DO ALINHAMENTO COM OS INSTRUMENTOS DE PLANEJAMENTO DA ADMINISTRAÇÃO PÚBLICA MUNICIPAL (Lei Federal 14.133/2021, art. 18, § 1º, II e art.6º, Inc. XIII do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024).**

11.1. A presente contratação não se encontra prevista no Plano de Contratações Anual – PCA formalmente instituído para o exercício de 2026. Tal circunstância, contudo, não constitui óbice ao regular prosseguimento da contratação, especialmente por se tratar de demanda necessária ao atendimento do interesse público e compatível com os objetivos estratégicos da Administração. contratação possui previsão na Lei Orçamentária Anual vigente, com recursos devidamente consignados na respectiva dotação orçamentária, conforme demonstrado na própria LOA e comprovado nos autos do procedimento licitatório, conforme dotação orçamentária, informado abaixo:

0301.04.122.0007.2009 - **Gestão Administrativa do Governo Municipal;**

1001.12.122.0007.2036 - **Gestão Administrativa da Secretaria de Educação;**

1101.10.122.0007.2066 - **Gestão Administrativa da Secretaria de Saúde;**

1201.08.122.0007.2.090 - **Gestão Administrativa da Secretaria do Trabalho Assistência Social,**

**Elemento de Despesa: 3.3.90.40.00 – Serv. Tecnologia Informação / Comunic. - P.J.**

## **12. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS (§ 2º do art. 18 da Lei nº 14.133/2021 e art.6º, Inc. XIV do Anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024)**

12.1. A contratação de serviços especializados em segurança da informação, compreendendo a análise de vulnerabilidades e o teste de invasão (pentest) no ambiente externo de tecnologia da informação, tem como objetivo elevar o nível de proteção cibernética do Município de Frecheirinha/CE. Com a execução dos serviços, pretende-se alcançar os seguintes resultados concretos e mensuráveis:

<b>Fortalecimento da Segurança Cibernética</b>	Identificação proativa de vulnerabilidades em sistemas, redes e aplicações utilizadas pela administração municipal;
	Realização de testes controlados de intrusão para

	avaliar a resiliência das defesas tecnológicas;
	Implementação de recomendações técnicas para mitigação imediata dos riscos identificados.
<b>Aprimoramento do Monitoramento e da Resposta a Incidentes</b>	Disponibilização de relatórios técnicos detalhados, contendo nível de criticidade e prioridade das vulnerabilidades;
	Melhoria da capacidade de resposta a incidentes, reduzindo tempo de detecção e contenção de ataques;
	Integração das informações obtidas ao plano municipal da segurança da informação;
<b>Conformidade com Normas e Boas Práticas</b>	Alinhamento às diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normativos aplicáveis;
	Adequação a padrões internacionais de segurança da informação (ISO/IEC 27001, OWASP, NIST);
	Fortalecimento do controle interno e da rastreabilidade das ações.
<b>Capacitação e Sensibilização Técnica</b>	Transferência de conhecimento para a equipe interna de TI, promovendo autonomia na gestão de riscos;
	Elaboração de orientações técnicas e recomendações operacionais para prevenção de novos incidentes;
	Estímulo à cultura organizacional voltada à segurança da informação.
<b>Eficiência Operacional e Sustentabilidade Tecnológica</b>	Redução de custos decorrentes de indisponibilidades ou incidentes de segurança;
	Melhoria da performance e confiabilidade dos serviços digitais prestados à população;
	Garantia de maior continuidade operacional dos sistemas e serviços públicos informatizados.

12.2. Com a execução integral dos serviços contratados, o Município pretende fortalecer a governança de TI, proteger de forma mais efetiva os dados institucionais e pessoais sob sua responsabilidade, reduzir vulnerabilidades e riscos cibernéticos, além de garantir maior confiabilidade, integridade e disponibilidade das informações, promovendo uma gestão pública mais segura, moderna e alinhada às melhores práticas de segurança digital.

### 13. PROVIDÊNCIAS A SEREM ADOTADAS PREVIAMENTE À CELEBRAÇÃO DO CONTRATO (art.6º, Inc. XV do anexo II do Decreto Municipal Nº 002/2024, DE 02 DE JANEIRO DE 2024)

13.1. Em conformidade com o artigo 60, inciso XV, do Anexo II do Decreto Municipal nº 002/2024, algumas providências devem ser observadas previamente à formalização contratual, com o objetivo de assegurar segurança jurídica, eficiência administrativa e conformidade com a legislação vigente na contratação de serviços de segurança da informação, compreendendo a realização de análise de vulnerabilidades e teste de invasão (pentest) no ambiente externo de tecnologia da informação. As principais medidas a serem adotadas são:

**Elaboração e Publicação do Edital de Licitação** → Redação do instrumento convocatório com definição clara do objeto, escopo dos serviços, exigências técnicas e contratuais, critérios de julgamento e mecanismos de controle, garantindo legalidade, isonomia e transparência, em conformidade com a Lei nº 14.133/2021.

**Pesquisa de Mercado e Definição do Valor de Referência** → Levantamento de preços praticados por empresas especializadas em serviços de segurança da informação, com base em cotações, painéis de preços e contratações similares, observando economicidade e vantajosidade.

**Verificação da Compatibilidade Orçamentária** → Avaliação da disponibilidade orçamentária e financeira para a contratação, com previsão em dotação específica e observância da Lei de Responsabilidade Fiscal (LC nº 101/2000).

**Análise de Riscos** → Identificação e mitigação de riscos jurídicos, técnicos, operacionais e financeiros que possam comprometer a eficácia da contratação, nos termos do artigo 25 da Lei nº 14.133/2021.

**Definição de Critérios de Fiscalização e Gestão do Contrato** → Designação de fiscal e gestor do contrato, com atribuições claras para o acompanhamento da execução, conforme estabelece o artigo 117 da Lei nº 14.133/2021.

**Definição de Indicadores de Desempenho** → Estabelecimento de parâmetros de qualidade e metas de segurança cibernética, assegurando efetividade na execução dos serviços e mensuração dos resultados entregues.

**Planejamento da Integração com a Estrutura de TI do Município** → Avaliação da melhor forma de incorporação das atividades de análise de vulnerabilidades e pentest à rotina da Administração, garantindo alinhamento com as políticas e procedimentos internos de segurança.

**Capacitação e Apoio Técnico aos Servidores Envolvidos** → Planejamento de ações de capacitação e orientação aos servidores municipais que atuarão diretamente na execução e fiscalização do contrato, garantindo alinhamento técnico e metodológico com as melhores práticas de segurança da informação.

13.2. A adoção criteriosa dessas providências garantirá que a contratação dos serviços de segurança da informação ocorra com eficiência, segurança jurídica e aderência aos princípios da legalidade, planejamento e interesse público, fortalecendo a proteção dos ativos digitais e a resiliência cibernética do Município.

### 14. DA NÃO PARTICIPAÇÃO DE CONSÓRCIO



14.1. Considerando a natureza técnica e altamente especializada dos serviços de segurança da informação, que envolvem a implementação, monitoramento e gestão de medidas de proteção, prevenção e resposta a incidentes cibernéticos, não será permitida a participação de consórcios na presente contratação. Essa vedação se justifica pelas seguintes razões:

<b>RESPONSABILIDADE TÉCNICA UNIFICADA</b>	A execução do objeto exige atuação direta, contínua e coordenada de uma única empresa especializada em segurança da informação, com equipe própria, qualificada e experiência comprovada em análise de vulnerabilidades e testes de invasão (pentest). A responsabilização única assegura maior controle, transparência e eficiência no cumprimento das metas contratuais.
<b>CONFIDENCIALIDADE E PROTEÇÃO DE DADOS SENSÍVEIS</b>	Os serviços envolvem o acesso e tratamento de informações críticas e sigilosas da infraestrutura tecnológica municipal. A contratação de um único prestador facilita o cumprimento da Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), reduzindo riscos de vazamentos e assegurando a adequada proteção das informações
<b>PADRONIZAÇÃO METODOLÓGICA E TÉCNICA</b>	O trabalho de segurança da informação exige uniformidade na aplicação de metodologias, protocolos e ferramentas de monitoramento, prevenção e resposta a incidentes. A contratação de consórcios poderia comprometer essa padronização, diante de possíveis divergências entre práticas adotadas por empresas distintas, prejudicando a eficácia das medidas
<b>CELERIDADE E EFICIÊNCIA NA EXECUÇÃO CONTRATUAL</b>	A centralização dos serviços em um único contratado contribui para respostas rápidas a incidentes, execução ágil de testes e correções, evitando entraves operacionais decorrentes da divisão de tarefas e responsabilidades entre empresas consorciadas.

14.2. Dessa forma, a vedação à participação de consórcios está fundamentada nos princípios da economicidade, eficiência administrativa, segurança jurídica e no interesse público, garantindo que o Município de Frecheirinha/CE obtenha uma prestação de serviços em segurança da informação alinhada aos seus objetivos estratégicos de proteção de dados, continuidade operacional e conformidade com a legislação vigente, especialmente no que se refere à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018).

## **15. DA DECLARAÇÃO DE VIABILIDADE E DA MODALIDADE DE LICITAÇÃO SUGERIDA**

16.1. A contratação da solução proposta – serviços especializados de segurança da informação, compreendendo análise de vulnerabilidades e teste de invasão (pentest) no

ambiente externo de tecnologia da informação – revela-se viável técnica, operacional, econômica e juridicamente, conforme os estudos e análises constantes neste Estudo Técnico Preliminar.

16.2. A pesquisa de soluções existentes no mercado demonstrou a disponibilidade de empresas especializadas e capacitadas para atender integralmente ao objeto, com preços praticados compatíveis com a realidade orçamentária do Município de Frecheirinha/CE e em consonância com os princípios da economicidade, da eficiência e da seleção da proposta mais vantajosa para a Administração Pública.

16.3. Dessa forma, declara-se viável a contratação da solução, considerando a clareza do objeto, a padronização da demanda, a conformidade com a legislação vigente, especialmente a Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), e a existência de fornecedores aptos no mercado nacional.

16.4. Quanto à modalidade de licitação sugerida, propõe-se a adoção do Pregão, preferencialmente na forma eletrônica, nos termos do art. 28, inciso I, da Lei nº 14.133/2021, uma vez que o objeto se enquadra como serviço comum de tecnologia da informação, com critérios objetivos de julgamento e requisitos técnicos padronizados.

16.5. O julgamento deverá ocorrer pelo critério de menor preço, por item único (solução completa), assegurando a vantajosidade da proposta e a ampla competitividade entre as empresas especializadas.

Apêndice ao ETP – Mapa de Risco.