



CONSELHO REGIONAL DE NUTRIÇÃO 2ª REGIÃO

Av. Taquara, 586, Porto Alegre/RS, CEP 90460-210

Telefone: 51-33309324 - <https://www.crn2.org.br/> - E-mail: crn2@crn2.org.br

TERMO DE REFERÊNCIA

Processo nº 020207.000024/2024-35

1. CONDIÇÕES GERAIS DE CONTRATAÇÃO

1.1. DEFINIÇÃO DO OBJETO

1.1.1. O presente Termo de Referência tem como objeto a contratação de uma empresa especializada no fornecimento de licença e suporte para o software **Bitdefender** na sua versão **Business Security Premium** para **42 (quarenta e dois) dispositivos**, pelo período de **12 (doze) meses**, de acordo com os descritivos e quantitativos do edital e seus anexos.

1.2. DESCRIÇÃO DO OBJETO

1.2.1. A solução precisa ser do tipo solução corporativa de antivírus institucional com gerenciamento centralizado e suporte, e deve contemplar o direito de uso de **42 (quarenta e duas) licenças** de software antivírus, anti-spyware e anti-ransomware, incluindo os serviços de implantação, garantia e atualização contínua, configuração e assistência técnica, pelo período de **12 (doze) meses**.

1.2.2. Especificações técnicas mínimas:

a) A solução deve incluir um servidor de administração centralizado e um console de gerenciamento acessível via web na nuvem, permitindo monitoramento e configuração remota de todos os dispositivos protegidos.

b) A solução deve garantir a segurança de todos os tipos de dispositivos, sejam físicos ou virtualizados, oferecendo proteção abrangente para estações de trabalho, servidores e dispositivos móveis.

c) A plataforma de gerenciamento deve ser consolidada em uma única interface, permitindo a gestão e configuração integrada de antivírus, antispymware, firewall, sistemas de detecção de intrusão, controle de dispositivos, gerenciamento de aplicações e criptografia de discos.

d) A solução deve ser capaz de desinstalar automaticamente o antivírus atualmente em uso e realizar a instalação remota do agente de segurança por meio do console de gerenciamento, sem a necessidade de intervenção manual em cada dispositivo.

1.2.3. O produto deverá possuir, no mínimo, os seguintes módulos e funcionalidade:

a) Console de Gerenciamento: Interface centralizada para gestão e configuração de políticas de segurança, permitindo monitoramento e ajustes em tempo real.

b) Módulos para Diversos Dispositivos: Inclusão de módulos dedicados à proteção de estações de trabalho físicas, notebooks e servidores, assegurando a cobertura completa de todos os tipos de dispositivos utilizados pela organização.

c) Módulo para Ambientes Virtualizados: Módulo específico para ambientes virtuais, oferecendo proteção adaptada e otimizada para esse tipo de infraestrutura.

d) Detecção Proativa de Ameaças (Heurística): Capacidade de identificar códigos maliciosos de forma proativa, utilizando técnicas heurísticas para detectar novos tipos de ameaças, mesmo sem a presença de assinaturas.

e) Proteção Contra Exploração de Vulnerabilidades (Anti-Exploit): A solução deverá oferecer proteção contra a exploração de vulnerabilidades em softwares instalados, reduzindo o risco de infecções. Caso o software desejado não inclua proteção para uma aplicação específica, deverá ser possível adicionar aplicações externas e seus processos para bloquear tentativas de exploração, tanto de vulnerabilidades conhecidas quanto desconhecidas.

f) Tecnologia Anti-Ransomware: Solução nativa para detectar e bloquear ameaças de ransomware, impedindo a criptografia não autorizada de arquivos em recursos compartilhados. Em caso de ataque, a solução deve restaurar os arquivos criptografados ao seu estado original, prevenindo a perda de dados corporativos.

g) Inventário de Software: Capacidade de gerar e manter um inventário detalhado de todos os softwares instalados na rede, facilitando a gestão de atualizações e garantindo a conformidade de segurança.

h) Sandbox em Nuvem: Tecnologia de “sandbox” na nuvem, onde arquivos potencialmente perigosos são analisados em ambiente isolado, na infraestrutura do fabricante, antes de serem executados no ambiente de produção, minimizando riscos de infecção.

i) Proteção Baseada em Assinaturas: O antivírus deverá contar com um mecanismo de proteção baseado em assinaturas (vacinas), garantindo a detecção e bloqueio de ameaças conhecidas.

j) Console de Gerenciamento em Nuvem ou Appliance Virtual: A solução deverá fornecer o console de gerenciamento como um appliance virtual ou como um executável para instalação em servidores Windows, ou disponibilizado diretamente na nuvem do fabricante.

1.2.4.

Características gerais:

a) A solução deve ser completamente em português, garantindo fácil entendimento e uso pelos administradores e equipes responsáveis.

b) Licenciamento flexível, permitindo ajustes conforme a demanda e facilitando a gestão de licenças conforme o crescimento da infraestrutura.

c) A arquitetura de atualização deve ser simples e eficiente, possibilitando a atualização de todas as funções e serviços de segurança com um único clique, garantindo agilidade e minimizando interrupções nos dispositivos.

d) Deve permitir ao administrador escolher quais pacotes de atualização serão aplicados, proporcionando controle total sobre o processo de atualização e a flexibilidade para aplicar mudanças específicas conforme a necessidade.

e) Notificações claras e visíveis devem ser destacadas como itens "não lidos" no sistema, e o administrador deverá ser notificado por e-mail sempre que houver novas atualizações, alertas ou problemas de segurança.

f) O sistema deve enviar notificações para, no mínimo, os seguintes eventos: problemas com licenciamento, alertas de surto de vírus, máquinas desatualizadas, e eventos críticos relacionados ao antimalware, garantindo que o administrador esteja sempre informado sobre o status da segurança.

1.2.5.

Painel de Monitoramento:

a) O painel de monitoramento deve ser baseado em portlets configuráveis, permitindo que o administrador personalize a interface conforme suas necessidades. Cada portlet deve exibir informações claras e relevantes, com, no mínimo, as seguintes especificações: nome do relatório, tipo de relatório e alvo do relatório, garantindo fácil acesso a dados de segurança em tempo real.

1.2.6.

Relatórios:

- a) A solução deve gerar relatórios detalhados para cada serviço de segurança, como antivírus, firewall, controle de dispositivos e detecção de intrusão, proporcionando uma visão abrangente do status da segurança em todos os dispositivos da rede.
- b) A interface de relatórios deve ser intuitiva e de fácil utilização, com uma visualização simplificada, permitindo ao administrador gerar relatórios com facilidade, sem a necessidade de treinamento adicional.
- c) O sistema deve possibilitar o agendamento de relatórios com opção de envio automático por e-mail para qualquer destinatário, conforme a escolha do administrador, garantindo que as partes interessadas recebam as informações pertinentes de forma contínua e em tempo hábil.
- d) Deve ser possível aplicar filtros de agendamento para selecionar a periodicidade dos relatórios e os critérios de envio, permitindo uma personalização completa conforme a necessidade do administrador.
- e) A solução deve manter um arquivo com todas as instâncias de relatórios agendados, facilitando a consulta de relatórios passados e o acompanhamento histórico de dados de segurança.
- f) Os relatórios devem ser exportáveis nos formatos PDF e/ou CSV, oferecendo flexibilidade para análise externa, arquivamento e compartilhamento de informações.
- g) O sistema deve permitir a criação de relatórios dinâmicos diretamente no dashboard, proporcionando ao administrador a capacidade de gerar relatórios personalizados e instantâneos conforme as necessidades do momento.

1.2.7.

Usuários:

- a) A administração de usuários deve ser baseada em regras, permitindo o controle de acesso e permissões de forma granular, de acordo com a função de cada usuário na organização.
- b) A solução deve disponibilizar tipos de usuários pré-definidos, como, por exemplo:
 - I - Administrador: Responsável pela gestão completa dos componentes da solução, com permissões totais para configurar, monitorar e administrar a segurança.
 - II - Administrador de rede: Responsável pela gestão dos serviços de segurança, incluindo a configuração e monitoramento de políticas de segurança em toda a rede.
 - III - Usuário de Relatório: Responsável por monitorar e gerar relatórios de segurança, com permissões limitadas à visualização e criação de relatórios.
- a) Além dos tipos de usuários pré-definidos, deve ser possível customizar tipos de usuários, permitindo a criação de perfis específicos, com permissões adaptadas às necessidades da organização, garantindo a flexibilidade no controle de acesso.

1.2.8.

Logs:

- a) O sistema deve registrar todas as ações dos usuários no console de gerenciamento, mantendo um registro detalhado de cada atividade realizada, como mudanças de configuração, acesso a dados sensíveis e alterações em políticas de segurança.
- b) Deve ser possível detalhar cada ação realizada pelo usuário, com informações sobre o que foi feito, quando e por qual usuário, facilitando auditorias e investigações de incidentes de segurança.
- c) O sistema deve oferecer a possibilidade de busca complexa nos logs, permitindo a consulta filtrada por ações específicas, usuários ou intervalos de tempo, garantindo que o administrador consiga localizar rapidamente registros importantes para análise e diagnóstico.

1.2.9. **Proteção para estações de trabalho e servidores físicos:**

- a) A solução deve permitir a configuração personalizada do escaneamento do antivírus para as estações de trabalho, com as seguintes opções de scan: Scan local: Realização do escaneamento diretamente na máquina local; Scan local/remoto: Realização do escaneamento local e, se necessário, em outros dispositivos remotamente; Scan remoto: Permitir o escaneamento remoto de dispositivos em rede, sem a necessidade de intervenção local no dispositivo.
- b) A solução deve ser compatível com os seguintes sistemas operacionais para estações de trabalho: Windows 10 e Windows 11.
- c) A solução deve oferecer suporte, no mínimo, para os seguintes sistemas operacionais em servidores: Windows Server 2025, Windows Server 2022 e Windows Server 2016.

1.2.10. **Componentes e funcionalidade gerais do antivírus:**

- a) O software deverá fazer scan em tempo real de maneira automática.
- b) Deverá ser configurável para não realizar scan de arquivos conforme necessidade do administrador (por tamanho ou por tipo de extensão, por exemplo).
- c) Deve possuir escaneamento de comportamento heurístico.
- d) Deve fazer escaneamento em tempo real de mídias externas (CD/DVD, discos externos, pen-drives);
- e) Deverá permitir a escolha e configuração das pastas a serem escaneadas.
- f) O antivírus deve ter no mínimo três tipos de detecção: baseado em assinaturas, baseado em heurística, baseado em monitoramento contínuo de processos.
- g) Deverá possuir ferramentas antiphishing com verificação de links (em e-mail ou em sites).
- h) Deverá possuir módulo de firewall, com possibilidade de ser instalado/desinstalado ou não.
- i) Nas estações de trabalho, o módulo de firewall deverá ser possível de configurar o modo invisível tanto em nível de rede local quanto em nível de internet.
- j) Deverá ter módulo de controle de usuário, com características como: bloqueio de acesso à internet, bloqueio de acesso à aplicações definidas pelo administrador, bloqueio de acesso a sites definidos pelo administrador (sejam sites específicos ou por determinado tipo de conteúdo do site).
- k) Deve realizar a inspeção SSL/TLS das estações a fim de proteger contra tráfego criptografado mal intencionado e realizar os bloqueios de sites com melhor precisão.

1.2.11. **Quarentena:**

- a) A solução deve permitir o envio automático de arquivos para quarentena para o laboratório de vírus, garantindo que arquivos suspeitos sejam analisados de forma segura antes de serem liberados ou descartados.
- b) Deve ser possível mover arquivos da quarentena para seu local original ou outro destino que o administrador definir, oferecendo flexibilidade para a gestão de arquivos após a análise de segurança.
- c) A solução deve permitir a criação de exclusões para arquivos restaurados da quarentena, permitindo que arquivos confiáveis sejam recuperados sem a necessidade de reanálise constante, agilizando o processo de recuperação de dados.
- d) A funcionalidade de quarentena deve permitir o escanamento de arquivos na quarentena após as atualizações de assinaturas de vírus, garantindo que novos riscos sejam avaliados com base nas definições mais recentes de malware.

1.2.12. **Instalação e Configuração:**

- a) A instalação e os testes dos produtos devem estar inclusos no custo do produto, sem custos adicionais para o contratante.
- b) A instalação deve ser planejada e executada de forma a minimizar as interrupções no ambiente de produção, com as intervenções sendo estritamente necessárias para a realização da instalação, garantindo que as operações não sejam impactadas.
- c) Durante a execução dos serviços de instalação e configuração, deverá estar presente ao menos um representante do CONTRATANTE, que fará parte da equipe designada para coordenar as atividades, garantindo que todas as necessidades e requisitos sejam atendidos.

1.2.13. **Garantia e Manutenção técnica:**

- a) O prazo de garantia das licenças da solução ofertada deverá ser de no mínimo 12 (doze) meses, contados a partir da data de aceite definitivo do produto, assegurando a cobertura de quaisquer problemas que possam surgir após a implementação.;
- b) A CONTRATADA deve fornecer uma Central de Serviços para abertura de chamados técnicos, com atendimento em horário comercial, das 08:30 às 17:30 de segunda a sexta-feira. A Central de Serviços deve garantir um acordo de nível de serviço (ANS) para iniciar o atendimento em até 12 horas após a abertura do chamado.
- c) A Central de Serviços deve estar disponível por telefone, e-mail ou sistema de suporte online, oferecendo múltiplos canais de contato para a abertura de chamados, de acordo com a conveniência do contratante.
- d) Todos os chamados técnicos deverão ser atendidos via acesso remoto, utilizando-se de softwares apropriados ou, se necessário, com atendimento via telefone, garantindo a resolução eficiente e rápida dos problemas relatados.

1.2.14. **Instalação e Testes:** A assistência para instalação e testes das licenças deverá estar inclusa no custo total do serviço, sem custos adicionais para o contratante. A instalação deverá ser realizada de maneira a minimizar ao máximo as interrupções no ambiente de produção, garantindo que as operações diárias da organização não sejam impactadas, e que o processo de integração seja o mais eficiente possível, respeitando o cronograma acordado.

1.2.15. **Garantia das Licenças:** O prazo de garantia das licenças da solução ofertada será válido durante todo o período de vigência das licenças, assegurando que qualquer eventualidade ou falha técnica seja corrigida dentro do período de cobertura, sem custos adicionais ao contratante, garantindo a continuidade e confiabilidade do serviço durante toda a sua utilização.

1.2.16. O licenciamento da solução deverá ser **de uso único e exclusivo da contratante**, não sendo permitida a transferência, compartilhamento ou sublicenciamento para terceiros. O uso da licença será restrito **somente à contratante**, para a qual a solução foi adquirida, garantindo que os direitos de uso estejam diretamente vinculados à sua estrutura e necessidades operacionais.

2. **FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO**

2.1. A presente contratação visa a aquisição de licenciamento de software antivírus Bitdefender Business Premium, com o intuito de garantir a continuidade e a segurança da infraestrutura tecnológica do Conselho Regional de Nutrição da 2ª Região (CRN-2), em conformidade com os princípios da eficiência, economicidade e da continuidade dos serviços públicos, conforme preconiza a Lei nº 14.133/2021.

2.2. O CRN-2 possui uma infraestrutura tecnológica essencial para o cumprimento de suas atribuições legais, que abrange armazenamento de dados, gestão de sistemas corporativos, documentos administrativos, gestão de usuários, backup e segurança cibernética. A crescente complexidade dos ataques cibernéticos, além da necessidade de garantir a integridade, confidencialidade e disponibilidade

das informações institucionais, torna a implementação de soluções de segurança digital uma necessidade premente.

2.3. A contratação de uma solução de segurança eficiente e integrada é imprescindível para proteger os ativos digitais da autarquia, mantendo a segurança e o bom funcionamento das estações de trabalho, servidores e sistemas. Atualmente, o CRN-2 utiliza a solução Bitdefender Business Premium, que já está plenamente integrada à infraestrutura tecnológica existente e demonstrou ser eficaz no cumprimento das funções de proteção, controle e monitoramento das estações de trabalho. Durante o período de vigência da licença anterior, a solução se revelou vantajosa, atendendo aos requisitos institucionais e proporcionando a continuidade dos serviços sem interrupções ou prejuízos operacionais.

2.4. Com base na experiência positiva anterior e no fato de a solução estar já configurada em todas as 42 estações de trabalho, a aquisição de novas licenças do Bitdefender Business Premium permitirá a manutenção da segurança cibernética, sem custos adicionais relacionados a migrações ou treinamentos extensivos. A substituição do antivírus implicaria não apenas em custos extras com migração, mas também em riscos de incompatibilidade com os sistemas já existentes, o que comprometeria a eficiência operacional e a continuidade dos serviços.

2.5. A contratação do licenciamento do Bitdefender Business Premium está alinhada ao Plano Anual de Contratações do CRN-2 e atende aos requisitos legais e normativos de governança e segurança da informação, conforme estabelecido pela Lei nº 14.133/2021, que impõe a adoção de medidas que garantam a eficiência, a economicidade e a continuidade dos serviços públicos prestados à sociedade.

2.6. Portanto, a necessidade da contratação é justificada pela busca pela continuidade da segurança da informação, pela proteção contra ameaças cibernéticas, pela manutenção da eficiência da infraestrutura tecnológica e pela conformidade com as exigências legais e regulamentares, promovendo, dessa forma, um ambiente seguro e eficiente para o desempenho das atividades institucionais do CRN-2.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

3.1. Solução corporativa de antivírus institucional com gerenciamento centralizado e suporte, e deve contemplar o direito de uso de **42 (quarenta e duas) licenças** de software antivírus, anti-spyware e anti-ransomware, incluindo os serviços de implantação, garantia e atualização contínua, configuração, treinamento e assistência técnica, pelo período de **12 (doze) meses**.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de segurança e privacidade:

a) A CONTRATADA e seus profissionais envolvidos na contratação deverão seguir os seguintes procedimentos e premissas de segurança envolvidos na prestação dos serviços:

I - manter sigilo sobre todo e qualquer assunto de interesse da CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução dos serviços contratados, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;

II - não veicular publicidade acerca do contrato, salvo se houver prévia autorização da CONTRATANTE;

III - manter sigilo de todas as informações a que tiveram acesso inclusive após o término da vigência contratual ou eventual rescisão;

IV - assinar Termo de Compromisso e de Manutenção do Sigilo.

V - atender à legislação vigente, em especial nas questões atinentes à Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, que é a legislação brasileira que regula

as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

4.2. **Requisitos de Experiência Profissional e Requisitos de Formação da Equipe:**

- a) utilizar empregados habilitados e com conhecimentos especializados dos serviços a serem executados, em conformidade com as normas e determinações em vigor;
- b) providenciar a imediata substituição de qualquer profissional que não atenda às necessidades inerentes à execução dos serviços contratados.
- c) guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

5. **DO ESTUDO TÉCNICO PRELIMINAR**

5.1. Nos termos da Lei nº 12.527, de 18 de novembro de 2011, as informações contidas no ETP não podem ser divulgadas por conter informações sigilosas.

6. **CONDIÇÕES DE PARTICIPAÇÃO**

6.1. Poderão participar do certame as empresas que tenham objeto social compatível com o objeto da licitação e que:

- a) comprovem de que a pessoa jurídica tem atividade relacionada com o objeto do certame, mediante a juntada de contrato social e respectivas alterações em que fiquem comprovadas as suas atividades.
- b) sejam legalmente constituídas, com idoneidade econômico-financeira, regularidade jurídico-fiscal e não tenham sofrido penalidade de suspensão do direito de licitar ou contratar com a Administração Pública.
- c) não estejam sob falência, recuperação judicial ou extrajudicial, concurso de credores, dissolução, liquidação, consórcios de empresas, e não sejam controladoras, coligadas ou subsidiárias entre si.
- d) não tenham sido declaradas inidôneas por qualquer órgão da Administração Pública, direta ou indireta, federal, estadual, municipal ou do Distrito Federal.
- e) não poderão se beneficiar do regime diferenciado e favorecido em licitações, concedido às microempresas e empresas de pequeno porte, pela Lei Complementar nº 123/2006, que se enquadrarem em qualquer das exclusões relacionadas no parágrafo quarto do seu artigo terceiro.
- f) não será admitida a participação de empresas estrangeiras que não funcionem no País.
- g) é vedada a sub-contratação total ou parcial do objeto.

7. **DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA**

7.1. Cumprir todas as obrigações relacionadas no Termo de Referência e sua proposta, as quais têm pleno conhecimento e que faz parte integrante deste instrumento.

7.2. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato.

7.3. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

7.4. Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados.

7.5. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

7.6. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo Página 29 de 37 CONSELHO REGIONAL DE NUTRICIONISTAS 2ª REGIÃO (RS) fixado pelo fiscal do contrato, os bens nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

7.7. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos.

7.8. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

- I - Prova de regularidade relativa à Seguridade Social;
- II - certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;
- III - certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;
- IV - Certidão de Regularidade do FGTS – CRF; e
- V - Certidão Negativa de Débitos Trabalhistas – CNDT.

7.9. Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato.

7.10. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

7.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

7.12. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação.

7.13. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021).

7.14. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, Página 30 de 37 CONSELHO REGIONAL DE NUTRICIONISTAS 2ª REGIÃO (RS) da Lei n.º 14.133, de 2021).

7.15. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

7.16. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

- 7.17. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança contratante.
- 7.18. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.
- 7.19. Orientar e treinar seus empregados sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato.
- 7.20. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local de execução do objeto e nas melhores condições de segurança, higiene e disciplina.
- 7.21. Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.
- 7.22. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

8. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

- 8.1. Conferir e atestar as Notas Fiscais/Faturas.
- 8.2. Efetuar o pagamento à Contratada, de acordo com o prazo estabelecido no Aviso de Dispensa Eletrônica, sempre que forem atendidos os requisitos do Termo de Referência, ou indicar as razões da recusa.
- 8.3. Fornecer as informações solicitadas pela Contratada acerca de eventuais problemas verificados na prestação dos serviços.
- 8.4. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada.
- 8.5. Proporcionar todas as facilidades necessárias ao bom andamento dos serviços contratados.
- 8.6. Observar para que, durante a execução do objeto, sejam mantidas todas as condições de qualificações exigidas para a contratação, bem como, a sua compatibilidade com as obrigações assumidas.
- 8.7. Acompanhar e fiscalizar a execução os serviços, através de empregado designado para este fim, na forma prevista no artigo 117 da Lei nº 14.133/2021.
- 8.8. Exigir o cumprimento de todos os compromissos assumidos pela Contratada, de acordo com as especificações do Aviso de Dispensa e seus anexos.
- 8.9. Notificar por escrito à Contratada, sobre imperfeições, falhas ou irregularidades constatadas nos serviços prestados, para que sejam adotadas as medidas corretivas necessárias.
- 8.10. Aplicar as penalidades previstas no Contrato de Prestação de Serviços e Lei nº 14.133/21, sempre que a conduta da pessoa jurídica Contratada ou da pessoa jurídica licitante recomendar essas sanções.
- 8.11. Dirimir as dúvidas que surgirem no curso da execução do objeto.
- 8.12. Providenciar as publicações oficiais pertinentes no DOU.

9. PROPOSTA DE PREÇOS

- 9.1. As empresas interessadas deverão atender, na formulação de suas propostas, as seguintes condições:

a) A proposta, emitida por computador, redigida em língua portuguesa, em papel timbrado da licitante ou identificada com carimbo padronizado com CNPJ e endereço completo, com clareza, sem emendas, rasuras, acréscimos ou entrelinhas, devidamente datada e assinada, como também rubricadas todas as suas folhas pela licitante ou seu representante.

b) Para estipulação do preço global da proposta, a licitante deverá considerar e observar o seguinte:

I - a plataforma deverá funcionar 24 horas por dia, 7 dias por semana.

II - preço total da proposta, em algarismo, expresso em moeda corrente nacional (real), com 02 (duas) casas decimais após a vírgula e, de acordo com a estimativa de preços praticados no mercado e proposto no Aviso.

III - declaração expressa de que no preço cotado estão incluídos todos os custos necessários e despesas inerentes à prestação dos serviços licitados, tais como todos os impostos, encargos trabalhistas, previdenciários, fiscais e comerciais, deslocamentos de pessoal, e quaisquer outros custos ou despesas que incidam ou venham a incidir direta ou indiretamente sobre o fornecimento dos serviços constantes da proposta, abrangendo, assim, todos os custos necessários ao fornecimento do objeto e a manutenção destas condições durante a vigência do Contrato.

IV - indicação do prazo de validade da proposta não inferior a 60 (sessenta) dias, a contar da data de abertura do certame. Caso este prazo não esteja expressamente indicado na proposta, o mesmo será considerado de 60 (sessenta) dias correntes.

10. JULGAMENTO DAS PROPOSTAS

10.1. Será considerada vencedora a proposta que ofertar o menor preço global, observada classificação final após os lances e cuja proponente atenda às condições de habilitação, na forma das normas regulamentadoras das licitações na modalidade de dispensa eletrônica.

11. SOBRE OS PAGAMENTOS

11.1. O pagamento será feito através de boleto bancário ou transferência bancária em conta de titularidade da Contratada, quando da entrega da nota fiscal na sede do CRN-2, sujeitando-se às seguintes regras:

a) a NF/Fatura de prestação dos serviços deverá ser encaminhada ao e-mail coordadm@crn2.org.br logo a execução do serviço, com as devidas retenções de impostos (IR, CSLL, COFINS, PIS/PASEP, INSS E ISS), juntamente com as certidões de INSS e FGTS atualizadas;

b) a NF/Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta online ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021;

c) constando-se, junto ao SICAF, a situação de irregularidade da empresa Contratada, deverão ser tomadas as providências previstas no art. 31 da Instrução Normativa nº 03, de 26 de abril de 2018;

d) havendo erro na apresentação da NF/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando ônus para a Contratante;

e) encontrando-se a empresa inadimplente junto ao INSS e FGTS na data do pagamento, poderá ser concedido, a critério do CRN2, prazo de até 15 (quinze) dias para que a

empresa regularize a sua situação, sob pena de, não o fazendo, ter o contrato rescindido com aplicação das sanções cabíveis;

f) os valores ficam condicionados à prévia certificação quanto à execução a contento dos serviços;

g) o pagamento será feito em até 10 (cinco) dias úteis após a entrega da NF/Fatura ao CRN-2;

h) não serão efetuados quaisquer pagamentos enquanto perdurar pendência de liquidação de obrigações, em virtude de penalidades impostas à Contratada, ou inadimplência contratual.

12. **CUSTOS ESTIMADOS**

12.1. O custo total estimado para esta contratação é de **R\$ 4.190,00 (quatro mil cento e noventa reais)**.

13. **DOTAÇÃO ORÇAMENTÁRIA**

13.1. Os recursos para custeio das despesas decorrentes da contratação que se seguir à licitação de que trata este Termo de Referência correrão à conta da dotação orçamentária 6.2.2.1.1.01.04.04.005 para o exercício de 2025.

14. **LOCAL E DATA**

14.1. Porto Alegre, 03 de fevereiro de 2025.

15. **RESPONSÁVEIS PELA ELABORAÇÃO**

15.1. Jaudir Schaun da Cruz, Assessor de Tecnologia da Informação.



Documento assinado eletronicamente por **Jaudir da Cruz, Assessor(a) de Tecnologia da Informação**, em 07/02/2025, às 15:18, conforme horário oficial de Brasília, com fundamento no §2º, do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site http://sei.cfn.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1865391** e o código CRC **98E08999**.