ESTUDO TÉCNICO PRELIMINAR (ETP)

Processo SEI nº 00242.002785/2026-50
Interessado: Departamento de Tecnologia da Informação – DTI
Objeto: Contratação de empresa para fornecimento de solução de antivírus corporativo, com licenciamento, instalação, treinamento, suporte técnico, garantia e atualização.
Unidade Requisitante: Departamento de Tecnologia da Informação – DTI
Responsável pela demanda: Eduardo Lessa de Andrade Cavalcanti
Equipe designada: Eduardo Lessa de Andrade Cavalcanti e Guilherme Fernando de Moura Silva, conforme Portaria COREN-PE nº 1106/2026.

1. INTRODUÇÃO

O presente Estudo Técnico Preliminar tem por finalidade analisar a viabilidade técnica, operacional, econômica e administrativa da contratação de empresa especializada para fornecimento de solução corporativa de segurança para endpoints, abrangendo licenciamento, instalação, desinstalação, configuração, treinamento, suporte técnico, garantia e atualizações durante o período de 12 meses.

A contratação pretendida destina-se à proteção dos ativos tecnológicos do Conselho Regional de Enfermagem de Pernambuco – COREN-PE, incluindo estações de trabalho, notebooks, servidores e demais equipamentos institucionais que demandem proteção ativa contra ameaças digitais, tais como malwares, ransomware, spywares, tentativas de exploração de vulnerabilidades, acessos indevidos e demais códigos maliciosos capazes de comprometer a segurança, a integridade, a confidencialidade e a disponibilidade das informações institucionais.

O estudo foi elaborado com base no Documento de Formalização da Demanda, na Portaria de designação da equipe responsável, nas necessidades técnicas identificadas pelo Departamento de Tecnologia da Informação e nas diretrizes aplicáveis às contratações públicas de soluções de Tecnologia da Informação e Comunicação.

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

O COREN-PE depende de ambiente tecnológico seguro, estável e monitorado para a execução de suas atividades administrativas, finalísticas, fiscalizatórias e institucionais. A tramitação de processos, o atendimento aos profissionais de enfermagem, a operação de sistemas corporativos, o armazenamento de dados, a comunicação institucional e a execução de rotinas internas dependem diretamente da integridade e disponibilidade dos equipamentos e sistemas utilizados pelo Conselho.

Nesse contexto, a proteção dos endpoints institucionais constitui medida essencial de segurança da informação. Estações de trabalho, notebooks, servidores e demais dispositivos conectados à rede institucional representam pontos críticos de acesso ao ambiente tecnológico e, caso não estejam adequadamente protegidos, podem se tornar vetores de infecção, vazamento de dados, paralisação de

serviços, sequestro de informações, comprometimento de credenciais e propagação de ameaças para outros ativos da infraestrutura.

A ausência de solução corporativa de antivírus ativa, atualizada e gerenciada centralmente expõe a Autarquia a riscos relevantes, especialmente diante do crescimento de ameaças cibernéticas, ataques de ransomware, tentativas de phishing, exploração de vulnerabilidades e acesso indevido a ambientes corporativos.

A contratação, portanto, visa assegurar a continuidade da proteção tecnológica institucional, reduzir riscos de incidentes de segurança da informação, preservar a disponibilidade dos serviços digitais e manter ambiente operacional compatível com as necessidades do COREN-PE.

3. ALINHAMENTO INSTITUCIONAL E ESTRATÉGICO

A contratação está alinhada ao objetivo estratégico de manutenção da infraestrutura física, administrativa e tecnológica do Conselho Regional, bem como à iniciativa de manutenção da infraestrutura necessária ao desenvolvimento dos processos de trabalho.

Conforme indicado no DFD, a demanda encontra-se vinculada ao objetivo estratégico **OE6 – Manter a infraestrutura física, administrativa e tecnológica do Conselho Regional**, bem como à iniciativa estratégica relacionada à **manutenção da infraestrutura do Conselho Regional para o desenvolvimento dos processos de trabalho**.

A contratação também se mostra compatível com as boas práticas de governança de TIC, segurança da informação, continuidade de serviços e proteção de dados institucionais, uma vez que a solução pretendida atua diretamente na mitigação de riscos tecnológicos capazes de impactar as atividades administrativas e finalísticas do Conselho.

4. ÁREA REQUISITANTE E ÁREA TÉCNICA

A área requisitante da solução é o Departamento de Tecnologia da Informação do COREN-PE, unidade responsável pela identificação da necessidade, acompanhamento técnico da solução, suporte à implantação, definição dos requisitos mínimos e monitoramento da execução contratual.

Considerando a natureza eminentemente tecnológica do objeto, a área requisitante e a área técnica coincidem no âmbito do Departamento de Tecnologia da Informação, sem prejuízo da atuação da área administrativa competente nas etapas de instrução processual, seleção do fornecedor, formalização contratual e acompanhamento dos aspectos administrativos da contratação.

5. REQUISITOS DA CONTRATAÇÃO

A solução a ser contratada deverá atender, no mínimo, aos seguintes requisitos técnicos, operacionais e administrativos:

5.1. Requisitos técnicos mínimos

A solução deverá contemplar:

a) fornecimento de **300 licenças/hosts** de solução corporativa de segurança para endpoints;
b) vigência de licenciamento pelo período de **12 meses**;
c) proteção para estações de trabalho, notebooks, servidores e demais ativos tecnológicos institucionais;
d) proteção contra malwares, ransomware, spywares, códigos maliciosos, tentativas de exploração de vulnerabilidades, acessos indevidos e ameaças correlatas;
e) atualização automática da solução e das bases de detecção disponibilizadas pelo fabricante;
f) gerenciamento centralizado dos endpoints protegidos;
g) aplicação e administração de políticas de segurança;
h) monitoramento do status dos equipamentos protegidos;
i) emissão de alertas, registros de eventos e relatórios gerenciais;
j) recursos de prevenção, detecção e resposta a ameaças;

k) compatibilidade com o ambiente tecnológico atualmente utilizado pelo COREN-PE;
l) suporte à instalação, desinstalação, configuração e ativação remota;
m) suporte técnico durante toda a vigência contratual;
n) treinamento ou orientação técnica mínima para adequada utilização da solução pela equipe de TIC.

5.2. Requisitos de segurança da informação

A solução deverá preservar a confidencialidade, integridade e disponibilidade das informações institucionais, devendo possibilitar:

a) controle centralizado das políticas de proteção;
b) rastreabilidade mínima de eventos e alertas de segurança;
c) registro de ocorrências relevantes;
d) atualização contínua contra ameaças conhecidas e emergentes;
e) resposta célere a incidentes;
f) redução da exposição dos endpoints a ameaças digitais;
g) mitigação de riscos de vazamento, perda, sequestro ou indisponibilidade de dados.

5.3. Requisitos de suporte, garantia e atualização

Durante toda a vigência contratual, deverão estar incluídos:

a) direito de uso da solução;
b) suporte técnico;
c) garantia de funcionamento;
d) atualizações da solução e das bases de detecção;
e) apoio técnico remoto para instalação, desinstalação, configuração e resolução de falhas;
f) orientações à equipe de TIC para administração e uso adequado da solução.

5.4. Requisitos de compatibilidade e continuidade

A solução deverá ser compatível com o ambiente tecnológico atualmente utilizado pelo COREN-PE, abrangendo equipamentos físicos ou virtuais, observados os sistemas operacionais em uso e suportados pelos respectivos fabricantes.

Considerando que o COREN-PE já utiliza solução corporativa de segurança com licenciamento, instalação, suporte, garantia e atualizações, a contratação deverá preservar a continuidade operacional, evitando interrupção da proteção, perda de configurações, exposição temporária dos ativos, retrabalho de implantação e prejuízo ao funcionamento regular dos serviços institucionais.

5.5. Requisitos de competitividade e não restrição indevida

A indicação de marca ou modelo de referência deverá ser compreendida como parâmetro técnico destinado à preservação da compatibilidade, continuidade operacional, padronização e redução de riscos de descontinuidade da proteção dos endpoints.

Caso seja mantida a exigência da solução atualmente utilizada, recomenda-se que a contratação seja estruturada de modo a permitir disputa entre empresas aptas ao fornecimento do licenciamento, suporte e serviços correlatos, especialmente revendas, distribuidores ou canais autorizados, quando aplicável, evitando-se direcionamento indevido a fornecedor específico.

A eventual restrição à aceitação de solução equivalente deverá estar tecnicamente motivada no processo, com demonstração objetiva dos riscos de migração, incompatibilidade, perda de gerenciamento, necessidade de reconfiguração, retrabalho de implantação, custos indiretos e exposição temporária dos ativos tecnológicos.

6. LEVANTAMENTO DE MERCADO E ANÁLISE DAS ALTERNATIVAS

Foram consideradas, em nível preliminar, as seguintes alternativas para atendimento da necessidade administrativa:

6.1. Alternativa 1 — Renovação/fornecimento da solução corporativa atualmente utilizada

Consiste na contratação de licenciamento da solução corporativa de segurança para endpoints já integrada ao ambiente do COREN-PE, com manutenção do gerenciamento centralizado, políticas de segurança, rotinas de monitoramento, atualizações, suporte técnico e continuidade da proteção dos equipamentos institucionais.

Essa alternativa apresenta vantagens relevantes, tais como:

a) continuidade operacional;
b) redução de riscos de desproteção temporária;
c) preservação de configurações e políticas já existentes;
d) menor necessidade de retrabalho de implantação;
e) menor curva de aprendizado pela equipe técnica;
f) menor risco de incompatibilidade com o ambiente atual;
g) manutenção da padronização tecnológica;
h) possibilidade de disputa entre fornecedores autorizados, se tecnicamente viável.

6.2. Alternativa 2 — Substituição por nova solução corporativa equivalente

Consiste na contratação de solução distinta de segurança para endpoints, com implantação de nova plataforma, novas políticas, reconfiguração dos equipamentos, eventual remoção da solução anterior, treinamento da equipe técnica e migração do ambiente.

Embora essa alternativa possa ser tecnicamente possível, apresenta riscos e custos indiretos relevantes, especialmente em razão da necessidade de migração, reconfiguração de políticas, adaptação operacional, eventual indisponibilidade temporária da proteção e maior esforço técnico para implantação.

No caso concreto, considerando a urgência da demanda, a essencialidade da proteção dos endpoints e o prazo de vigência de 12 meses, a substituição da solução atualmente utilizada pode não se mostrar a alternativa mais eficiente, salvo se demonstrada vantagem técnica e econômica significativa em pesquisa de mercado.

6.3. Alternativa 3 — Utilização de soluções gratuitas, domésticas ou individualizadas

Consiste na utilização de antivírus gratuitos, versões domésticas ou soluções instaladas isoladamente em cada equipamento, sem gerenciamento centralizado corporativo.

Essa alternativa não se mostra adequada ao ambiente institucional do COREN-PE, pois não atende satisfatoriamente aos requisitos de administração centralizada, monitoramento, emissão de relatórios, aplicação uniforme de políticas, suporte técnico institucional e gestão integrada dos endpoints.

Além disso, soluções gratuitas ou domésticas geralmente não são concebidas para ambiente corporativo público, podendo gerar fragilidade de controle, ausência de suporte adequado e dificuldade de responsabilização.

6.4. Alternativa 4 — Não contratação

A não contratação não é alternativa tecnicamente aceitável, pois deixaria os endpoints institucionais sem proteção corporativa adequada, expondo o Conselho a riscos de incidentes de segurança da informação, indisponibilidade de sistemas, perda de dados, sequestro de informações, comprometimento de credenciais e paralisação de atividades administrativas e finalísticas.

7. JUSTIFICATIVA TÉCNICA E ECONÔMICA DA SOLUÇÃO ESCOLHIDA

A solução mais adequada, à luz das informações disponíveis nesta fase preliminar, é a contratação de solução corporativa de segurança para endpoints com licenciamento para 300 hosts, pelo período de 12 meses, contemplando gerenciamento centralizado, atualizações, suporte técnico, instalação, desinstalação, configuração remota, garantia e treinamento.

Recomenda-se, tecnicamente, a manutenção da solução atualmente utilizada, indicada no DFD como **Bitdefender GravityZone Business Security**, desde que a instrução processual demonstre a compatibilidade técnica, a continuidade operacional, a redução de riscos e a vantajosidade em comparação com alternativas de substituição.

A escolha se justifica porque a segurança dos endpoints é componente crítico da infraestrutura tecnológica institucional, sendo indispensável para a proteção dos equipamentos, sistemas e dados do COREN-PE. A manutenção de solução já integrada ao ambiente reduz riscos operacionais, evita retrabalho, preserva políticas existentes e contribui para continuidade da proteção tecnológica.

Do ponto de vista econômico, a manutenção da solução atual tende a reduzir custos indiretos relacionados à migração, reconfiguração, treinamento ampliado, reimplantação e eventual descontinuidade temporária da proteção, sem prejuízo da necessidade de validação do preço por meio de pesquisa de mercado adequada na etapa própria da instrução.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução pretendida compreende a contratação de empresa especializada para fornecimento de licenciamento corporativo de segurança para endpoints, contemplando 300 licenças/hosts pelo período de 12 meses, com os seguintes componentes integrados:

a) fornecimento das licenças de uso;
b) disponibilização de console de gerenciamento centralizado;
c) proteção ativa dos endpoints institucionais;
d) atualização automática da solução e das bases de detecção;
e) aplicação de políticas de segurança;
f) monitoramento do status dos equipamentos protegidos;
g) emissão de alertas, registros e relatórios;
h) suporte técnico remoto;
i) instalação, desinstalação, ativação e configuração remota, conforme necessidade do DTI;
j) treinamento ou orientação técnica para uso da solução;
k) garantia e suporte durante toda a vigência contratual.

A execução deverá abranger a sede do COREN-PE, subseções e demais unidades institucionais que possuam equipamentos abrangidos pela solução, admitindo-se ativação, configuração, gerenciamento e suporte de forma remota, conforme necessidade do Departamento de Tecnologia da Informação.

9. ESTIMATIVA DAS QUANTIDADES E MEMÓRIA DE CÁLCULO

A quantidade estimada para a contratação é de **300 licenças/hosts**, conforme DFD corrigido.

A estimativa considera a necessidade de cobertura dos endpoints institucionais do COREN-PE, incluindo estações de trabalho, notebooks, servidores e demais ativos tecnológicos que demandem proteção ativa.

A adoção do quantitativo de 300 licenças/hosts busca assegurar margem operacional suficiente para cobrir o parque tecnológico atualmente existente, eventuais substituições, equipamentos em implantação, crescimento moderado da infraestrutura e necessidade de manutenção da proteção em todas as unidades institucionais abrangidas.

Recomenda-se que, para reforço da instrução processual, seja juntada aos autos, quando disponível, planilha ou relatório interno do DTI contendo demonstrativo do parque tecnológico estimado, com indicação aproximada de estações de trabalho, notebooks, servidores e demais ativos protegidos ou a proteger.

10. ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO

O valor estimado preliminar constante do DFD é de **R$ 22.800,00**, considerando 300 unidades ao valor unitário estimado de **R$ 76,00**.

A estimativa de valor deverá ser ratificada na etapa própria de pesquisa de preços, observando-se os parâmetros normativos aplicáveis, contratações similares, painéis oficiais, consultas a fornecedores, preços praticados por outros órgãos públicos, valores de mercado e eventuais referências de licenciamento disponibilizadas pelo fabricante ou por canais autorizados.

A estimativa constante deste ETP possui caráter preliminar e deve subsidiar a avaliação inicial de viabilidade econômica, sem prejuízo da consolidação do orçamento estimado pela área competente na sequência da instrução.

11. JUSTIFICATIVA PARA O NÃO PARCELAMENTO

O objeto deverá ser contratado de forma global, sem parcelamento, considerando a natureza integrada da solução.

O fornecimento de licenciamento, instalação, configuração, suporte técnico, garantia, atualizações, treinamento e gerenciamento centralizado integra uma única solução tecnológica de segurança para endpoints. A divisão do objeto em itens ou lotes distintos poderia gerar fragmentação de responsabilidades, dificuldades de integração, inconsistência na aplicação de políticas de segurança, aumento da complexidade da gestão contratual e risco de prejuízo à continuidade da proteção.

Além disso, a contratação global favorece a uniformidade tecnológica, a responsabilização direta da contratada, a padronização do ambiente de segurança, a simplificação da fiscalização e a mitigação de riscos operacionais.

Dessa forma, o não parcelamento mostra-se tecnicamente justificado e adequado à natureza da solução pretendida.

12. SISTEMA DE REGISTRO DE PREÇOS

Não se recomenda, nesta demanda específica, a adoção do Sistema de Registro de Preços, considerando que o quantitativo já se encontra definido, a necessidade é concreta, imediata e vinculada à proteção do parque tecnológico institucional pelo período de 12 meses.

A contratação pretendida não apresenta, neste momento, característica de demanda eventual, futura ou incerta que justifique a formação de ata de registro de preços.

13. CONTRATAÇÕES CORRELATAS E INTERDEPENDENTES

Identifica-se a existência de contratação anterior relacionada ao objeto, conforme referência constante do DFD ao Processo SEI nº 00242.636/2022-COREN-PE.

A contratação ora pretendida guarda relação de continuidade com a proteção tecnológica já existente, sendo importante que a nova contratação preserve a transição regular entre o licenciamento anterior e o novo período de cobertura, a fim de evitar descontinuidade da proteção dos endpoints.

Não se identificam contratações interdependentes indispensáveis à execução do objeto, uma vez que a solução será aplicada sobre infraestrutura tecnológica já existente. Contudo, sua adequada execução depende da atuação coordenada do Departamento de Tecnologia da Informação, especialmente quanto à disponibilização de informações sobre equipamentos, acessos administrativos necessários, validação da ativação das licenças e acompanhamento da configuração.

14. PREVISÃO NO PLANO DE CONTRATAÇÕES ANUAL E ADEQUAÇÃO ORÇAMENTÁRIA

Conforme indicado no DFD, a contratação encontra-se prevista no Plano de Contratações Anual e possui natureza de Tecnologia da Informação e Comunicação.

A dotação/classificação orçamentária indicada no DFD é **6.2.2.1.1.01.33.90.039.002.014 – Serviços relacionados a Tecnologia da Informação**, com fonte de recursos próprios.

A efetiva disponibilidade orçamentária deverá ser confirmada pela unidade competente antes da formalização da contratação, observadas as normas internas de planejamento, orçamento e execução da despesa.

15. RESULTADOS PRETENDIDOS

Com a contratação, pretende-se alcançar os seguintes resultados:

a) manter proteção contínua dos endpoints institucionais do COREN-PE;
b) reduzir riscos de infecção por malwares, ransomware, spywares e demais ameaças digitais;
c) preservar a integridade, confidencialidade e disponibilidade das informações institucionais;
d) assegurar gerenciamento centralizado da solução de segurança;
e) manter políticas uniformes de proteção nos equipamentos abrangidos;
f) possibilitar monitoramento, emissão de alertas e geração de relatórios;
g) reduzir a exposição dos ativos tecnológicos a incidentes de segurança;
h) preservar a continuidade das atividades administrativas, fiscalizatórias e finalísticas do Conselho;
i) garantir suporte técnico e atualizações durante todo o período de vigência;
j) evitar descontinuidade da proteção tecnológica institucional.

16. PROVIDÊNCIAS PRÉVIAS À CONTRATAÇÃO

Antes da formalização e início da execução contratual, recomenda-se a adoção das seguintes providências:

a) confirmação do quantitativo final de endpoints a serem protegidos;
b) conferência do parque tecnológico institucional pelo DTI;
c) validação da existência de console de gerenciamento, credenciais administrativas e políticas atualmente aplicadas;
d) verificação do prazo de expiração da solução atualmente em uso, quando aplicável;
e) definição dos servidores responsáveis pelo acompanhamento técnico da execução;
f) definição de gestor e fiscais do contrato, conforme etapa própria;
g) elaboração do Termo de Referência com requisitos técnicos mínimos, obrigações da contratada, prazos, critérios de aceitação, suporte, sanções e condições de pagamento;
h) realização de pesquisa de preços;
i) confirmação da disponibilidade orçamentária;
j) definição de cronograma de ativação, renovação ou implantação das licenças;
k) previsão de mecanismos de comprovação da entrega/ativação das licenças.

17. SUSTENTABILIDADE E IMPACTOS AMBIENTAIS

A contratação possui baixo impacto ambiental direto, por se tratar de solução de software/licenciamento, com execução predominantemente digital e suporte remoto.

A adoção de instalação, configuração e suporte remoto contribui para redução de deslocamentos, emissão de documentos físicos e consumo de recursos materiais. Não há previsão de aquisição de equipamentos físicos, descarte de bens, geração de resíduos ou necessidade de logística reversa.

Recomenda-se, sempre que possível, que comunicações, relatórios, comprovantes, certificados de licenciamento e documentos de suporte sejam emitidos em meio eletrônico.

18. SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS

Considerando que o objeto da contratação envolve solução de segurança para endpoints e eventual tratamento indireto de informações técnicas do ambiente institucional, a contratada deverá observar requisitos mínimos de segurança da informação e privacidade.

Deverão ser previstas no Termo de Referência obrigações quanto à confidencialidade das informações acessadas, uso restrito de dados técnicos do ambiente, não divulgação de informações institucionais, proteção de credenciais, registro de atendimentos técnicos, responsabilização por condutas indevidas e comunicação de incidentes relacionados à execução contratual.

A contratação deverá observar, no que couber, a Lei Geral de Proteção de Dados Pessoais – LGPD, especialmente quanto à segurança, prevenção, responsabilização e adoção de medidas técnicas e administrativas aptas a proteger dados pessoais e informações institucionais.

19. ANÁLISE DE RISCOS PRELIMINAR

Risco identificado	Impacto	Medida preventiva/mitigadora
Descontinuidade da proteção dos endpoints	**Alto**	**Planejar ativação antes do término da cobertura atual e exigir prazo curto de entrega/ativação.**
Atraso na entrega ou ativação das licenças	**Alto**	**Estabelecer prazo de execução de até 10 dias e prever sanções por descumprimento.**
Incompatibilidade da solução com o ambiente institucional	**Alto**	**Exigir compatibilidade com sistemas operacionais e ambiente tecnológico em uso.**
Perda de configurações e políticas de segurança	**Médio/Alto**	**Priorizar continuidade da solução já integrada ou exigir plano de migração assistida.**
Restrição indevida de competitividade	**Alto**	**Justificar tecnicamente eventual especificação de solução específica e permitir disputa entre fornecedores aptos.**
Suporte técnico insuficiente	**Médio/Alto**	**Prever requisitos mínimos de suporte, canais de atendimento e prazos de resposta.**
Quantitativo insuficiente	**Alto**	**Validar previamente inventário de equipamentos e manter quantitativo de 300 licenças/hosts.**
Falha na comprovação da entrega	**Médio**	**Exigir comprovação formal de ativação/licenciamento e validação pelo DTI.**
Exposição de informações técnicas do ambiente	**Alto**	**Prever cláusulas de confidencialidade, segurança da informação e proteção de dados.**

20. MODELO DE EXECUÇÃO E FISCALIZAÇÃO

A execução contratual deverá ser acompanhada pelo Departamento de Tecnologia da Informação, que verificará a disponibilização das licenças, a ativação da solução, a compatibilidade com o ambiente institucional, a manutenção da proteção dos endpoints, a prestação de suporte técnico e a atualização da solução durante a vigência contratual.

A fiscalização deverá observar, entre outros aspectos:

a) entrega ou ativação das 300 licenças/hosts;
b) validade do licenciamento por 12 meses;
c) funcionamento do gerenciamento centralizado;
d) atualização da solução e das bases de detecção;
e) disponibilidade de suporte técnico;
f) atendimento às solicitações do DTI;
g) manutenção da proteção dos endpoints;
h) emissão de comprovantes, relatórios ou evidências de licenciamento;
i) conformidade com as obrigações contratuais.

21. FORMA DE SELEÇÃO DO FORNECEDOR

Do ponto de vista técnico, o objeto possui características de solução comum de TIC, uma vez que seus padrões de desempenho e qualidade podem ser definidos objetivamente no Termo de Referência, por meio de especificações usuais de mercado.

A definição da modalidade ou forma de contratação deverá ser realizada pela área competente de licitações e contratos, com o apoio jurídico quando necessário, considerando o valor estimado, a urgência indicada no DFD, a natureza do objeto, a possibilidade de contratação direta e os requisitos legais aplicáveis.

Tecnicamente, recomenda-se que a seleção preserve a ampla competitividade possível, observadas as justificativas de compatibilidade, continuidade operacional e padronização, especialmente caso seja mantida a indicação da solução atualmente utilizada.

22. VIGÊNCIA CONTRATUAL

A vigência pretendida é de 12 meses, correspondente ao período de licenciamento, garantia, suporte técnico e atualizações da solução.

Considerando a natureza contínua da proteção de endpoints, recomenda-se que o instrumento contratual ou equivalente preveja mecanismos que assegurem a continuidade da cobertura durante todo o período contratado, inclusive quanto à renovação das bases de detecção, atualização da solução, suporte técnico e manutenção do gerenciamento centralizado.

23. DECLARAÇÃO DE VIABILIDADE

Diante da análise realizada, conclui-se pela **viabilidade técnica, operacional e econômica preliminar** da contratação de empresa para fornecimento de solução corporativa de segurança para endpoints, contemplando 300 licenças/hosts, pelo período de 12 meses, com gerenciamento centralizado, atualizações, suporte técnico, instalação, desinstalação, configuração remota, treinamento e garantia.

A contratação mostra-se necessária, adequada e proporcional à necessidade institucional identificada, pois visa preservar a segurança dos equipamentos, sistemas e dados do COREN-PE, reduzir riscos de incidentes de segurança da informação e assegurar a continuidade das atividades administrativas e finalísticas da Autarquia.

Recomenda-se o prosseguimento da instrução processual, com elaboração do Termo de Referência, realização da pesquisa de preços, confirmação da disponibilidade orçamentária, definição da forma de contratação pela área competente e adoção das providências necessárias à formalização da contratação.

Recife-PE, 25 de maio de 2026.

EDUARDO LESSA DE ANDRADE CAVALCANTI
Chefe do Departamento de Tecnologia da Informação
COREN-PE

GUILHERME FERNANDO DE MOURA SILVA
Assessor de Tecnologia da Informação
COREN-PE

Documento assinado eletronicamente por **EDUARDO LESSA DE ANDRADE CAVALCANTI - Matr. 130**, **Chefe do Departamento de Tecnologia da Informação**, em 25/05/2026, às 08:17, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **GUILHERME FERNANDO DE MOURA SILVA - Matr. 195**, **Chefe do Setor de Suporte Tecnológico**, em 26/05/2026, às 09:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.cofen.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1797286** e o código CRC **EE14728A**.

Referência: Processo nº 00242.002785/2026-50 SEI nº 1797286