CONSELHO REGIONAL DE MEDICINA DO ESTADO DO TOCANTINS

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO

1. INTRODUÇÃO

1.1. Este Estudo Técnico Preliminar (ETP) é a primeira etapa do planejamento da contratação e tem como finalidade avaliar, de forma detalhada, a viabilidade técnica, operacional e econômica da contratação de Serviços Gerenciados de Segurança da Informação para o Conselho Regional de Medicina do Estado do Tocantins (CRMTO).

1.2. O documento fundamenta-se na Lei nº 14.133/2021, que estabelece normas gerais de licitação e contratação, e segue as boas práticas de governança de TI e segurança da informação, bem como diretrizes de órgãos de controle, como TCU e CGU.

1.3. O CRM-TO, por meio desta contratação, busca fortalecer sua segurança cibernética de forma abrangente, mitigando riscos e garantindo proteção contínua a seus sistemas, dados e usuários.

2. DESCRIÇÃO DA NECESSIDADE

2.1. O CRM-TO enfrenta desafios significativos em sua infraestrutura tecnológica, composta por servidores, estações de trabalho e sistemas críticos que armazenam dados sensíveis, incluindo informações pessoais e profissionais de médicos registrados.

2.2. Entre os problemas identificados, destacam-se:

2.2.1. Ausência de soluções de proteção de rede e endpoints;
2.2.2. Vulnerabilidade a ataques cibernéticos (ransomware, phishing, DDoS, invasões);
2.2.3. Risco de perda ou indisponibilidade de dados devido à falta de backups gerenciados;
2.2.4. Dificuldade da equipe interna em acompanhar, de forma proativa, incidentes de segurança;
2.2.5. Exposição a riscos de não conformidade com a Lei Geral de Proteção de Dados (LGPD).

2.3. A manutenção de uma estrutura própria com hardware, software e equipe técnica dedicada mostrou-se inviável, devido ao alto custo, complexidade de

operação e necessidade de atualização constante.

2.4. Portanto, a terceirização da segurança da informação para um fornecedor especializado, com serviços gerenciados e monitoramento é a solução mais adequada. Essa abordagem reduz a sobrecarga da equipe técnica interna, permitindo que os recursos humanos da instituição sejam direcionados a atividades estratégicas e de atendimento à sua missão institucional.

3 – REQUISITOS DA CONTRATAÇÃO

3.1. A contratação deve abranger um pacote integrado de serviços gerenciados de segurança, com fornecimento de equipamentos em comodato, softwares licenciados e suporte contínuo. Os principais requisitos incluem:

3.1.1. Serviços de Firewall Gerenciado (Next Generation Firewall – NGFW)

3.1.1.1. Fornecimento e gerenciamento de appliances de firewall em regime de comodato;

3.1.1.2. Recursos de inspeção profunda de pacotes, prevenção contra intrusões (IPS), controle de aplicações, VPN segura, antivírus de rede, filtro web e proteção contra ameaças avançadas;

3.1.1.3. Gestão centralizada de regras e políticas de segurança;

3.1.1.4. Monitoramento proativo com resposta a incidentes conforme Acordo de Nível de Serviço (ANS).

3.1.2. Serviços de Backup Gerenciado

3.1.2.1. Solução de backup para servidores e máquinas virtuais, compatível com ambientes Windows, Linux, VMware e Hyper-V;

3.1.2.2. Replicação em datacenter externo para garantir resiliência em caso de desastres;

3.1.2.3. Monitoramento do status dos backups e relatórios periódicos.

3.1.3. Serviços de Implantação

3.1.3.1. Horas de serviços técnicos especializados para implantação da solução;

3.1.3.2. Parametrização inicial dos equipamentos e softwares;

3.1.3.3. Treinamento básico à equipe interna para acompanhamento das soluções.

3.1.3.4. Documentação (As built) das soluções implementadas

3.1.4. Serviços de Suporte Técnico e Central de Serviços

3.1.4.1. Atendimento remoto e presencial (em Palmas-TO);

3.1.4.2. Central de Serviços disponível via telefone, e-mail e portal web;

3.1.4.3. Registro e rastreabilidade de chamados;

3.1.4.4. Reposição de equipamentos com defeito em até 48 horas.

3.1.4.5. Monitoramento contínuo (8x5) dos eventos de segurança;

3.1.4.6. Relatórios executivos e técnicos periódicos;

3.1.4.7. Detecção e resposta a incidentes críticos.

3.1.5. DEFINIÇÃO DA SOLUÇÃO E REQUISITOS DE ARQUITETURA (Art. 11, Incisos I, II e III da IN SGD nº 94/2022)

3.1.5.1. Para o atendimento da necessidade, define-se a solução de TIC com as seguintes especificações técnicas e arquiteturais:

3.1.5.1.1. Definição e Especificação da Solução (Inciso I): A solução consiste na contratação de Serviços Gerenciados de Segurança da Informação

(MSS), operando nas seguintes frentes tecnológicas:

3.1.5.1.1.1. Proteção de Perímetro (Firewall NGFW): Fornecimento em regime de comodato de appliance físico dedicado (hardware) de Próxima Geração (Next Generation Firewall), com capacidade mínima de inspeção de ameaças (Threat Protection) de 600 Mbps e suporte a SD-WAN, incluindo licenciamento para IPS, Anti-Malware, Filtro de Conteúdo e Controle de Aplicações.

3.1.5.1.1.2. Proteção de Dados (Backup): Solução de software de backup profissional compatível com ambientes físicos e virtuais (VMware/Hyper-V), com suporte a desduplicação, criptografia AES-256 e replicação de dados para datacenter externo (nuvem).

3.1.5.1.1.3. Armazenamento: Provisão de 6 TB de armazenamento em disco para retenção segura dos dados.

3.1.5.1.2. Alinhamento com a Arquitetura Tecnológica e Padrões (Inciso II): A solução proposta é compatível com a infraestrutura tecnológica atual do CRM-TO, baseada em rede TCP/IP e arquitetura cliente-servidor:

3.1.5.1.2.1. Padrões de Hardware: O equipamento ofertado não deve estar em fim de vida útil (end-of-life) e deve pertencer à geração atual ou penúltima do fabricante

3.1.5.1.2.2. Padrões de Segurança: A solução deve aderir aos frameworks de segurança ABNT NBR ISO/IEC 27001 e NIST Cybersecurity Framework, conforme diretrizes da política de segurança da informação do órgão

3.1.5.1.3. Necessidade de Desenvolvimento e Integração (Inciso III): Não haverá desenvolvimento de software customizado. A solução exige, contudo, as seguintes integrações nativas para pleno funcionamento:

3.1.5.1.3.1. Integração de Diretório: Integração com Microsoft Active Directory (AD) e LDAP para autenticação de usuários e aplicação de políticas de segurança por grupos

3.1.5.1.3.2. Plataforma Gov.br: Alinhamento com a estratégia de governo digital para oferta de serviços seguros

3.1.5.1.3.3. Interoperabilidade: Capacidade de estabelecer VPNs (IPsec/SSL) com equipamentos de diferentes fabricantes de mercado

4. LEVANTAMENTO DE MERCADO

4.1. Modelos de contratação analisados

4.1.1. No processo de estudo das alternativas possíveis para suprir as necessidades do CRM-TO em relação à segurança da informação, foram analisados dois modelos distintos de contratação. Cada um deles apresenta vantagens e desvantagens que precisam ser avaliadas à luz das restrições orçamentárias, da capacidade operacional da equipe interna e da necessidade de continuidade e confiabilidade dos serviços.

4.1.2. Aquisição interna de equipamentos e equipe própria

4.1.2.1. A primeira alternativa considerada seria a aquisição direta, pelo CRM-TO, de todos os equipamentos e softwares necessários, bem como a constituição de uma equipe interna altamente especializada para gerenciar a segurança da

informação.

4.1.2.2. Embora esse modelo proporcione maior autonomia e controle direto sobre a infraestrutura, ele apresenta desvantagens significativas. O custo inicial de aquisição de equipamentos de última geração (firewalls, soluções de backup, sistemas de monitoramento, etc.) é elevado, impactando diretamente o orçamento da instituição. Além disso, há a necessidade de manutenção constante, substituição de hardware obsoleto e renovação de licenças, o que implica em despesas recorrentes de alto valor.

4.1.2.3. Outro ponto crítico é a necessidade de equipe técnica altamente qualificada, capaz de operar, monitorar e atualizar continuamente os sistemas. Considerando a realidade do CRM-TO, que possui quadro técnico reduzido e com atribuições voltadas principalmente ao suporte e manutenção da infraestrutura básica, não seria viável manter especialistas em cibersegurança de forma permanente.

4.1.2.4. Por fim, há o risco de obsolescência tecnológica, já que o ciclo de vida dos equipamentos de segurança é relativamente curto e novas ameaças exigem atualizações constantes. Isso levaria a instituição a enfrentar a necessidade de investimentos periódicos pesados, sem garantia de que os recursos seriam suficientes para acompanhar a evolução do cenário de ameaças cibernéticas.

4.1.3. Contratação fragmentada (serviços separados por fornecedores distintos)

4.1.3.1. A segunda alternativa seria a contratação dos serviços de segurança da informação de forma fragmentada, ou seja, recorrendo a diferentes fornecedores para cada solução específica. Por exemplo: um fornecedor para o firewall, outro para o backup, e assim sucessivamente.

4.1.3.2. Embora essa abordagem permita uma maior flexibilidade na escolha das soluções e fornecedores, ela gera uma série de desafios de integração e gestão. Em primeiro lugar, há o risco de problemas de compatibilidade entre as soluções contratadas, uma vez que diferentes tecnologias podem não se comunicar de forma eficaz ou exigir ajustes complexos para funcionar em conjunto.

4.1.3.3. Outro aspecto negativo é a multiplicidade de pontos de contato. Isso significa que, em caso de falha ou incidente de segurança, o CRM-TO teria de acionar diferentes fornecedores, muitas vezes sem clareza de quem é o responsável direto pela resolução do problema. Esse cenário pode gerar atrasos na resposta a incidentes, dificultar a apuração de responsabilidades e comprometer a continuidade dos serviços.

4.1.3.4. Além disso, a gestão de contratos fragmentados torna-se burocrática e onerosa, exigindo acompanhamento constante da execução de cada contrato, dos prazos de garantia e suporte, dos níveis de serviço e dos custos associados. Essa fragmentação compromete a eficiência administrativa e aumenta o risco de falhas no controle interno, o que é indesejável para a instituição.

4.1.4. Contratação de serviços gerenciados em lote único (modelo adotado)

4.1.4.1. A terceira alternativa, e considerada a mais vantajosa, é a contratação de serviços gerenciados de segurança em lote único, por meio de fornecedor especializado. Nesse modelo, todos os serviços, firewall, backup, suporte técnico e monitoramento são fornecidos de forma integrada, sob responsabilidade de um único prestador.

4.1.4.2. Essa abordagem traz diversos benefícios concretos. Em primeiro lugar, permite a centralização da gestão da segurança em um fornecedor especializado, que detém expertise, certificações e equipe dedicada para lidar com incidentes, atualizações e monitoramento contínuo.

4.1.4.3. Em segundo lugar, garante maior eficiência, uma vez que as soluções

serão implementadas de forma conjunta, evitando incompatibilidades e reduzindo riscos de falhas na comunicação entre sistemas.

4.1.4.4. Outro ponto relevante é a otimização de recursos humanos internos. Com a terceirização da segurança da informação, a equipe técnica do CRM-TO pode concentrar-se em atividades estratégicas e de suporte ao negócio institucional, enquanto o fornecedor contratado assume as atividades operacionais de segurança.

4.1.4.5. Por fim, esse modelo assegura escalabilidade e atualização tecnológica garantida, pois os contratos de serviços gerenciados normalmente preveem a substituição e atualização periódica dos equipamentos e softwares utilizados, acompanhando a evolução do mercado e garantindo que a instituição esteja protegida contra ameaças emergentes.

4.1.4.6. Dessa forma, após análise comparativa, o modelo de contratação em formato de serviços gerenciados em lote único foi considerado o mais vantajoso para o CRM-TO, equilibrando custo, eficiência, segurança e governança.

4.1.4.7. Além disso, a vigência contratual estabelecida em 12 (doze) meses, está no fato de que prazos reduzidos tendem a gerar maior complexidade administrativa, pois obrigam a instituição a realizar processos licitatórios ou de renovação em intervalos muito curtos, aumentando a carga de trabalho e os riscos de descontinuidade dos serviços.

4.1.4.8. A vigência de 12 meses proporciona maior estabilidade contratual, garantindo previsibilidade orçamentária e operacional, além de permitir que a relação com o fornecedor seja consolidada de forma estratégica, favorecendo ganhos de eficiência, amadurecimento do suporte e continuidade da proteção cibernética.

4.1.4.9. Outro ponto a considerar é que períodos mais longos possibilitam ao fornecedor investir com mais segurança em recursos, tecnologia e equipe, dado que há maior horizonte de tempo para retorno dos investimentos, refletindo em melhores condições técnicas e comerciais para a Administração.

4.1.4.10. Dessa forma, a adoção do prazo de 12 meses representa um equilíbrio adequado entre segurança jurídica, eficiência administrativa e maturidade tecnológica, evitando a fragmentação da gestão em pequenos intervalos e garantindo que os objetivos estratégicos da contratação sejam plenamente atendidos.

4.1.5. Fabricantes e fornecedores de referência no mercado

4.1.5.1. No levantamento de mercado foram identificados fabricantes líderes e fornecedores especializados que oferecem soluções consolidadas de segurança da informação, incluindo tanto produtos quanto serviços gerenciados. Entre os fabricantes de destaque, encontram-se: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

4.1.5.2. Além desses, o mercado nacional conta com integradores e provedores de serviços especializados, que atuam como parceiros estratégicos para órgãos públicos e empresas privadas, oferecendo não apenas a implementação das soluções, mas também seu monitoramento, gestão e atualização contínua.

4.1.5.3. Esses players possuem experiência consolidada na prestação de serviços de segurança em diferentes segmentos e estão aptos a atender às demandas do CRM-TO, fornecendo soluções robustas, escaláveis e alinhadas às melhores práticas internacionais de cibersegurança.

5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

5.1. A solução proposta para o CRM-TO baseia-se na contratação integrada de serviços gerenciados de segurança da informação, em lote único, sob a responsabilidade de um fornecedor especializado. A opção pelo modelo integrado visa garantir maior eficiência, padronização tecnológica e simplificação da gestão contratual, assegurando que todas as camadas de segurança trabalhem de forma coordenada e sob monitoramento contínuo.

5.2. A contratação abrangerá um conjunto de serviços e tecnologias essenciais para a proteção da infraestrutura crítica da instituição, conforme descrito a seguir:

5.2.1. Serviços Gerenciados de Firewall

5.2.1.1. A CONTRATADA disponibilizará e gerenciará um firewall de última geração (NGFW – Next Generation Firewall), capaz de realizar inspeção profunda de pacotes, prevenção contra intrusões (IPS), controle de aplicações, filtragem de conteúdo web, VPN segura, detecção de malwares e análise de tráfego criptografado.
O gerenciamento será centralizado pelo fornecedor, incluindo atualização contínua de assinaturas, monitoramento de eventos e ajustes de regras de segurança conforme a evolução do ambiente. Esse serviço é fundamental para garantir a primeira linha de defesa contra ameaças externas e acessos não autorizados.

5.2.2. Serviços Gerenciados de Backup

5.2.2.1. A solução de backup contemplará a proteção de servidores, bancos de dados e máquinas virtuais, assegurando cópias locais e replicação em datacenter externo.
Essa abordagem permitirá recuperação rápida de informações em caso de falhas, incidentes de segurança ou desastres físicos.

5.2.3. Suporte Técnico e Central de Serviços Para Monitoramento e Gestão

5.2.3.1. O fornecedor deverá disponibilizar Central de Serviços (Service Desk) para atendimento remoto e presencial em Palmas-TO, com registro eletrônico e rastreabilidade de chamados. O suporte incluirá resolução de incidentes, manutenção preventiva e corretiva, substituição de equipamentos em caso de falhas e apoio na configuração de políticas de segurança.
Esse recurso assegurará atendimento padronizado, com cumprimento de Acordo de Nível de Serviço (ANS) previamente definido em contrato.

6. ESTIMATIVA DE QUANTIDADES E CUSTOS

6.1. A definição dos quantitativos que compõem a presente contratação levou em consideração não apenas o cenário atual da infraestrutura tecnológica do CRM-TO, mas também a projeção de crescimento futuro da instituição e a necessidade de

garantir a escalabilidade da solução ao longo da vigência contratual. Assim, buscou-se adotar uma abordagem preventiva, que assegure margem de expansão e evite a necessidade de aditivos frequentes ou novas licitações para suprir demandas que já são previsíveis.

6.2. Das Quantidades

LOTE	ITEM	DESCRIÇÃO	QTD	UNIDADE	PERÍODO
1	1	SERVIÇOS TÉCNICOS ESPECIALIZADOS DE IMPLANTAÇÃO	36	serviço/horas	N/A
	2	SERVIÇOS GERENCIADOS DE FIREWALL	1	serviços/mês	12 meses
	3	SERVIÇOS GERENCIADOS DE BACKUP	4	serviços/mês	12 meses
	4	SERVIÇOS DE ARMAZENAMENTO PARA BACKUP (TB)	6	serviços/mês	12 meses
			VALOR ESTIMADO TOTAL:		R$ 62.725,72

6.2.1. 36h (trinta e seis horas) de serviços técnicos especializados de implantação

6.2.1.1. O quantitativo de 36 horas foi dimensionado com base na complexidade da implantação dos serviços contratados, incluindo instalação, configuração inicial, integração com os sistemas existentes, ajustes de políticas de segurança, testes de funcionamento e documentação. Além disso, esse montante contempla a possibilidade de ajustes finos e atividades adicionais durante o processo de estabilização da solução, o que garante maior segurança na entrega do serviço.

6.2.2. 1 (um) appliances de firewall gerenciado

6.2.2.1. A quantidade de um equipamento de firewall foi definida de forma estratégica, levando em conta não apenas a necessidade de proteção do ambiente tecnológico atual, mas também a possibilidade de expansão da estrutura física do CRM-TO.

6.2.2.2. Assim, a escolha por um appliance reflete uma decisão preventiva e alinhada ao planejamento de médio e longo prazo da instituição, evitando futuras contratações emergenciais e assegurando que a infraestrutura esteja preparada para diferentes cenários de evolução.

6.2.3. 4 (quatro) instâncias de backup profissional

6.2.3.1. As quatro instâncias de backup refletem o número atual de servidores e máquinas virtuais a serem protegidos, mas também consideram a possibilidade de crescimento do parque tecnológico ao longo do contrato. O CRM-TO possui perspectiva de expansão de sistemas internos, além da possível virtualização de novos serviços, o que poderá aumentar a necessidade de armazenamento seguro de dados. Esse quantitativo garante, portanto, que o ambiente esteja protegido desde o início e preparado para absorver futuras demandas.

6.2.4. 6 (seis) unidades de armazenamento

6.2.4.1. As seis unidades de armazenamento representam 06 TB (terabytes) alinhada as necessidades de proteção de dados sensíveis em sistemas de diferentes áreas da instituição. Além de cobrir a demanda

atual, esse quantitativo prevê a expansão natural do volume de dados armazenados, especialmente em razão da digitalização de processos e do cumprimento das exigências da LGPD (Lei Geral de Proteção de Dados), que demandam maior controle, retenção e preservação das informações.

6.3. Considerações sobre os Custos

6.3.1. Embora os quantitativos tenham sido calculados com base nas necessidades atuais, a previsão de margens de crescimento proporciona maior eficiência econômica ao contrato, uma vez que evita a realização de novas contratações emergenciais ou fragmentadas no curto prazo.

6.3.2. Dessa forma, a estimativa de custos resultante contempla não apenas o atendimento à situação presente, mas também a resiliência e a escalabilidade necessárias para suportar a evolução tecnológica e institucional do CRM-TO durante toda a vigência contratual.

6.4. Estimativa de Custos

6.4.1. Com base em consultas de mercado e contratações semelhantes em órgãos públicos e cotações com fornecedores especializados, estima-se um investimento de R$ 62.725,72 (sessenta e dois mil setecentos e vinte e cinco reais e setenta e dois centavos) durante a vigência contratual, contemplando todos os serviços em regime de terceirização.

7. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO

7.1. A contratação será realizada em lote único, abrangendo todos os serviços necessários à proteção da infraestrutura tecnológica do CRM-TO. A adoção dessa estratégia foi definida após análise comparativa entre os modelos possíveis (aquisição interna, contratação fragmentada e contratação integrada), verificando-se que a integração das soluções em um único contrato oferece maior eficiência, menor risco e melhor custo-benefício para a instituição.

7.2. A opção por não parcelar a contratação fundamenta-se nos seguintes pontos:

7.2.1. Gestão centralizada com um único fornecedor: A contratação em lote único assegura que todas as responsabilidades técnicas e operacionais estejam concentradas em um prestador especializado, que será responsável pela entrega do serviço de forma completa e integrada. Isso reduz os pontos de contato, elimina a sobreposição de responsabilidades e proporciona maior agilidade na resolução de incidentes de segurança, evitando o cenário em que diferentes fornecedores atribuem falhas uns aos outros.

7.2.2. Maior eficiência administrativa e contratual: A fiscalização e o acompanhamento da execução contratual tornam-se mais simples e eficientes quando realizados com um único fornecedor. Em contratações fragmentadas, o órgão precisaria acompanhar diversos contratos, cada um com seu próprio objeto, prazos, garantias e ANS (Acordo de Nível de Serviço), o que aumenta a carga administrativa e o risco de falhas no controle interno. No modelo adotado, a gestão do contrato é unificada, permitindo monitoramento mais efetivo da execução e maior transparência nos resultados.

7.2.3. Economia de escala e previsibilidade de custos: A contratação consolidada em lote único favorece a negociação de melhores condições comerciais, uma vez que o fornecedor assume toda a solução, garantindo economia de escala. Além disso, proporciona maior previsibilidade orçamentária ao CRM-TO, que passa a ter um contrato único, com valor fixado para todos os serviços, evitando gastos adicionais e fragmentados ao longo da vigência.

7.2.4. Escalabilidade e visão de futuro: A contratação em lote único também foi pensada para suportar a expansão futura da infraestrutura, como a eventual abertura de novos anexos no estado ou o crescimento da demanda por serviços digitais. O modelo integrado permite ajustes graduais de capacidade sem necessidade de múltiplas licitações, assegurando maior agilidade e flexibilidade para atender às necessidades da instituição.

8. PRAZO DE PAGAMENTO

8.1. Até o 25º dia útil subsequente ao mês de execução do serviço.

9. CONTRATAÇÕES CORRELATAS

9.1. Não há contratações em andamento diretamente correlatas. Todavia, a solução deverá ser compatível com os sistemas internos já utilizados pelo CRM-TO.

10. ALINHAMENTO COM O PAC

10.1. A demanda encontra-se prevista no Plano Anual de Contratações do CRM-TO em 2026, alinhada às diretrizes estratégicas da instituição e à necessidade de garantir proteção de dados e continuidade de serviços críticos.

11. RESULTADOS PRETENDIDOS

11.1. A adoção da solução em lote único traz benefícios diretos e estratégicos para o CRM-TO, uma vez que todos os serviços passam a ser coordenados por um único fornecedor especializado, garantindo visão unificada da segurança cibernética e eliminando falhas de integração que poderiam comprometer a proteção do ambiente. Essa abordagem assegura maior eficiência operacional, pois o monitoramento e a gestão centralizados permitem reduzir significativamente o tempo de resposta a incidentes, além de garantir continuidade das operações críticas sem paralisações.
11.2. Outro aspecto relevante é a redução da sobrecarga da equipe técnica interna, que poderá direcionar esforços para atividades estratégicas e de suporte ao negócio institucional, enquanto a gestão tática e operacional da segurança fica sob responsabilidade do fornecedor. O modelo também garante atualização tecnológica contínua, permitindo ao CRM-TO acesso a soluções de ponta sem a necessidade de constantes investimentos em renovação de equipamentos ou softwares.
11.3. Do ponto de vista de governança e conformidade, a contratação contribui para o atendimento à LGPD e demais normas de segurança da informação, assegurando

maior integridade e resiliência dos dados armazenados, além de redução efetiva das vulnerabilidades e riscos de incidentes. Em síntese, o modelo adotado promove a elevação do nível de segurança cibernética do CRM-TO, conciliando eficiência, inovação tecnológica, integridade de dados e conformidade regulatória em uma solução integrada e sustentável.

12. CRONOGRAMA DE IMPLANTAÇÃO

12.1. **Planejamento (até 15 dias):**

12.1.1. Definição de prazos, estratégias de execução e detalhamento do plano de testes. Essa fase estabelece a base metodológica e organizacional para a implantação da solução, alinhando expectativas entre a contratada e o CRM-TO.

12.2. **Implantação (até 30 dias):**

12.2.1. Instalação, configuração e integração de todas as soluções de segurança contratadas, abrangendo firewall, backup e monitoramento.

12.3. **Testes e Homologação (até 15 dias):**

12.3.1. Realização de validações técnicas, simulações de incidentes e avaliação da performance do ambiente. Entrega da documentação "As Built", que registra a configuração final e garante a rastreabilidade da implantação.

12.4. **Operação Assistida (30 dias):**

12.4.1. Acompanhamento contínuo do ambiente já em produção, com suporte ativo do fornecedor para ajustes, correções e estabilização da solução, além de transferência de conhecimento para a equipe interna do CRM-TO.

13. IMPACTOS AMBIENTAIS

13.1. **Redução do consumo energético:**

13.1.1. Adoção de equipamentos modernos, de última geração e com maior eficiência energética, garantindo melhor desempenho com menor gasto de energia elétrica em comparação a equipamentos legados.

13.2. **Mitigação da obsolescência precoce:**

13.2.1. Fornecimento de equipamentos em regime de comodato, evitando aquisições diretas que rapidamente se tornam defasadas e diminuindo o descarte frequente de hardware.

13.3. **Contribuição para a sustentabilidade institucional:**

13.3.1. A combinação de tecnologias eficientes e práticas modernas garante menor impacto ambiental, alinhando a segurança cibernética do CRM-TO às

políticas de responsabilidade socioambiental.

14. VIABILIDADE DA CONTRATAÇÃO

14.1. A análise demonstra que a contratação é:

14.1.1. Tecnicamente viável:

14.1.1.1. A solução contempla tecnologias avançadas, como firewalls de próxima geração (NGFW) — que incluem IPS, proteção antimalware avançada, sandbox e controle de aplicações —, backup gerenciado com transferência de dados para datacenter externo , monitoramento contínuo 24/7 e suporte técnico especializado. Todos esses serviços são integrados em um modelo de gerenciamento centralizado, conduzido por equipe qualificada do fornecedor. Essa abordagem assegura que o CRM-TO disponha de um ambiente seguro, atualizado e em conformidade com as melhores práticas internacionais, como a ISO/IEC 27001 e o Framework de Cibersegurança do NIST.

14.1.2. Economicamente vantajosa:

14.1.2.1. O modelo de contratação em serviços gerenciados permite significativa redução de custos em CAPEX (Capital Expenditure), uma vez que elimina a necessidade de aquisição direta de equipamentos caros, sua manutenção constante e renovação periódica. Além disso, reduz-se a dependência de uma equipe interna numerosa e altamente especializada, que demandaria altos investimentos em capacitação e folha salarial. O contrato, portanto, concentra os custos em OPEX (Operational Expenditure) previsível, trazendo maior controle orçamentário, economia de escala e previsibilidade financeira para a instituição.

14.1.3. Operacionalmente adequada:

14.1.3.1. A gestão da segurança em lote único garante centralização e padronização de processos, com um único ponto de contato para administração, suporte e resolução de incidentes. Isso reduz falhas de comunicação, melhora o tempo de resposta a ocorrências e aumenta a confiabilidade dos serviços. Ao mesmo tempo, libera a equipe interna do CRM-TO para concentrar esforços em atividades estratégicas e institucionais, fortalecendo o foco no core business e deixando a gestão tática e operacional da segurança sob responsabilidade do fornecedor especializado.

15. CONSIDERAÇÕES FINAIS

15.1. O presente Estudo Técnico Preliminar evidencia que a contratação de serviços gerenciados de segurança da informação em lote único constitui a alternativa mais adequada para o CRM-TO, considerando aspectos técnicos, operacionais e legais.

15.2. A adoção desta estratégia apresenta vantagens estratégicas e operacionais, tais como:

15.2.1. Proteção abrangente da infraestrutura: A utilização de soluções de segurança gerenciadas permite monitoramento contínuo, detecção proativa de ameaças e aplicação de medidas preventivas, mitigando riscos tanto internos quanto externos à rede.

15.2.2. Continuidade operacional: A terceirização com monitoramento e gestão especializada assegura mínima interrupção das atividades do CRM-TO em caso de ataques ou falhas, promovendo resiliência organizacional.

15.2.3. Atendimento às exigências legais: O modelo contratado suporta conformidade com a Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), garantindo transparência, economicidade e eficiência; além de promover aderência à LGPD, protegendo dados pessoais de clientes, colaboradores e parceiros, minimizando riscos legais e reputacionais.

15.3. Além disso, a terceirização com fornecedor especializado e equipe técnica qualificada,com suporte 24/7, se apresenta como o modelo mais vantajoso para assegurar os pilares da segurança da informação: integridade, disponibilidade e confidencialidade dos dados do CRM-TO. Este modelo permite que a equipe interna se concentre em atividades estratégicas, enquanto a gestão operacional da segurança é realizada por profissionais com experiência dedicada e ferramentas avançadas.

15.4. Portanto, a contratação proposta não apenas atende aos requisitos legais e normativos, mas também proporciona eficiência operacional, mitigação de riscos e proteção robusta da informação, consolidando a segurança da infraestrutura de TI do CRM-TO.

16. POSICIONAMENTO CONCLUSIVO

Com base nos elementos técnicos, econômicos e operacionais analisados neste Estudo Técnico Preliminar, a Equipe de Planejamento da Contratação declara que a presente contratação é **viável e adequada** para o atendimento da necessidade a que se destina, conforme preconiza o art. 18, § 1º, inciso XIII, da Lei nº 14.133/2021.

A solução de Serviços Gerenciados de Segurança da Informação (Firewall e Backup) demonstra ser a alternativa mais vantajosa para o CRM-TO, garantindo a mitigação de riscos cibernéticos e o alinhamento com os objetivos estratégicos da instituição.

17. APROVAÇÃO E ASSINATURA

Athos Alencar de Almeida
Assistente de Tecnologia da Informação
Matrícula: 78

Integrante Requisitante

Athos Alencar de Almeida
Assistente de Tecnologia da Informação
Matrícula: 78

Integrante Técnico

Autoridade Máxima da Área de TIC
Wordney Carvalho Camarço Presidente do CRM-TO (em exercício) Portaria SEI-N° 64/2026

Documento assinado eletronicamente por **Athos Alencar de Almeida**, **Assistente de Tecnologia da Informação**, em 02/07/2026, às 14:21, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

Documento assinado eletronicamente por **Wordney Carvalho Camarço**, **Presidente do CRM-TO**, em 02/07/2026, às 15:01, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

A autenticidade do documento pode ser conferida no site https://sei.cfm.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **4476440** e o código CRC **30698066**.