CONSELHO REGIONAL DE ENFERMAGEM DE SÃO PAULO

ESTUDO TÉCNICO PRELIMINAR (ETP)[1] – SOLUÇÕES DE TIC
PROCESSO ADMINISTRATIVO Nº 1521/2021

Área de Negócios/Requisitante	Gerência de Tecnologia da Informação – Setor de Infraestrutura
Área Técnica (TI)	Gerência de Tecnologia da Informação
Área de Apoio Administrativo	Gerência de Compras e Contratos – GCC

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	
Integrante Requisitante	Rafael Conceição da Silva, 455
Integrante Técnico	Régis de Oliveira Araújo, 1044
Integrante da Área de Apoio Administrativo	Henrique Pereira Soares, 975

INTRODUÇÃO
O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.
Referência: Art. 11 da IN SGD/ME nº 1/2019.

1. DEFINIÇÃO E ESPECIFICAÇÃO DA NECESSIDADES E REQUISITOS

1.1. CONTEXTUALIZAÇÃO DA DEMANDA

1.1.1. A Visão de futuro do Coren-SP é "Ser uma autarquia de destaque na fiscalização profissional, reconhecida pela celeridade e modernidade e comprometida com a valorização do profissional de enfermagem.". Os Atributos de valor para a sociedade do Coren-SP são "Ética, Eficiência, Transparência, Acessibilidade, Modernidade, Comprometimento, Responsabilidade, Profissionalismo, Credibilidade, Inovação e celeridade.". Para atingir esses objetivos, é necessário que seja realizada a devida proteção dos equipamentos de TI contra ameaças digitais, garantindo a continuidade dos serviços de TI em todo o Coren-SP. Além disso, o serviço de proteção contra softwares maliciosos e contra ataques cibernéticos não pode sofrer interrupção, uma vez que isso tornaria as estações e servidores, que hoje estão protegidos, vulneráveis a acessos indesejados e a infecções, bem como a perda ou vazamento de informações importantes.

1.1.2. Há a necessidade de cumprir os requerimentos da Política de Segurança da Informação do Coren-SP. O item 6.2 e 6.3 da Norma – Prevenção de Vírus[2], explicitamente definem que todas as estações e servidores Windows do Coren-SP devem possuir antivírus instalado e atualizado. Apenas um parque de máquinas com licenças ativas de antivírus permite que suas definições sejam atualizadas. Segue abaixo a transcrição dos itens citados:

[1] Adaptado de modelo disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/2-estudo-tecnico-preliminar-v2-0.odt (versão de 24/05/2021).
[2] Malware e Vírus de Computador são classes de programas de computador e/ou arquivos que possuem funções e/ou códigos maliciosos, que executam funções não desejadas pelos usuários. As diferentes classes de malware (tais quais adware, spyware, trojan, worm, rootkit e vírus) são comumente referenciadas apenas como "Vírus".

> *[...] 6.2. Toda e qualquer estação de trabalho do Coren-SP deve possuir antivírus instalado, licenciado e atualizado, com atraso de atualização máximo de 10 dias (ou 40 para casos de funcionários em férias);*
>
> *6.3. Todo e qualquer servidor Windows do Coren-SP deve possuir antivírus instalado e atualizado, com atraso de atualização de definições máximo de 5 dias. [...]*

1.1.3. A ausência de uma solução de antivírus instalada, ativa, licenciada e atualizada em todas as máquinas Windows do Coren-SP significa ausência da proteção básica a essas máquinas contra ataques de rede internos e externos, exploração de vulnerabilidades e infecções. Essa ausência de proteção deixaria o órgão exposto a diversos impactos, sejam esses vazamentos de dados confidenciais (observa-se a Lei Geral de Proteção de Dados – LGPD), impacto a reputação (dada uma eventual indisponibilidade dos serviços causada por vírus ou outro ataque), impacto legal do não cumprimento de Normas internas e Legislação, entre outros.

1.1.4. No ambiente do Coren-SP, a última contratação para Solução Antivírus ocorreu por meio do Pregão Eletrônico nº 11/2018 (PA 2225/2017), tratando-se de um processo de *"Registro de preços para aquisição de licenças, para instalação, suporte e gerenciamento centralizado de software Antivírus do tipo "Proteção de Endpoint" para 600 máquinas, com validade de 36 meses, para utilização nas máquinas do Coren-SP (inclusive estações e servidores).* A licitante vencedora, a Global TTI Soluções em Tecnologia Ltda. - ME, ofertou licenças da fabricante ESET (Eset Endpoint Protection Advanced), ativadas em outubro de 2018 e que virão a expirar em 17/10/2021. Assim posto, porque se aproxima a data limite para uso das licenças atuais, bem como o incremento do número de máquinas do parque tecnológico do Coren-SP (no período 2017-2021) – demandando contratação de novas licenças - são as justificativas para a abertura de processo de contratação e da realização deste ETP.

1.2. ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTOS INSTITUCIONAIS

1.2.1. A referida contratação está alinhada como parte da ação prevista no planejamento da area, referente ao período de 2021-2024. Cadastrada no módulo de Planejamento Estratégico do sistema Agiliza, conforme abaixo:

Planejamento	
01/01/2021 à 31/12/2024	
Programa	
Apoio à atividade finalística	
Projeto/Atividade	
ID	**Nome**
20	Manter os recursos tecnológicos próprios e contratados atualizados, visando à segurança e ao atendimento das necessidades de negócio do Coren-SP.

1.3. RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS

1.3.1. Manter o provimento de Infraestrutura de TI segura e adequada para que o ambiente computacional do Coren-SP continue operacional;

1.3.2. Contribuir para garantia de um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

1.3.3. Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo endpoints comprometidos (estações de trabalho e notebooks);

1.3.4. Evitar, mitigar e conter a propagação de pragas digitais facilitando o tratamento destes incidentes (vírus/malwares/spywares, spam, dentre outros) com a administração centralizada da solução de proteção;

1.3.5. Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;

1.3.6. Gerar economicidade e melhoria de qualidade do serviço de proteção de endpoints;

1.3.7. Mitigar riscos de infecção na transição entre soluções de antivírus.

1.4. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

1.4.1. Manutenção de uma Solução de segurança para dispositivos fins contra ameaças cibernéticas e comprometimento de computadores e servidores do Coren-SP, com garantia de operação de toda a solução por parte da contratada;

1.4.2. Manutenção do gerenciamento centralizado da solução de segurança das estações de trabalho e servidores institucionais.

1.4.3. Manutenção do monitoramento e rastreamento em tempo real de atividades, arquivos e processos maliciosos na infraestrutura de TI - sendo essencial no processo de tratamento de incidentes;

1.4.4. Proteção das informações e dados pessoais e corporativos, atendendo às exigências da Lei geral de Proteção de Dados pessoais (LGPD);

1.4.5. A desnecessidade de treinar as equipes de TI para a administração dessa solução decorrentes da manutenção de uma solução já estável no ambiente do Coren-SP. Isso gera economia na contratação ao permitir que utilizemos os conhecimentos e experiências já adquiridos;

1.4.6. A desnecessidade de instalar novos clientes de antivírus em mais de 600 máquinas espalhadas por todo o Estado decorrente da manutenção de uma solução já instalada no ambiente do Coren-SP. Instalações tão grandes estão passíveis de falhas e consequentemente, abertura de vulnerabilidades que podem comprometer toda a rede do Coren-SP. Isso também gera economia na contratação, visto que não necessitaremos pagar horas de técnicos de fornecedor para auxiliar nas instalações e configurações;

1.4.7. O trabalho remoto imposto pela pandemia de Covid-19. Muitos colaboradores do grupo de risco estão com computadores do Coren-SP em casa, com a solução ESET já instalada. A perda dessa licença acarretaria em vulnerabilidade imediata para a rede do Coren-SP, bem como a necessidade de troca de solução envolveria custos com a logística de transporte de todas essas máquinas até uma unidade para que a instalação pudesse ser feita, gerando nesse ultimo, exposição dos colaboradores em grupo de risco.

1.4.8. A desnecessidade de instalação de novo servidor, o que acarreta em perda de históricos de ações e de detecções, importante em processos administrativos internos, tomada de decisões no ambiente tecnológico e administração para eventuais revogações de acesso, conforme previsto na Norma – Prevenção de Vírus.

1.5. IDENTIFICAÇÃO DAS NECESSIDADES TECNOLÓGICAS

1.5.1. A Solução deve englobar softwares necessários ao atendimento das especificações técnicas do objeto durante o prazo de vigência do contrato, incluindo garantia, manutenção e

atualização dos produtos;

1.5.2. Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço.

1.5.3. A empresa licitante a ser contratada deverá apresentar declaração informando que a licitante é a fabricante, revendedora ou distribuidora autorizada do fabricante, ou ainda, revendedora autorizada de distribuidor autorizado pelo fabricante dos produtos.

1.5.4. A contratada deverá responder com agilidade às solicitações de verificação de arquivos que a CONTRATANTE suspeite de detecção falso-negativa ou falso-positiva.

1.5.5. A contratada deverá ter canal de atendimento e responder com agilidade a chamados de problema ou solicitações na solução ofertada.

1.5.6. O referido objeto deve incluir licença para instalação/utilização/suporte do software de gerenciamento da referida solução ofertada;

1.5.7. O referido software de gerenciamento deverá ser compatível com, pelo menos, os seguintes sistemas operacionais (64 bits) que deverão funcionar em infraestrutura de rede padrão IPv4:

1.5.7.1. Windows Server 2012, Windows Server 2016 e Windows Server 2019 ou outro sistema operacional acompanhado de licença entregue pela própria CONTRATADA. Poderá ser instalação no padrão de Appliance virtual com SO customizado desde que todo o software necessário seja disponibilizado pela CONTRATADA e que haja total compatibilidade com o ambiente de virtualização do Coren-SP (VMWARE ESXI 5.5). Nesse último caso, o gerenciamento de antivírus (console de gerenciamento) deverá ser feito através de interface web acessível através de qualquer navegador remotamente na rede do Coren-SP.

1.5.8. O servidor de gerenciamento deve ser capaz de:

1.5.8.1. Administrar todos os clientes de proteção Endpoint licenciados de forma centralizada;

1.5.8.2. Autenticar usuários administradores diretamente do domínio Active Directory para administração das políticas e configurações da solução Endpoint;

1.5.8.3. Configurar e administrar tarefas agendadas para instalação/desinstalação de software, geração de relatório (com envio automático por e-mail), ativação de clientes, atualização de sistema operacional e atualização de módulos de antivírus;

1.5.9. Configurar grupos dinâmicos, com pelo menos os filtros abaixo:

a) Versão do Sistema Operacional;

b) Status da licença;

c) Versão e existência de software de proteção;

d) Computadores com problemas/alertas;

1.5.9.2. Gerar relatórios e buscas customizadas e padronizadas de ameaças, definições de vírus e saúde do ambiente em diversos períodos de tempo selecionáveis e utilizando-

se de, pelo menos, as seguintes variáveis:

a) Status;

b) Hostname;

c) Endereço IP;

1.5.9.3. Apresentar Dashboard de visualização de status da solução e infecções detectadas no ambiente para rápida análise de infecções generalizadas (epidemias);

1.5.9.4. Realizar configurações de proteção Endpoint de forma remota (através da gerência), tais como: agendamento ou execução de scans, configuração de políticas globais e de grupos específicos (como exceções de antivírus, ativação e desativação de tecnologias de proteção, etc.);

1.5.9.5. Definir se os clientes de software de proteção Endpoint atualizarão suas definições pela internet, repositório local, ou pelo próprio servidor de gerenciamento, bem como definir a banda máxima utilizada;

1.5.9.6. Executar comandos nos clientes como scan sob demanda, restart da máquina, atualização das definições de vírus e atualização do software de proteção antivírus;

1.5.10. Todas as configurações, políticas e comandos devem poder ser executados/configurados, pelo menos, por grupos de máquinas;

1.5.11. O referido software deverá ser compatível com, pelo menos, os seguintes sistemas operacionais (arquiteturas 32 e 64 bits) que deverão funcionar em infraestrutura de rede padrão IPv4 e/ou IPv6:

1.5.11.1. Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows 7, Windows 8.1, Windows 10 e Windows 11;

1.5.11.2. Distribuições Linux padrão Debian devem possuir Scanner de vírus compatível, disponibilizado pela CONTRATADA, atualização de definições e engine, licença ativa e suporte (referente à definições/infecções e software);

1.5.12. O mesmo precisa ser suportado e funcional em máquinas desktops e notebooks com 2GBs de memória RAM ou mais;

1.5.13. Deverá ser possível configuração de exceções de antivírus e demais tecnologias de proteção, na forma de, pelo menos: arquivo, extensão de arquivo, caminho e caminho com subpastas;

1.5.14. Deverá ter a capacidade de bloqueio de portas USB, SD-Cards e Drives-ROM e liberação de exceções por grupo de usuários no Active Directory;

1.5.15. Deverá possuir funcionalidade de proteção contra intrusões e outros ataques (IPS de Host e/ou engines anti-exploit);

1.5.16. Deverá possuir funcionalidade de firewall de host;

1.5.17. Deverá possuir funcionalidade de proteção proativa de ameaças, com análise de comportamento de processos em memória para detecção de malwares que não possuam definições criadas (malwares ainda não catalogados);

1.5.18. Deverá possuir funcionalidade de análise de caminhos de internet (endereços de

navegação) para alerta aos usuários durante a navegação, caso algo suspeito seja detectado;

1.5.19. Deverá possuir filtro web por categorias de websites;

1.5.20. Deverá possuir filtro de e-mails do Outlook para proteção antispam;

1.5.21. Deverá possuir capacidade de escanear arquivos compactados em, por exemplo, .zip e .rar;

1.5.22. Deverá possuir capacidade de limitação do consumo de CPU, sendo aceitos nesse caso a definição da porcentagem de CPU utilizada ou diferenciação entre consumo máximo e background ou configuração equivalente. Tal alteração pode ser feita dinamicamente pela ferramenta (nesse último caso, a funcionalidade deve ser descrita em documento do fabricante da solução);

1.5.23. A solução ofertada deverá ter a capacidade de instalação remota e silenciosa (sem interação nem percepção por parte do usuário final). A mesma poderá fazer uso do Microsoft Configuration Manager do Coren-SP (com utilização do arquivo .msi da solução por exemplo);

1.5.24. Tal instalação deverá adicionar a maquina do endpoint automaticamente à gerência de antivírus, sem necessidade de interação local;

1.5.25. Todas as funcionalidades citadas acima devem ser configuráveis pela gerencia centralizada da solução;

1.5.26. A licença ofertada deverá incluir suporte para a solução e também para análise de comportamentos suspeitos, para correção de falso-negativos e falso-positivos junto ao fabricante;

1.5.27. O suporte deverá ser feito via telefone, e-mail ou portal web do fabricante ou representante oficial. Ficando o método a critério da CONTRATANTE;

1.5.28. No caso de suporte por telefone, o mesmo deverá possuir número para chamadas locais de São Paulo/SP ou gratuitas (0800);

1.5.29. A licença deverá ter duração de 3 (três) anos a partir do momento de sua ativação e poderá ser renovada conforme manifestação de intenção do Coren-SP;

1.5.30. Com a referida licença ativa, a CONTRATANTE deverá conseguir solicitar ao fabricante através dos canais acima citados, minimamente:

1.5.30.1. Suporte para análise e correção de falhas em qualquer uma das soluções e features acima citadas;

1.5.30.2. Suporte para análise de suspeitas de ameaças em sistemas a fim de que definições de malwares sejam criadas para os casos em que o fabricante ainda não as possua;

1.5.30.3. Suporte para análise de suspeitas de falso-positivos para correção de definições de malware que detectam arquivos legítimos como maliciosos;

1.5.30.4. Suporte para análise de falhas e melhorias dos produtos ofertados.

1.6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

1.6.1. REQUISITOS DE CAPACITAÇÃO

1.6.1.1. A Contratada deverá realizar transferência de conhecimento relativo à instalação, gerenciamento, operacionalização, configuração e utilização da Solução ofertada, o que poderá ocorrer por meios de ambiente virtual.

1.6.2. REQUISITOS LEGAIS

1.6.2.1. Além da legislação e instruções relacionadas à generalidade das contratações públicas e outras que, por ventura, não tenham sido citadas, os seguintes normativos estão vinculados ao objeto desta contratação:

1.6.2.2. Instrução Normativa SGD/ME nº 01/2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação TIC pelos órgãos e entidades da Administração Direta do Poder Executivo Federal e adotado pelo Coren SP como boa prática;

1.6.2.3. Portaria Coren SP/Plenário/024/2016, de 22 de dezembro de 2016 que dispõe sobre a Política de Segurança da Informação no âmbito Coren SP Regional de Enfermagem de São Paulo.

1.6.3. REQUISITOS DE MANUTENÇÃO

1.6.3.1. Serão ofertados pela Contratada, durante todo o período de vigência contratual serviços de suporte técnico de manutenção para toda a Solução contratada;

1.6.3.2. O serviço de suporte técnico da Contratada deverá ser efetuado segundo as melhores práticas do fabricante/desenvolvedor da Solução, visando sempre o máximo desempenho, disponibilidade e segurança, por técnico certificado por este, de modo a garantir total interoperabilidade no ambiente computacional;

1.6.3.3. Os serviços deverão ser prestados pela Contratada ou, a depender da natureza do chamado, diretamente pelo fabricante/desenvolvedor da Solução (ficando a Contratada obrigada a mediar este atendimento, se necessário);

1.6.3.4. O suporte da Contratada deverá disponibilizar acesso a canais de atendimento (telefônico e eletrônico) para abertura de chamados, consultas e envio de arquivos para análise durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana e 365 dias no ano durante todo o período da contratação;

1.6.3.5. Todas as formas de abertura de chamado disponíveis deverão estar efetivamente operacionais;

1.6.3.6. Os chamados serão classificados, em comum acordo pelas partes, de acordo com a SEVERIDADE do problema, como seguem:

NÍVEL 1	**Situação Crítica / Sistema Indisponível**	• Algum serviço Crítico do Coren-SP está indisponível por infecção por vírus ou suspeita de ataque similar; • Um componente de software da solução Endpoint está tornando serviços de redes indisponíveis;
NÍVEL 2	**Impacto Grave**	• Serviço crítico parcialmente indisponível ou com degradação de tempo de resposta devido a infecção por vírus, suspeita de infecção por vírus ou ataque similar.
NÍVEL 3	**Impacto Moderado**	• A Solução de Endpoint não está funcionando adequadamente, gerando falso-negativos no ambiente ou lentidão que não impacta consideravelmente o funcionamento dos serviços;

NÍVEL 4	**Impacto Mínimo**	• Há uma necessidade de configuração adicional no ambiente; • Há uma necessidade de relatório ou dúvida da equipe técnica referente ao funcionamento da Solução.

1.6.3.7. Os Prazos – em horas corridas - para início de atendimento e prazos para o fim do atendimento com uma solução definitiva ou de contorno são:

Nível de Severidade	Prazo para início de atendimento (resposta) partir da abertura do chamado	Prazo para o fim do atendimento
1	1 (uma) hora	2 (duas) horas
2	2 (duas) horas	4 (quatro) horas
3	8 (oito) horas	16 (dezesseis) horas
4	16 (dezesseis) horas	36 (trinta e seis) horas

1.6.3.8. Ao término de atendimentos de Suporte, quando solicitado pela Contratante, a Contratada deverá disponibilizar Relatório de Atendimento contendo, minimamente, data e hora da abertura do chamado; data e hora do início e do término do atendimento; número de identificação do chamado; identificação do defeito ou falha na Solução; nome do funcionário da Contratante que abriu o chamado; nome do funcionário da Contratada que efetuou o atendimento; descrição do problema; nível de classificação do chamado; informações sobre alteração de nível; e descrição da solução adotada e sobre a sua eficácia.

1.6.3.9. A Contratante poderá solicitar à Contratada, ou ter acesso por meio de sítio na internet ou aplicação eletrônica a relatórios mensais referentes às solicitações de serviços, abrangendo: Informações completas dos chamados abertos e fechados, com um status para aqueles resolvidos no período; e Acesso a informações sobre a disponibilização de novas versões, entre outras consideradas de relevância.

1.6.4. REQUISITOS TEMPORAIS

1.6.4.1. A CONTRATADA deverá cumprir, além de outros prazos previstos nos aneos deste documento, os prazos máimos especificados na Tabela 1: Marcos, prazos, eventos e responsáveis do Contrato, que disciplina as etapas de planejamento, instalação, configuração e início de funcionamento da solução CONTRATADA. A contagem dos prazos se dará a partir da data de início da vigência contratual:

1.6.4.2. TABELA 1: MARCOS, PRAZOS, EVENTOS E RESPONSÁVEIS DO CONTRATO:

MARCOS	PRAZOS (EM DIAS CORRIDOS)	EVENTO	RESPONSÁVEL(IS)
Dia 'D'	0 (zero)	Início da vigência contratual, após a assinatura do Contrato entre o Coren-SP e a licitante vencedora	Coren-SP e CONTRATADA
Dia 'D1'	D + 7	Reunião de alinhamento	Coren-SP e CONTRATADA
Dia 'D2'	D1 + 3	Entrega do plano de instalação/migração do antivírus	CONTRATADA
Dia 'D3'	D2 + 5	Início da instalação dos clientes de antivirus ou migração nas maquinas do Coren-SP	CONTRATADA

MARCOS	PRAZOS (EM DIAS CORRIDOS)	EVENTO	RESPONSÁVEL(IS)
Dia 'D4'	D3 + 15	Data limite para conclusão das instalações ou migrações de antivírus em todas as máquinas do Coren-SP. Sem Pendências adicionais importantes para o funcionamento da solução e segurança contra ameaças.	CONTRATADA
Dia 'D5'	Dia da conclusão efetiva das instalações/migrações + 10	Recebimento definitivo, autorização para emissão de faturamento e conclusão da entrega do objeto.	Coren-SP
PERÍODO TOTAL: 40 (quarenta) dias corridos, contados a partir do início da vigência contratual			

1.6.5. REQUISITOS DE SEGURANÇA

1.6.5.1. A Contratada guardará e fará com que seu pessoal guarde absoluto sigilo sobre os dados, informações e documentos fornecidos pelo Contratante aos quais tiver acesso em decorrência da prestação de serviços objeto do referido Contrato, ficando terminantemente proibida de fazer uso ou revelação destes, sob qualquer justificativa.

1.6.5.2. Todas as informações, resultados, relatórios e quaisquer outros documentos obtidos ou elaborados pela Contratada na execução dos serviços serão de exclusiva propriedade do Contratante, não podendo a Contratada utilizá-los para quaisquer fins, divulgá-los, reproduzi-los ou veiculá-los, a não ser que prévia e expressamente autorizado pelo Contratante.

1.6.5.3. Ademais, deverão ser observadas pela Contratada as normas internas do Coren-SP, tais como: a Portaria Coren-SP/Plenário/024/2016, que normatiza a Política de Segurança da Informação e Comunicações – POSIC e outras que venham a complementá-la.

1.6.6. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS

1.6.6.1. Os softwares devem ser fornecidos em meio digital, sem a necessidade de entrega de versões dos produtos em mídias físicas;

1.6.6.2. A documentação técnica deve ser fornecida em meio digital, com um descritivo completo do processo de implantação de cada produto ofertado, explicações sobre o registro e uso de licenças de software, forma de acesso ao site do fabricante para download da solução antivírus completa, assim como de seus upgrades e updates;

1.6.6.3. Não serão aceitas cópias impressas da documentação das licenças;

1.6.6.4. Não foram observados outros requisitos aplicáveis ao objeto licitatório.

1.6.7. REQUISITOS DE ARQUITETURA TECNOLÓGICA

1.6.7.1. Não se aplicam, pois se trata da contratação de Solução composta por software 'de prateleira'.

1.6.8. REQUISITOS DE PROJETO E IMPLEMENTAÇÃO

1.6.8.1. Não se aplicam para a Solução em questão, uma vez que o atendimento dos

requisitos de negócio do objeto não demandarão qualquer tipo de projeto ou ato específico de implementação para a Contratada.

1.6.9. REQUISITOS DE IMPLANTAÇÃO

1.6.9.1. Caso a solução ofertada seja diferente da solução atualmente implantada no Coren-SP (ESET), a CONTRATADA deverá realizar toda a instalação da gerência, software e hardware adicionais e clientes de Endpoint em todas as máquinas do Coren-SP (incluindo servidores Windows) de forma transparente para os usuários (sem impactar nas suas funções diárias), incluindo a desinstalação da solução atual;

1.6.9.2. O hiato de tempo entre a desinstalação da solução atual e a instalação de nova solução deverá ser o mínimo possível para que não haja riscos de infecção nesse período.

1.6.9.3. A CONTRATADA deverá deslocar funcionário próprio para instalação manual do antivírus em máquinas onde a instalação remota não é possível, ou que apresente algum problema no processo.

1.6.9.4. A CONTRATADA deverá passar o conhecimento a respeito da implantação da solução para pelo menos 4 funcionários do Coren-SP.

1.6.10. REQUISITOS DE GARANTIA E SUPORTE

1.6.10.1. Os softwares licenciados devem ser instalados em sua versão mais estável e atualizada e estarem cobertos por contratos de suporte e atualização de versão do fabricante durante a validade das licenças.

1.6.10.2. Durante o período de vigência do contrato, bem como os períodos de prorrogações a Contratada deverá realizar a conTInuidade do suporte técnico e garantir a atualização tecnológica da solução na forma de atualizações de programas. As atualizações de programas deverão cobrir todos os programas de computador (software e firmware) adquiridos e incluir o fornecimento de correções (patches) e novas versões/revisões/distribuições (releases) assim que o fabricante as torne disponíveis. Entende-se por atualização de programas qualquer correção, pequena modificação, aperfeiçoamento (update), ou desenvolvimento de nova versão (upgrade) efetuado pelo fabricante para os produtos em questão.

1.6.11. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL

1.6.11.1. A Contratada deverá manter em seu quadro profissionais capacitados para atendimento das demandas relacionadas a suporte técnico durante a vigência contratual.

1.6.12. REQUISITOS DE FORMAÇÃO DE EQUIPE

1.6.12.1. Não se aplicam, pois se trata da contratação de Solução composta por software ‘de prateleira’.

1.6.13. REQUISITOS DE METODOLOGIA DE TRABALHO

1.6.13.1. Não se aplicam, pois se trata da contratação de Solução composta por software ‘de prateleira’.

1.6.14. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

1.6.14.1. Como software de Segurança, a CONTRATADA e a solução de antivírus devem estar aderentes as melhores práticas de Segurança do mercado, tais como a ISO 27000.

1.6.14.2. Os dados, informações e sistemas de informação do Coren-SP devem ser protegidos contra ameaças e mau uso, de forma a reduzir riscos e garantir a integridade, confidencialidade, disponibilidade e autenticidade, observando-se as normas do Coren-SP referentes a Política de Segurança da Informação e Comunicações.

1.6.14.3. Os dados e informações devem ser mantidos com o mesmo nível de proteção, independentemente do meio em que estejam sendo processados, armazenados ou trafegando.

1.6.14.4. As informações classificadas e sensíveis que trafegam em redes inseguras, incluindo as sem fio, devem ser criptografadas de modo adequado.

1.6.14.5. A segurança é um processo que deve estar inserido em todas as etapas do ciclo de desenvolvimento do sistema e implantação da solução.

1.6.14.6. Os sistemas devem possuir registros históricos (logs) para permitir auditorias e provas materiais, sendo imprescindível a adoção de um sistema de sincronismo de tempo centralizado.

1.6.14.7. Os funcionários da CONTRATADA e usuários devem conhecer suas responsabilidades com relação à segurança e devem estar capacitados para a realização de suas tarefas e utilização correta dos meios de acesso.

1.6.15. OUTROS REQUISITOS APLICÁVEIS

1.6.15.1. A CONTRATADA deve executar o objeto do certame em estreita observância dos ditames estabelecidos pela Lei nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais LGPD), quando aplicável ao objeto.

2. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

2.1. O Coren-SP possui em operação, atualmente, um conjunto de 620 máquinas (entre desktops, notebooks e servidores Windows) que demandam proteção contra vírus. Neste momento, trabalhamos com rotação de licenças, tendo sempre ativas simultaneamente, em torno de 600 máquinas, totalizando 600 licenças da Solução Endpoint ESET em operação.

2.2. Considerando a data de validade das licenças em uso, a princípio, o Coren-SP demanda a renovação ou a contratação de novas licenças para, minimamente, 650 máquinas, correspondentes ao parque tecnológico atual.

2.3. Porém, considerando projeção de expansão da quantidade de máquinas em operação, espera-se que, nos próximos 36 meses, pode haver demanda para 150 licenças adicionais (completando um total de 800 licenças). Tendo em vista a possível implementação de trabalho remoto de forma definitiva e considerando também critérios orçamentários e de organização administrativa e técnica internos em relação à compra/instalação de terminais (o que justifica o registro de preços de licenças como objeto, da licitação qualquer que seja a Solução escolhida, considerando que se encontra atendido o requisito do art. 3, IV do Decreto nº 7.892/2013)

2.4. Importante notar que houve um aumento inesperado no uso simultâneo de licenças de Antivírus em 2020, devido ao trabalho remoto com o uso simultâneo de dois computadores por usuário decorrentes do acesso remoto (notebook em casa + estação no Coren-SP).

2.5. Em relação à quantidade de bens/serviços a serem demandados, tem-se que, conforme detalhamento na análise de soluções abaixo, a renovação das licenças em uso não demandará serviços de implantação/treinamento para operação e a troca de Solução demandará, além das licenças acima quantificadas, a contratação de serviços de implantação da Solução (instalação/desinstalação/configuração) e de treinamento para operação da Solução pelos Administradores de TI.

3. ANÁLISE DE SOLUÇÕES

A – LEVANTAMENTO DE SOLUÇÕES DISPONÍVEIS

3.1. NECESSIDADES SIMILARES EM OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA E AS SOLUÇÕES ADOTADAS

3.1.1. Toda empresa, pública ou não precisa possuir solução de antivírus contratada e instalada em suas máquinas com sistema operacional Windows;

3.1.2. Diversos órgãos tratam de realizar contratação de licenças para segurança de Endpoints, a exemplo da Câmara Municipal de Campinas no contrato nº 43/2020 (https://www.campinas.sp.leg.br/transparencia/contratos/2020/contrato-n-deg43-2020), que contratou 162 licenças de ESET Endpoint Security + File Security.

3.2. ALTERNATIVAS DO MERCADO

3.2.1. Atualmente não existe substituição/alternativa a solução de Antivírus (Endpoint);

3.3. POLÍTICAS, OS MODELOS E OS PADRÕES DE GOVERNO (A EXEMPLO DO EPING, EMAG, EPWG, ICP-BRASIL E E-ARQ BRASIL, QUANDO APLICÁVEIS)

3.3.1. Não se aplica;

3.4. NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO OU ENTIDADE PARA VIABILIZAR A EXECUÇÃO CONTRATUAL

3.4.1. Não se aplica;

3.5. AQUISIÇÃO NA FORMA DE BENS X CONTRATAÇÃO COMO SERVIÇO

3.5.1. Não existe licença perpétua de antivírus devido a característica intrínseca do software, que se trata de solução que precisa ser constantemente atualizada com as definições de ameaças que surgem constantemente ao redor do mundo.

3.6. DIFERENTES MODELOS DE PRESTAÇÃO DO SERVIÇO

3.6.1. Antivírus para empresas são comercializados no modelo licença por máquina;

3.7. DIFERENTES TIPOS DE SOLUÇÕES EM TERMOS DE ESPECIFICAÇÃO, COMPOSIÇÃO OU CARACTERÍSTICAS DOS BENS E SERVIÇOS INTEGRANTES

3.7.1. Não se aplica;

3.8. AMPLIAÇÃO OU SUBSTITUIÇÃO DA SOLUÇÃO IMPLANTADA

3.8.1. Atualmente o Coren-SP possui um total de 600 licenças de antivírus ESET. Sendo necessária ampliação da quantidade em 200 licenças para o próximo contrato, tendo em vista o aumento na quantidade de máquinas simultaneamente ativas e em uso no ambiente, em grande parte, decorrente do trabalho remoto imposto pela pandemia da

Covid19.

3.8.2. Ampliações adicionais as 800 previstas deverão ocorrer por meio de contratação de licenças adicionais, por meio de processo licitatório.

3.9. DIFERENTES MÉTRICAS DE PRESTAÇÃO DO SERVIÇO E DE PAGAMENTO

3.9.1. O pagamento é em parcela única no momento da ativação do pacote de licenças. Não se tratando de serviço com pagamento mensal;

B – IDENTIFICAÇÃO DAS SOLUÇÕES

ID	DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO)
1	**Manutenção da Solução Atual (ESET, através da extensão/contratação de licenças)** Nesse cenário, será comprada apenas a licença Endpoint Security ESET para 800 máquinas e o suporte para o período do contrato, não sendo necessária a contratação de treinamento nem de horas técnicas de consultoria para instalação e configuração do novo ambiente, visto que a infraestrutura da solução ESET já se encontra instalada, configurada e estável no Coren-SP. Assim, nesse cenário, a compra e as atividades técnicas necessárias para adequação são extremamente mais simples. Não necessitando de contratação de treinamento para a equipe de TI nem de contratação de técnicos certificados para a instalação do Antivírus nas mais de 600 máquinas do Coren-SP, espalhadas por todo o Estado, inclusive em residências de funcionários. Aumentaremos a quantidade das atuais 600 para 800 licenças através da pura aquisição de 800 licenças, não sendo aplicada a diferenciação de 600 licenças de extensão mais as 200 da aquisição. Visto que a precificação nesse caso não apresentou diferença conforme cotação recebida de fornecedor. Não é necessário também nesse cenário, que haja qualquer analise de atendimento da solução as especificações/necessidades do Coren-SP nem de amostra (considerando licenças ESET Endpoint Security + File Security), visto que esta já provou nos atender com perfeição nos últimos 3 (três) anos de funcionamento dentro do Coren-SP. Não existe licença perpétua nem software livre de antivírus devido a característica intrínseca do software, que se trata de solução que precisa ser constantemente atualizada com as definições de ameaças que surgem constantemente ao redor do mundo. A manutenção desse serviço, incluso nas licenças de antivírus, envolve diversas equipes de pesquisa e resposta ao redor do mundo inteiro, necessitando de tratamento rápido as novas ameaças encontradas, bem como tratativas em resposta a comportamentos suspeitos e tendências identificadas em tráfego de rede global.
2	**Troca de Solução (licitação genérica para contratação de Solução de Antivírus do tipo Endpoint)** Nesse cenário, seria necessária, além da compra das licenças e suporte para o período do contrato, a contratação de curso com profissional certificado e a contratação de fornecedor para remoção do antivírus atual e instalação do novo antivírus em todas as mais de 600 maquinas do Coren-SP, inclusive as diversas máquinas que se encontram em posse de funcionários em trabalho remoto imposto pela pandemia de Covid19. Além dos pontos mencionados, uma nova solução pode encarecer excessiva e desnecessariamente o custo total da contratação, visto que são poucas as soluções de antivírus que incluem todas as funcionalidades que fazemos uso no Coren-SP. Caso essa nova

	solução não seja entregue com as funcionalidades adicionais amplamente utilizadas no Coren-SP, citadas no item "Identificação das necessidades tecnológicas" deste estudo técnico, teríamos que fazer novas contratações separadas para atender a esses requisitos. Adicionalmente, é importante citar o tempo de 'deploy' dos clientes de antivírus de uma possível nova solução. Para usarmos como parâmetro de comparação, a instalação do novo antivírus na contratação de 2018 levou aproximadamente 50 dias (de 19/11/2018 a 10/01/2019). Esse período de instalação é marcado por diversas horas de diversos colaboradores da TI e fornecedores para a instalação propriamente dita, solução de eventuais problemas, configurações e entendimento do comportamento da solução na rede. Inclui-se nessa somatória de horas o tempo que funcionários fora da TI podem precisar disponibilizar suas máquinas para instalação e soluções de problemas pontuais. Todo esse período de instalação é um período que representa vulnerabilidade no ambiente, visto que sempre ocorrem casos de máquinas com soluções de segurança que não instalam completamente, falham e ficam paradas ou necessitam de reboot para começar a proteger a maquina e a rede. O tempo que leva-se para a correção dessa vulnerabilidade pode ser suficiente para que um vírus se propague na rede impactando serviços disponibilizados pelo Coren-SP a sociedade, em alguns casos, até mesmo de forma permanente.

C – ANÁLISE COMPARATIVA DE SOLUÇÕES

REQUISITO	SOLUÇÃO	SIM	NÃO	NÃO SE APLICA
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2			X
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

4.1. Com destaque às informações elencadas no título 'Levantamento de Soluções Disponíveis' acima, não foram identificadas soluções inviáveis para o objeto de estudo deste ETP.

5. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

5.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

5.1.1. SOLUÇÃO VIÁVEL 1: Manutenção da Solução Atual (ESET, através da extensão/contratação de licenças)

5.1.1.1. Além das questões não ligadas a custo financeiro (expostas nos demais itens desse estudo), observa-se que a Solução Viável 1 apresenta, também, vantajosidade econômica em relação à Solução Viável 2, conforme exposto a seguir:

5.1.1.2. Devido a não necessidade de desinstalar e instalar uma nova Solução de Segurança Endpoint bem como a não necessidade de treinamento para nova Solução, manter a solução ESET instalada no ambiente do Coren-SP permite à Administração economizar com os itens abaixo, visto que não haverá necessidade de dispendê-los ou contratá-los:

a) Custo com Trabalhador TI para acompanhamento, ajustes e atividades de instalação (2 funcionários);

b) Custo com Serviço de Instalação;

c) Custo com Treinamento da nova Solução, para 4 funcionários da TI;

5.1.1.3. O Anexo I deste ETP resume a pesquisa de preços elaborada pela Equipe de Planejamento da Contratação. A tabela do subitem '5.2.5' abaixo está relacionada à **aquisição de licenças com validade de 36 (trinta e seis) meses**, entendido como alternativa que proporcionará maior economicidade para a Administração.

5.1.2. SOLUÇÃO VIÁVEL 2: Troca de Solução (licitação genérica para contratação de Solução de Antivírus do tipo Endpoint)

5.1.2.1. Essa opção, como detalhado nas tabelas do subitem 5.2 abaixo, representa um aumento de aproximadamente 19,7% (de R$ 113.200,00 para R$ 140.853,02) no custo total estimado da Solução, segundo o estudo realizado com as variáveis descritas no item "Mapa Comparativo dos Cálculos Totais de Propriedade (TCO)";

5.1.2.2. Esse aumento no custo total se dá pela necessidade de contabilização de alguns itens necessários para a adequada implementação de nova Solução de Segurança Endpoint;

5.1.2.3. Nessa opção de Solução é preciso contabilizar as horas de Trabalho da própria equipe de TI do Coren-SP para acompanhamento e realização de atividades de apoio e solução de problemas na desinstalação do software atual e instalação do software novo;

5.1.2.4. Outro custo necessário para a contabilização do custo total nessa opção de Solução é custo do serviço de desinstalação da Solução atual e instalação da nova solução nas centenas de estações de trabalho e servidores do Coren-SP espalhadas por todo o estado, inclusive em residências de funcionários devido a empréstimos motivados pelo trabalho remoto imposto pela pandemia da Covid-19;

5.1.2.5. Por último, o custo e horas de treinamento oficial para a nova solução

eventualmente contratada também precisa ser contabilizado no custo total dessa Solução.

5.1.2.6. Destaque-se que – apenas - para fins de comparação dos custos totais de propriedade na tabela do subitem '5.2.1' abaixo, foi reproduzido o valor de custo de licença de software ESET.

5.2. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

5.2.1. A tabela abaixo está relacionada à subscrição de licenças por 36 (trinta e seis) meses, entendido como alternativa que proporcionará maior economicidade para a Administração.

5.2.2. Pode-se afirmar que o tempo aproximado para conclusão das desinstalações e instalações de nova Solução de Segurança Endpoint é de, aproximadamente, 50 (cinquenta) dias corridos, considerando a experiência mais recente da TI do Coren-SP no último contrato para esse tipo de Solução (implantação das licenças adquiridas por meio do PE 15/2018);

5.2.3. Assim sendo, considerando que o período de cinquenta dias corridos corresponde a, aproximadamente, 36 (trinta e seis) dias úteis e, considerando a m.d.o. em período parcial (4 horas) de 1 Analista de Segurança da Informação, responsável pela atividade, e de 1 técnico de informática, apoiando a implantação da Solução, tem-se cerca de 144 (cento e quarenta e quatro) horas úteis de trabalho dispendidas por cada empregado na referida atividade. Esse cálculo, destaque-se, não inclui horas de outros analistas que tambem se envolvem nas implementações na rede, direta e indiretamente.

5.2.4. A tabela abaixo estima um custo de pessoal interno envolvido na implantação de uma Solução de Segurança Endpoint:

SALÁRIO MÉDIO (TÉCNICO DE INFORMÁTICA E ANALISTA DE SI)[3]	CUSTO HOMEM-HORA (SALÁRIO DIVIDIDO PELA QTDE DE HORAS TRABALHADAS NO MÊS – 176HS)	QUANTIDADE DE HORAS TRABALHADAS NO PROJETO (MEIO PERÍODO POR 36 DIAS ÚTEIS - 50 DIAS CORRIDOS)	QUANTIDADE DE FUNCIONÁRIOS DA TI ENVOLVIDOS NO PROJETO	CUSTO TOTAL COM M.D.O.
R$ 6.393,00	R$ 36,00	144	2	**R$ 10.462,01**

5.2.5. Isto posto, a tabela abaixo ilustra o **Comparativa do Custo das Soluções** consideradas viáveis neste ETP.

5.2.5.1. Porém, para fins ilustrativos, considerar-se-á que as 800 (oitocentas) licenças foram subscritas em uma única oportunidade. Destaque-se que a tabela abaixo não vislumbra a hipótese de pagamentos parcelados, considerando que observamos o paradigma de pagamento total da subscrição após o recebimento da instalação como padrão de mercado nas contratações públicas.

5.2.5.2. A subscrição de licenças por um período de 3 anos (36 meses), destaque-se, proporcionará significativa economicidade para a Administração no sentido de ampliarmos a periodicidade da realização de licitações destinadas à manutenção da Solução, especialmente porque se trataria de procedimentos para renovação de

[3] Informação extraída do Portal da Transparência do Coren-SP, disponível em: http://ouvidoria.cofen.gov.br/coren-sp/transparencia/remuneracao-dos-empregados/?page=1. Acesso: 29/06/2021.

licenças de uma mesma Solução.

5.2.5.3. Cabe destacar que um objeto com preços registrados pode ser solicitado **dentro do período de vigência da Ata RP**, isto é, 12 (doze) meses (ENTRE OS ANOS 1 e 2, permitindo a realização de uma programação de dispêndio).

ID.	VARIÁVEL DE CUSTO	ESTIMATIVA DE TCO AO LONGO DOS ANOS			CUSTO TOTAL ESTIMADO (EM 36 MESES)
		ANO 1	ANO 2	ANO 3 (Realização de nova licitação manutenção/substituição da Solução)	
Solução Viável 1	Licenças com validade de 36 meses (incluindo suporte e manutenção)	**R$ 113.200,00** (máximo de 800 licenças, com validade de 36 meses x R$ 141,50, que é o custo unitário estimado)	R$ 0,00	R$ 0,00	**R$ 113.200,00**
	Mão de Obra (pessoal interno)	Não necessário			
	Custo de Instalação da Solução	Não necessário			
	Treinamento	Não necessário			
Solução Viável 2	Licenças com validade de 36 meses (incluindo suporte e manutenção)	**R$ 113.200,00** (máximo de 800 licenças, com validade de 36 meses x R$ 141,50, que é o custo unitário estimado)	R$ 0,00	R$ 0,00	**R$ 140.853,02**
	Mão de Obra (pessoal interno)	R$ 10.462,01			
	Custo de Instalação da Solução[4]	R$ 7.191,01			
	Treinamento[4]	R$ 10.000,00			

6. JUSTIFICATIVA PARA ESCOLHA DA SOLUÇÃO

6.1. Considerando critérios de ordem técnica e econômica, detalhados nos tópicos imediatamente anteriores deste ETP, a Equipe de Planejamento da Contratação considera que a **Solução 1 - Manutenção da Solução Atual (ESET, através da extensão/contratação de licenças)** é aquela que melhor atenderá o Coren-SP, pelos seguintes motivos:

6.1.1. Esse cenário mostra-se mais econômico ao possibilitar que abramos mão de serviços de instalação e treinamento, visto que a solução já se encontra instalada em todos os servidores e estações do Coren-SP;

6.1.2. A Solução também se encontra madura ao não apresentar problemas que necessitem de atenção das equipes técnicas e também ao podermos dizer que conhecemos a ferramenta, suas nuances e configurações, encurtando significativamente os tempos de tratativa de eventuais problemas;

6.1.3. Mostra-se também mais viável do ponto de vista técnico ao garantir a manutenção dos serviços nos moldes dos que possuímos hoje, com as devidas soluções adicionais de segurança

[4] Utilizado como referência valores de licitação similar (Solução Endpoint) contratados pela Funasa, por meio do PE 19/2020, homologado em 26/06/2021. Para tanto, foi definido valor proporcional de custo de instalação e de treinamento: instalação ficou R$ 8,98 por unidade (x 800 = R$ 7.191,01) e treinamento R$ 10.000,00 por unidade (vezes 4 = R$ 40.000,00).

e gerenciamento, detalhadas abaixo;

6.1.4. Nesse cenário é também excluída a coleção de vulnerabilidades que são expostas em situações de instalação de softwares de segurança em centenas de estações em diferentes localidades geográficas pelo Estado de São Paulo, garantindo que permaneçamos 100% do tempo aderentes à Política de Segurança da Informação interna e suas Normas.

6.1.5. Não há tampouco a necessidade de preocupação com incompatibilidades de software e Sistema Operacional, adequação de configurações e otimização/hardening das políticas de comportamento da solução, uma vez que essas atividades já foram todas realizadas e provadas úteis, adequadas e suficientes na solução atualmente instalada, prezando por um ambiente computacional o mais seguro o quanto possível, capaz de entregar confidencialidade, integridade e disponibilidade para os serviços dos departamentos internos do Coren-SP e consequentemente, ao público atendido pela Autarquia.

6.1.6. Finalmente, a Solução de Endpoint Protection instalada atualmente no Coren-SP (ESET) traz **funcionalidades adicionais** que são essenciais para a manutenção de um ambiente seguro e operacional. Essa solução se mostrou ao longo dos últimos 3 anos, ser efetiva no seu papel de proteger a rede de diversas ameaças, não apenas os vírus de computador, bem como entregar funcionalidades úteis na administração de TI e também de níveis de Segurança aceitáveis:

6.1.6.1. Controle de Mídias Removíveis: A solução ESET permite que façamos o bloqueio do uso de mídias removíveis (pendrives, CDs, etc.), liberando apenas para usuários que necessitam da liberação e passaram pelo processo de aprovação e assinatura do Termo de Responsabilidade, conforme definido no item 7.4 da Norma – Prevenção de Vírus: 7.4. O Coren-SP através do departamento de TI (Segurança da Informação) pode realizar o bloqueio de mídias removíveis (pen-drives, HDs externos, cartões de memória, etc.) através de ferramentas de gerenciamento com o intuito de aumentar os níveis de segurança do órgão. As exceções serão aqueles que comprovadamente necessitem dessa funcionalidade para exercício de suas funções inerentes ao Coren-SP. Tal exceção será aplicada apenas com aprovações do gestor imediato e assinatura do termo de responsabilidade;

6.1.6.2. Firewall e IPS de Host: Trata-se de uma camada adicional para proteção a ataques de rede e exploração remota de vulnerabilidades. Essa funcionalidade é essencial no ambiente do Coren-SP visto que possuímos máquinas que compartilham da mesma sub-rede (VLAN), e portanto, não tem sua comunicação interna na VLAN checadas pelo Firewall de Rede. Dessa forma, é essencial que se tenha firewall e IPS de host, sendo essa a única barreira de proteção contra ataques na mesma sub-rede, inclusive propagação de infecções por Worms.

6.1.6.3. Controle de Acesso Web e filtro de Email: o ESET Endpoint possui filtro Web para acessos a sites e endereços maliciosos e filtro de e-mails, como links de spam e phishing. Isso é importantíssimo hoje no nosso ambiente para aumentar o nível de bloqueio desses endereços, que caso não fossem duplamente filtrados (firewall de rede e Endpoint) poderíamos ter casos onde essa barreira é furada por atrasos de atualizações ou velocidades não adequadas na criação de definição de ameaças zero-day. Não depender de apenas um fabricante para essa proteção eleva consideravelmente nosso nível de proteção.

6.1.6.4. Controle de Banda para atualizações de definições de vírus: Existe no Coren-SP uma gama de diferentes velocidades de links de internet para as subseções. Isso implica na necessidade direta de que a solução de antivírus possua a possibilidade de controle da banda máxima a ser utilizada para atualização de definições de vírus. A ausência de tal funcionalidade deixaria as estações em determinadas subseções vulneráveis a ameaças, pois não conseguiriam concluir seus respectivos downloads de definições de vírus. Atualmente conseguimos ter esse controle devido a existência dessa funcionalidade na solução ESET instalada em nosso ambiente.

6.1.6.5. Agendamento de Reboot de Estações: Temos a necessidade de realizar reboots periódicos nas estações de trabalho do Coren-SP para conclusão de atualizações e eventuais limpezas de vírus, conclusões e aplicações de configurações, etc. Conforme definido na Norma de Uso Aceitável de Ativos, item 6.12, todas as estações devem ser reiniciadas ao menos uma vez por semana. A solução ESET permite que atendamos a essa demanda de forma simples e efetiva.

7. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

7.1. Descrição resumida da Solução

ITEM	DESCRIÇÃO/ESPECIFICAÇÃO	CÓDIGO CATSER	UNIDADE DE MEDIDA	QTDE TOTAL PARA REGISTRO	VALOR MÁXIMO ACEITÁVEL (UNITÁRIO)	VALOR TOTAL ESTIMADO PARA REGISTRO
1	Solução de segurança do tipo Endpoint Protection (Antivírus, Proteção Web, HIPS e Firewall de Host) e Gerência centralizada, incluindo, garantia, suporte e atualização por 36 (trinta e seis) meses.	350949	Unidade (licença)	800	**R$ 141,50**	**R$ 113.200,00**

7.2. JUSTIFICATIVA PARA O NÃO PARCELAMENTO DA SOLUÇÃO

7.2.1. Trata-se da contratação de Solução composta pelo fornecimento de licenças de software antivírus, com validade de 36 (trinta e seis) meses a partir da data de ativação/renovação das licenças e prestação de suporte técnico pela Contratada durante o período de validade das licenças. Assim sendo, tecnicamente, eventual parcelamento da contratação, ainda que utilizando mesmo software provocaria prejuízos em termos de operação e controle da Solução, tendo em vista a obrigação da Contratada em prestar suporte técnico ao Coren-SP sempre que necessário. Mesma justificativa é aplicável ao entendimento da Equipe de Planejamento da Contratação em não realizar a divisão do objeto em cota principal e cota reservada, tendo em vista que a divisão do objeto em dois itens provocaria prejuízo, do ponto de vista operacional, ao conjunto do objeto a ser contratado.

7.3. CÓDIGO CATSER: 350949 – Antivírus Corporativo.

8. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

8.1. Valor Total Estimado Para Registro de Preços: R$ 113.200,00 (cento e treze mil e duzentos

reais), conforme detalhamento da tabela do item 7.1 acima.

8.2. O valor unitário estimado das licenças foi definido a partir de pesquisas realizadas junto a fornecedores especializados, bem como referência de licitação da Administração, em atendimento aos parâmetros II e IV do art. 5 da IN SGD/ME nº 73/2017, que trata da pesquisa de preços para aquisição de bens e contratação de serviços pela Administração.

DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO
Considerando os elementos obtidos neste estudo preliminar, em termos de eficácia, eficiência, efetividade e economicidade, avalia-se como VIÁVEL a presente contratação.

APROVAÇÃO E ASSINATURA
Conforme o § 2º do Art. 11 da IN SGD/ME nº 01, de 2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC[5]:

INTEGRANTE REQUISITANTE/ TÉCNICO	**INTEGRANTE DA ÁREA DE APOIO ADMINISTRATIVO**
Regis de Oliveira Araujo Assinado de forma digital por Regis de Oliveira Araujo Dados: 2021.06.30 17:01:44 -03'00' _____ **Régis de Oliveira Araújo** Analista de Segurança da Informação – GTI/INFRA Matrícula 1044	Henrique Pereira Soares Assinado de forma digital por Henrique Pereira Soares Dados: 2021.06.30 16:53:28 -03'00' _____ **Henrique Pereira Soares** Coordenador II – GCC/SCC Matrícula 975
RESPONSÁVEL PELA ÁREA REQUSITANTE/TÉCNICA (GTI)	
Rafael Conceição da Silva Assinado de forma digital por Rafael Conceição da Silva Dados: 2021.06.30 16:39:06 -03'00' _____ **Rafael Conceição da Silva** Gerência - GTI Matrícula 455	

[5] No caso do Coren-SP, a Autoridade Superior realiza a aprovação dos artefatos da contratação por meio de Despacho Circunstanciado encartado nos autos do Processo Administrativo de Contratação, cf. etapa 10 do Anexo I da Norma Interna Coren-SP/CG/NI/001/2013 – Versão 3.0.