TERMO DE REFERÊNCIA - SERVIÇO SEI Nº 27711528/2025 - SAP.UGC

1. DEFINIÇÃO DO OBJETO, INCLUÍDOS SUA NATUREZA, OS QUANTITATIVOS, O PRAZO DO CONTRATO E, SE FOR O CASO, A POSSIBILIDADE DE SUA PRORROGAÇÃO

1.1 Objeto da contratação: Contratação de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint)

1.2 Especificações técnicas

1.2.1 São itens que compõem a contratação:

Item	Especificação	Unidade	Quantidade Ano 1	Quantidade Ano 2	Quantidade Ano 3	Quantidade Ano 4	Quantidade Ano 5
1	Solução corporativa de antivírus e antimalware com tecnologia EDR (aquisição temporária de licenças, atualizações, manutenção e suporte técnico para estações de trabalho, dispositivos móveis e servidores)	Serviço (Licenças de Uso de Software)	20.000	20.000	20.000	20.000	20.000

1.2.2 Os quantitativos apresentados na tabela do item 1.2.1, se referem ao quantitativo máximo anual que poderá ser contratado, sendo que **o quantitativo mínimo anual será de 10.000 (dez mil) licenças**.

1.2.3 As licenças têm validade de um ano a contar da data da entrega, sendo renovadas anualmente na mesma data, durante o período de execução do contrato.

1.2.4 Sempre que necessário e a critério da CONTRATANTE, poderá ocorrer solicitação para ativação de novas licenças, por meio de Ordem de Serviço limitando-se ao quantitativo máximo anual, conforme descrito na tabela do item 1.2.1.

1.2.4.1 No decorrer de cada anualidade (período de 12 meses), poderão ser adicionadas licenças, sendo que as mesmas têm vencimento na mesma data de renovação das licenças já ativadas. Exemplo: 100 licenças ativadas no início do contrato vencem no dia DD/MM/AA, após 6 meses de execução contratual são ativadas mais 50 licenças, então estas licenças vencem no mesmo dia (DD/MM/AA).

1.2.4.2 As licenças adicionais terão seu pagamento proporcional, considerando a quantidade de meses faltantes para término da anualidade. Exemplo: 100 licenças ativadas no início do contrato vencem no dia DD/MM/AA, após 6 meses de execução contratual são ativadas mais 50 licenças, então o pagamento destas licenças é equivalente ao valor de seis meses de uso (da ativação da licença ao término da anualidade).

1.2.5 A CONTRATADA deverá conduzir uma análise de ambiente (Assessment) da infraestrutura de TI da CONTRATANTE, com o objetivo de validar a compatibilidade da solução com os sistemas operacionais e realizar o dimensionamento ideal de recursos de rede e servidores. O relatório detalhado da análise de ambiente deverá ser entregue à CONTRATANTE em até 10 (dez) dias úteis após a assinatura da Ordem de Serviço Eletrônica.

1.2.6 A CONTRATADA deverá garantir a entrega das chaves de licença (part numbers do software) e a disponibilização para download da solução em um prazo máximo de 15 (quinze) dias úteis a partir da assinatura da Ordem de Serviço Eletrônica.

1.2.6.1 O início da implantação/configuração das licenças e do Console de Gerenciamento Centralizado deverá ocorrer em um prazo máximo de 20 (vinte) dias úteis após a assinatura da Ordem de Serviço Eletrônica.

1.2.6.2 A CONTRATADA terá prazo máximo de 30 (trinta) dias corridos, a contar da entrega das chaves de licença (part numbers do software), para finalizar a entrega dos produtos de software com seus serviços acessórios, incluindo instalação e configuração.

1.3 Da natureza

1.3.1 A presente contratação é classificada como "comum", pois seus padrões podem ser objetivamente definidos, conforme previsto no art. 6º, XIII, da Lei nº 14.133/2021.

1.3.2 A presente contratação será a de um serviço contínuo, cujo prazo de execução será de **60 (sessenta) meses**, prorrogável na forma do Art. 107 da Lei nº 14.133/2021, vez que a contratação está prevista no Plano Plurianual.

1.3.3 O prazo de vigência contratual será de **62 (sessenta e dois) meses**, vez que a contratação está prevista no Plano Plurianual, podendo ser prorrogado na forma do Art. 107 da Lei nº 14.133/2021, conforme as necessidades e conveniência da Administração Pública Municipal.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

O ambiente digital enfrenta um crescimento exponencial no número e na complexidade das ameaças cibernéticas. Ransomwares, malwares avançados, ataques de dia zero, engenharia social e outras técnicas maliciosas têm se tornado cada vez mais frequentes, atingindo tanto o setor privado quanto o setor público. Tais incidentes podem comprometer informações sigilosas, causar paralisações operacionais, prejuízos financeiros e danos à imagem institucional.

Diante desse cenário, soluções de segurança tradicionais - baseadas exclusivamente em assinaturas - têm se mostrado insuficientes para enfrentar ameaças modernas, que frequentemente são inéditas, persistentes e adaptáveis.

Nesse sentido, a contratação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint**)** evolui o conceito de antivírus tradicional ao oferecer um conjunto de funcionalidades voltadas à:

- Detecção comportamental de ameaças em tempo real.
- Resposta automatizada a incidentes.
- Isolamento de máquinas infectadas para evitar propagação.
- Coleta de dados e logs para análise forense.
- Visibilidade completa dos endpoints da rede.

Dessa forma, o EDR transforma o processo de proteção de endpoints (estações de trabalho, notebooks e servidores) em uma abordagem proativa, com monitoramento contínuo e capacidade de resposta imediata, mesmo diante de ameaças desconhecidas.

São benefícios esperados dessa contratação:

- **Detecção avançada de ameaças**: A tecnologia EDR oferece mecanismos de detecção baseados em comportamento e inteligência artificial, capazes de identificar ataques sofisticados, como ransomwares, malwares polimórficos e ameaças de dia zero, que geralmente não são identificadas por soluções tradicionais de antivírus.
- **Resposta automatizada e contenção de incidentes**: A solução permite a resposta automatizada a eventos suspeitos, com ações como isolamento de endpoints, encerramento de processos maliciosos e remoção de arquivos comprometidos. Isso reduz significativamente o tempo de reação e os impactos operacionais

decorrentes de incidentes de segurança.

- **Visibilidade e monitoramento centralizado**: Com um painel de controle unificado, a solução proporciona visibilidade contínua de todos os endpoints da rede, permitindo a análise de comportamento, detecção de anomalias e monitoramento em tempo real das ameaças.
- **Redução do risco de vazamento de dados**: A solução contribui diretamente para a proteção de dados sensíveis e estratégicos, reduzindo o risco de acessos não autorizados, sequestro de informações e exfiltração de dados.
- **Análise forense e suporte à auditoria**: A funcionalidade de EDR inclui coleta e armazenamento de logs detalhados de eventos relacionados à segurança, possibilitando análise forense posterior, auditoria de conformidade e aprimoramento contínuo das políticas de segurança da informação.
- **Alta disponibilidade e continuidade dos serviços**: Ao mitigar de forma proativa incidentes de segurança, a solução contribui para a estabilidade dos serviços digitais da instituição, evitando interrupções, perdas de produtividade e danos à imagem institucional.
- **Integração com ecossistemas de segurança**: A solução pode ser integrada a ferramentas complementares como firewalls, sistemas de prevenção de intrusão (IPS/IDS), soluções de backup e plataformas de gerenciamento de eventos e informações de segurança (SIEM), fortalecendo a abordagem de segurança em camadas.

Ademais, destacamos que a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com EDR (Detecção e Resposta de Endpoint) está amparada por fundamentos legais e boas práticas, tais como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que exige a adoção de medidas técnicas e administrativas adequadas para a proteção de dados pessoais, sob pena de sanções legais, o Marco Civil da Internet (Lei nº 12.965/2014), que estabelece a responsabilidade dos gestores públicos quanto à proteção da integridade dos dados e dos sistemas utilizados, além de atender boas práticas internacionais de segurança da informação, como as preconizadas pela ISO/IEC 27001:2022 e pelo framework NIST.

Diante o exposto e considerando os riscos crescentes no ambiente digital e da necessidade de proteger os sistemas e dados institucionais, a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), não é apenas recomendável, mas essencial. Trata-se de uma medida estratégica e necessária para garantir a integridade, disponibilidade e confidencialidade das informações, bem como a continuidade das operações realizadas pela Prefeitura de Joinville.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO TODO O CICLO DE VIDA DO OBJETO

3.1 Conforme Estudo Técnico Preliminar - ETP constante no presente processo, a melhor solução encontrada de momento para atendimento ao interesse público envolvido é a contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), conforme especificações técnicas, com disponibilização de atualizações, manutenção e suporte técnico para a Prefeitura de Joinville/SC pelo período de 60 (sessenta) meses.

4. REQUISITOS DA CONTRATAÇÃO

4.1 REQUISITOS TÉCNICOS

4.1.1 Os requisitos técnicos estão descritos no ANEXO I - ESPECIFICAÇÕES TÉCNICAS do presente Processo.

4.2 REQUISITOS DE SUPORTE TÉCNICO

4.2.1 A Solução deverá incluir suporte técnico, de manutenção dos tipos preventiva, corretiva e adaptativa, bem como atualizações.

4.2.2 O Serviço de Suporte Técnico deverá ocorrer sem custos adicionais e incluir, *no mínimo*:

4.2.2.1 Orientações e esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução.

4.2.2.2 Orientação e apoio às questões relacionadas à integração de dados e sistemas.

4.2.2.3 Interpretação da documentação dos softwares fornecidos.

4.2.2.4 Orientações para identificar a causa de falha ou defeito de software e a solução destes.

4.2.2.5 Orientação para solução de problemas de performance e de ajustes das configurações dos softwares ofertados.

4.2.2.6 Orientação quanto às melhores práticas para parametrização e customização da solução.

4.2.2.7 Apoio na recuperação de ambientes em caso de panes ou perda de dados cuja responsabilidade seja da CONTRATADA .

4.2.2.8 Apoio para execução de procedimentos de atualização para novas versões dos softwares instalados.

4.2.2.9 Resolução de problemas de natureza técnica.

4.2.3 O Suporte Técnico será acionado pela CONTRATANTE exclusivamente por servidores da Unidade de Tecnologia da Informação (SAP.UTI).

4.2.4 A CONTRATADA deverá disponibilizar uma ferramenta eletrônica de registro de solicitação de serviços, configurável, para os níveis mínimos de serviços exigidos pela CONTRATANTE. Sendo facultado, o acionamento do suporte técnico por ligação telefônica, desde que este posteriormente desdobre-se em uma solicitação registrada na ferramenta eletrônica.

4.2.5 O registro de chamados em sistema da CONTRATADA servirá para facilitar o gerenciamento do processo de Suporte Técnico e, deverá suportar transações de abertura, registro, decisões e encaminhamentos dos atendimentos, com monitoramento, análise, avaliação do atendimento, e disponibilidade para o gerenciamento dos níveis de serviços pela CONTRATANTE, devendo conter em sua base de dados no mínimo os seguintes dados acessíveis à CONTRATANTE:

4.2.5.1 Sistema disponível em regime 24X7 (vinte e quatro horas por dia, sete dias por semana em qualquer período do ano).

4.2.5.2 Horário de cada chamado efetuado pela CONTRATANTE.

4.2.5.3 Nível de serviço respectivo a cada chamado e suas características.

4.2.5.4 Forma de atendimento *in loco* e remoto.

4.2.5.5 Número de registro de cada demanda/incidente (código único, rastreável).

4.2.5.6 Dados de identificação do(s) autor(es) do(s) chamado(s).

4.2.5.7 Dados de identificação do(s) atendente(s): nome completo, função na CONTRATADA e contato.

4.2.5.8 Histórico acerca do problema identificado pelo usuário em cada chamado (campo texto livre) ou disponibilizar codificação para escolha, caso haja maturidade no processo.

4.2.5.9 Status atualizado do atendimento a cada consulta ao sistema pela CONTRATANTE.

4.2.5.10 Tempo decorrido após a abertura do chamado no sistema até o encerramento.

4.2.5.11 Horário do início do atendimento e tempo do atendimento.

4.2.5.12 Solução proposta pelos atendentes da CONTRATADA .

4.2.5.13 Solução alternativa adotada pelos atendentes da CONTRATANTE.

4.2.5.14 Data e horário previsto para a finalização do atendimento.

4.2.5.15 Dados de identificação do(s) responsável(is), na CONTRATANTE, pelo(s) aceite(s) da(s) solução(ões) implementadas pela CONTRATADA .

4.2.5.16 Data e horário de finalização do atendimento.

4.2.5.17 Tempo médio de resolução dos incidentes/demandas.

4.2.6.18 Indicativo de atendimento ou não ao acordo de nível de serviço.

4.2.5.19 Histórico do atendimento (campo livre para descrição do serviço executado, comentários, sugestões, apontamentos e eventuais erros operacionais, críticas, etc).

4.2.6 O suporte deverá ser todo no idioma local, ou seja, português do Brasil.

4.3 REQUISITOS REGULATORIOS

4.3.1 Compliance: Conformidade com LGPD, ISO/IEC 27001:2022 e NIST Cybersecurity Framework.

4.3.2 Auditoria: Logs detalhados, com telemetria completa e suporte a auditoria e análise forense.

4.3.3 Relatórios: Geração automática de dashboards de risco (executivo) e relatórios de conformidade regulatória.

4.3.4 A CONTRATADA deverá garantir a continuidade e a plena funcionalidade da Solução de Proteção de Endpoint e EDR/EPP no território nacional. Caso a solução ofertada venha a sofrer restrições por:

4.3.4.1 Restrições Geopolíticas ou Sanções;

4.3.4.2 Impedimento Legal ou Regulatório;

4.3.4.3 Risco à Segurança ou Continuidade Operacional;

4.3.4.4 Ruptura Comercial ou Suporte;

4.3.4.5 Eventos de Força Maior ou catástrofes (naturais ou não);

4.3.5 Qualquer outro evento que impeça ou comprometa o seu uso, o seu suporte, a obtenção de atualizações de vacinas e engines de detecção ou a comunicação com os servidores de Intelligence necessários, a CONTRATADA será obrigada a:

4.3.5.1 Prover Solução Alternativa: Substituir a solução integralmente por uma ferramenta de segurança de endpoint de outro fabricante, com funcionalidades e desempenho equivalentes ou superiores aos requisitos técnicos desta contratação.

4.3.5.2 Assumir Custos: Arcar integralmente com todos os custos envolvidos no processo de substituição, incluindo, mas não se limitando a, novas licenças, serviços de migração (desinstalação, deployment e configuração da nova solução) e treinamentos de reciclagem da equipe técnica da CONTRATANTE.

4.3.5.3 Prazo para Migração: Iniciar a migração, instalação e configuração da solução alternativa no prazo máximo de 30 (trinta) dias corridos após a notificação oficial da restrição.

4.4 GERENCIAMENTO DE INCIDENTES

4.4.1 Quando a CONTRATADA receber relato de problema com a solução, o serviço de Suporte Técnico da CONTRATADA deverá emitir o número do chamado, o qual deverá ser utilizado em todas as comunicações a ele relacionadas.

4.4.2 Os usuários da Solução CONTRATADA , ao detectarem algum problema no uso do sistema, estarão orientados a acionar o serviço de Suporte Técnico da Administração Municipal, através da ferramenta de chamados em uso pela CONTRATANTE. Após triagem inicial e concluindo que o incidente é procedente, a Unidade de Tecnologia da Informação da Secretaria de Administração e Planejamento abrirá chamado para o serviço de Suporte Técnico da CONTRATADA , classificando as ocorrências em Prioridade 1, Prioridade 2, Prioridade 3 ou Prioridade 4, sendo:

4.4.2.1 Prioridade 1 (P1) – Nível de severidade crítico, aplicável quando há indisponibilidade total da solução ou falha de segurança grave (ex: ataque ativo detectado).

4.4.2.2 Prioridade 2 (P2) – Nível de severidade alto, aplicável quando há degradação significativa do serviço, com impacto em múltiplos usuários.

4.4.2.3 Prioridade 3 (P3) – Nível de severidade médio, aplicável quando há problema técnico sem impacto crítico, afetando poucos usuário.

4.4.2.4 Prioridade 4 (P4) – Nível de severidade baixo, aplicável quando há dúvidas, solicitações de configuração ou melhorias.

4.4.3 Em nenhuma hipótese a CONTRATADA poderá alterar a classificação das ocorrências. A classificação é prerrogativa da CONTRATANTE e sua alteração só poderá ser feita com a anuência da mesma.

4.4.4 A CONTRATADA deverá respeitar as seguintes características e prazos, contados do registro do chamado, para atendimento ou solução de ocorrências:

Nível de Severidade	Prioridade	Descrição	Tempo de Resposta Inicial	Tempo de Solução
Crítico	P1	Indisponibilidade total da solução ou falha de segurança grave (ex: ataque ativo detectado)	Até 30 minutos	Até 4 horas
Alto	P2	Degradação significativa do serviço, com impacto em múltiplos usuários	Até 2 horas	Até 8 horas
Médio	P3	Problema técnico sem impacto crítico, afetando poucos usuário	Até 4 horas	Até 24 horas
Baixo	P4	Dúvidas, solicitações de configuração ou melhorias	Até 8 horas	Até 72 horas

4.4.4.1 Para efeitos de acompanhamento e auditoria dos chamados, será sempre considerado **horas corridas**.

4.4.5 Após, avaliação deste parecer inicial, a CONTRATANTE decidirá sobre a sua aceitabilidade. O não cumprimento do novo prazo acordado para a solução definitiva da ocorrência sujeitará a CONTRATADA às penalidades previstas no Contrato.

4.4.5.1 Desde que acordado com a CONTRATANTE, a CONTRATADA poderá, caso haja disponibilidade e respeitados os prazos definidos, atuar de forma remota utilizando-se das ferramentas homologadas pela CONTRATANTE para tal, visando maior celeridade no atendimento às demandas apresentadas.

4.4.6 A CONTRATANTE poderá prorrogar o prazo máximo do atendimento, desde que o atraso seja justificado pela CONTRATADA e a justificativa aceita pela CONTRATANTE.

4.4.6.1 A CONTRATADA deverá registrar as justificativas do possível atraso no sistema de acompanhamento de chamados e comunicar previamente a CONTRATANTE para que a prorrogação seja autorizada.

4.4.6.2 A justificativa de prorrogação deverá ser aprovada pela CONTRATANTE antes do término do prazo original, caso contrário não será considerada para fins de apuração dos níveis de serviço.

4.4.6.3 A prorrogação de prazo é totalmente discricionária por parte da CONTRATANTE em relação a um chamado específico. E, não necessariamente, prorrogam automaticamente chamados de natureza semelhante.

4.4.7 O fechamento do chamado será registrado pela CONTRATADA , ainda que a posterior, com base no horário em que o problema apresentou-se resolvido na ótica dos usuários da solução. Após, a CONTRATANTE aprovará ou rejeitará o fechamento.

4.4.8 O cálculo do indicador “tempo de resolução” será feito pela diferença entre data-hora-minuto de abertura de chamado de suporte técnico e data-hora-minuto de fechamento do chamado, conforme registrados em sistema próprio da CONTRATADA .

4.4.9 Após a disponibilização da versão e/ou *build*, o serviço será homologado pela CONTRATANTE e disponibilizado para uso em produção.

4.4.10 O serviço de manutenção contemplará, no mínimo, o que segue:

4.4.10.1 **Manutenção Preventiva:** consiste no serviço, sem custos adicionais, de reparo na solução a fim de mitigar ou eliminar potenciais defeitos, ou riscos à integridade das informações identificadas pela CONTRATANTE ou pela CONTRATADA .

4.4.10.1.1 A CONTRATADA deverá periodicamente efetuar Manutenção Preventiva para prevenir e mitigar ameaças e falhas em maiores proporções.

4.4.10.1.2 A CONTRATADA ao diagnosticar uma ameaça à solução, deverá informar a CONTRATANTE a ocorrência verificada e, as medidas adotadas para a correção da mesma, bem como o prazo para a correção e, os impactos em virtude da ameaça e falhas detectadas, submetendo a aprovação da CONTRATANTE.

4.4.10.1.3 A CONTRATANTE avaliará o prazo proposto e, os impactos nas rotinas de trabalho e, informará a CONTRATADA se acata ou não o prazo proposto para a resolutividade.

4.4.10.1.4 Os registros de chamados relativos à Manutenção Preventiva poderão ser realizados pela CONTRATANTE ou por iniciativa própria da CONTRATADA .

4.4.10.1.5 A solução de problemas referentes à Manutenção Preventiva não implicará em custos adicionais à CONTRATANTE.

4.4.10.2 **Manutenção Corretiva:** consiste no serviço de reparo de defeitos identificados em componentes de software da solução, inclusive os destinados a suportar a integração com dados e com outros sistemas, e decorrentes do processo de migração, sem ônus adicionais.

4.4.10.2.1 A CONTRATADA se compromete a eliminar defeitos, erros ou falhas detectadas na solução, que impeçam o pleno funcionamento da mesma, sem qualquer ônus adicional para a CONTRATANTE.

4.4.10.2.2 Havendo a necessidade de manutenção corretiva, sendo a causa responsabilidade da CONTRATANTE, será facultado à CONTRATADA a cobrança, desde que previamente acordadas e autorizadas.

4.4.10.2.3 Os usuários da Solução, ao detectarem algum problema no uso do sistema, estarão orientados a acionar o serviço de Suporte Técnico da Administração Municipal, através da ferramenta de chamados em uso pela CONTRATANTE.

4.4.10.3 **Manutenção Adaptativa**: A CONTRATADA ajustará a Solução para atender atualizações decorrentes de alterações da legislação federal, no prazo estabelecido pelo legislador, sem ônus para a CONTRATANTE.

4.4.11 A Manutenção Preventiva e a Manutenção Corretiva serão consideradas sempre como provenientes de um incidente e, portanto, deverão ser atendidas com as mesmas prioridades, indicadas no item Gerenciamento de Incidentes.

4.5 GERENCIAMENTO DAS ATUALIZAÇÕES

4.5.1 Atualização de versões incorporam correções de erros ou problemas registrados bem como melhorias implementadas em relação à versão em uso pela CONTRATANTE.

4.5.2 A CONTRATADA deverá disponibilizar as novas versões/releases da Solução, com a respectiva documentação, em área de transferência, simultaneamente ao seu lançamento, sem custos adicionais para a CONTRATANTE.

4.5.2.1 A área de transferência será estabelecida em conjunto com a CONTRATANTE e a CONTRATADA.

4.5.3 A CONTRATADA se obriga a informar, de imediato, a CONTRATANTE toda e qualquer nova versão ou release lançada, com os respectivos detalhes técnicos, para análise e avaliação da CONTRATANTE quanto à oportunidade e cronograma das novas instalações dessas inovações.

4.5.4 A CONTRATADA deverá acompanhar a instalação ou mesmo implantar toda nova versão disponibilizada, quando solicitado pela CONTRATANTE, sem qualquer custo adicional.

4.5.5 A CONTRATADA , deverá repassar à CONTRATANTE os conhecimentos técnicos necessários para a perfeita compreensão, instalação e operação da versão/releases.

4.5.6 A CONTRATANTE estabelecerá um único ambiente de produção. A CONTRATADA , quando solicitada pela CONTRATANTE, deverá acompanhar ou mesmo instalar, a nova versão/releases, em qualquer um dos ambientes, sem ônus.

4.5.7 Caso a CONTRATADA evolua o produto para uma versão ou release com tecnologia, arquitetura ou configuração que exijam mudanças significativas nos sistemas ou nos ambientes computacionais da CONTRATANTE, a instalação dessa versão/release atualizada do produto deverá ocorrer sem custos adicionais para a CONTRATANTE e, ser precedida de uma análise detalhada dos impactos.

4.5.8 As manutenções programadas que impliquem em indisponibilidade da Solução deverão ser previamente acordadas entre a CONTRATADA e a CONTRATANTE com antecedência mínima de 72 (setenta e duas) horas.

4.5.8.1 As manutenções programadas devem ocorrer prioritariamente nos finais de semana, feriados e pontos facultativos ou durante os dias úteis entre 19h00 e 6h00 (fora do horário comercial).

4.5.9 Em qualquer uma das manutenções previstas, havendo necessidade de alterações na estrutura ou nos registros do banco de dados, esta deverá ser previamente aprovada pela CONTRATANTE.

4.6 REQUISITOS DE TREINAMENTO

4.6.1 A CONTRATADA deverá realizar treinamento sobre a utilização da solução de antivírus fornecida. O treinamento deve envolver toda a estrutura da solução e seus módulos. Após o treinamento, a equipe técnica da CONTRATANTE deverá estar apta a efetuar a instalação, configuração, atualização e gerenciamento da solução.

4.6.1.1 O treinamento deverá envolver aspectos teóricos e aspectos práticos.

4.6.1.2 A carga horária mínima do treinamento deverá ser de 8 (oito) horas.

4.6.2 O treinamento deverá ser realizado em formato presencial e/ou remoto, conforme definido previamente pela CONTRATANTE.

4.6.2.1 Em caso de treinamento presencial, a CONTRATANTE providenciará a infraestrutura física (sala, projetor, computadores e acesso à rede) necessária para a realização do mesmo.

4.6.2.1.1 Quanto escolhido a modalidade presencial, o treinamento deverá ocorrer de segunda a sexta-feira das 08h00 às 12h00, devendo ser previamente agendado com a CONTRATANTE.

4.6.2.2 Em caso de treinamento remoto, deverão ser utilizadas plataformas que permitam a interação entre os participantes e o(s) instrutor(es) em tempo real.

4.6.3 Os treinamentos deverão atender aos diferentes perfis de usuários da solução, incluindo equipe técnica e administradores ou gestores do sistema.

4.6.3.1 A definição exata do público será feita em conjunto com a CONTRATANTE durante o planejamento da execução do mesmo.

4.6.4 Todos os treinamentos, tanto presenciais quanto remotos, deverão ser gravados na íntegra, com qualidade adequada de áudio e vídeo.

4.6.4.1 As gravações deverão ser disponibilizadas à CONTRATANTE em formato digital (.mp4 ou compatível).

4.6.4.2 As gravações e os materiais de apoio deverão ser disponibilizados em repositório eletrônico indicado pela CONTRATANTE, ou entregues em mídia digital, de forma a permitir a consulta posterior dos usuários.

4.6.5 A CONTRATADA deverá produzir e prover material didático completo necessário para o treinamento, garantindo que seja fornecido individualmente a todos os participantes. Incluindo minimamente, mas não se restringindo à: apostilas, manuais, apresentações, perguntas frequentes (FAQ), entre outros.

4.6.5.1 Todo o material deverá ser entregue em formato digital (PDF), em língua portuguesa, e deve refletir fielmente a versão implantada da solução.

4.6.5.2 A ementa do treinamento, com os todos os tópicos a serem abordados, deverá ser apresentada pela CONTRATADA em 05 (cinco) dias úteis após a assinatura da Ordem de Serviço Eletrônica, sendo permitido a CONTRATANTE solicitar a alteração (inclusão ou exclusão) de tópicos que julgar necessários em até 5 (cinco) dias úteis após a apresentação da ementa pela CONTRATADA .

4.6.6 A CONTRATADA deverá apresentar à CONTRATANTE:

4.6.6.1 Lista de presença (física ou digital) com identificação dos participantes.

4.6.6.2 Relatório com a carga horária realizada, datas e conteúdos ministrados.

4.6.7 O treinamento deverá ser realizado antes da entrada em produção da solução, ou conforme cronograma acordado entre as partes.

4.6.8 A CONTRATADA deverá disponibilizar e ministrar, anualmente, um Treinamento de Reciclagem (Refresher Training) com foco na equipe técnica e administradores ou gestores do sistema. Este treinamento deverá ter a carga horária mínima de 4 (quatro) horas e abordar as novas funcionalidades da solução implementadas no último ano, as tendências de malware e o aperfeiçoamento das técnicas de caça a ameaças (Threat hunting) na plataforma de EDR.

4.7 SUSTENTABILIDADE

4.7.1 Quando cabível, a CONTRATADA deverá realizar o descarte dos resíduos decorrentes da execução da contratação, bem como a e/ou a logística reversa dos produtos.

4.7.1.1 Como a presente contratação é de natureza intelectual e tecnológica, não há previsão de geração de resíduos sólidos ou produtos físicos que demandem logística reversa. Este item é mantido em caráter de conformidade com a legislação geral, caso haja a necessidade de algum descarte específico.

4.8 SUBCONTRATAÇÃO

4.8.1. Não é admitida a subcontratação do objeto.

4.9 GARANTIA DA CONTRATAÇÃO

4.9.1 O proponente deverá apresentar garantia de execução contratual (nos moldes do art. 96 e ss. da Lei n° 14.133/2021), no importe de **2% (dois por cento) do valor inicial do Contrato,** conforme previsto no art. 98 da Lei n° 14.133/2021, com validade durante a execução do Contrato e por **90 (noventa) dia**s após o término da vigência contratual;

4.9.1.1 No prazo máximo de **1 mês** após a homologação e anterior a assinatura do contrato, a contratada deverá apresentar comprovante de prestação de garantia, conforme art. 96, §3º da Lei nº 14.133/2021, caso opte pela modalidade seguro-garantia;

4.9.1.2 No prazo máximo de **10 (dez) dias úteis**, prorrogáveis por igual período, a critério do CONTRATANTE, contados da assinatura do Contrato, a CONTRATADA deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública ou fiança bancária;

4.9.1.3 Caso a modalidade de garantia escolhida for o depósito em dinheiro, este deverá ser efetuado em conta específica do CONTRATANTE, a ser indicado pelo gestor do contrato.

4.9.2 A CONTRATADA deverá apresentar comprovante de prestação de garantia, conforme art. 96, § 1º da Lei nº 14.133, podendo optar por caução em dinheiro, seguro-garantia, fiança bancária ou título de capitalização.

4.9.3 Na ocorrência de aditivos, com acréscimos de valores, a CONTRATADA deverá apresentar garantia complementar, equivalente a 2% (dois por cento), na mesma modalidade optada no contrato.

4.9.4 A CONTRATADA deverá apresentar comprovante de prestação de garantia;

4.9.4.1 A inobservância do prazo fixado (acima) para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor total do Contrato por dia de atraso, até o máximo de **2% (dois por cento);**

4.9.4.2 O atraso superior a **25 (vinte e cinco) dias** autoriza a CONTRATANTE a promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe **art. 137 da Lei n° 14.133/2021;**

4.9.5 A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de **90 (noventa) dias** após o término da vigência contratual.

4.9.6 A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

4.9.6.1 Prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações nele previstas;

4.9.6.2 Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo durante a execução do Contrato;

4.9.6.3 Multas moratórias e punitivas aplicadas pela CONTRATANTE à CONTRATADA;

4.9.7 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria;

4.9.8 Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

4.9.9 No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do **art. 827 do Código Civil;**

4.9.10 No caso de alteração do valor do Contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

4.9.11 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de **30 (trinta) dias úteis,** contados da data em que for notificada;

4.9.12 A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria;

4.9.13 Será considerada extinta a garantia:

4.9.13.1 com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado de que a CONTRATADA cumpriu todas as cláusulas do contrato;

4.9.13.2 no prazo de 90 (noventa) dias corridos após o término da vigência, caso a CONTRATANTE não comunique a ocorrência de sinistro.

4.10 VISTORIA

4.10.1. Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

4.11 DOS REQUISITOS DE PROTEÇÃO DE DADOS PESSOAIS

4.11.1 A CONTRATADA deverá observar e cumprir rigorosamente todos os dispositivos legais previstos na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), na Lei nº 12.965/2014 (Marco Civil da Internet) e demais normas aplicáveis à proteção de dados pessoais e segurança da informação.

4.11.2 Para os fins deste termo de referência e em conformidade com a LGPD:

4.11.2.1 A CONTRATANTE será considerada CONTROLADORA, sendo responsável por definir as finalidades e os meios de tratamento dos dados pessoais;

4.11.2.2 A CONTRATADA será considerada OPERADORA, sendo responsável por realizar o tratamento dos dados pessoais em nome da CONTRATANTE e exclusivamente de acordo com as instruções documentadas e fornecidas pela CONTRATANTE.

4.11.2.3 Eventuais subcontratadas deverão assumir idênticas obrigações de proteção de dados e segurança da informação.

4.11.3 O tratamento dos dados pessoais (como username, nome da máquina, IPs, logs de processos, etc.) coletados pela solução EDR será realizado exclusivamente para a finalidade de Segurança da Informação do CONTRATANTE, nos termos do Art. 7º, II (cumprimento de obrigação legal) ou VI (Administração Pública para execução de políticas públicas), e Art. 23 da LGPD.

4.11.4 É vedada a utilização dos dados para qualquer outro objetivo, bem como sua cessão ou comercialização.

4.11.5 A CONTRATADA deverá colaborar com a CONTRATANTE no atendimento aos direitos dos titulares de dados previstos nos artigos 17 a 22 da LGPD, incluindo acesso, retificação, anonimização, bloqueio, eliminação e oposição ao tratamento.

4.11.6 As solicitações dos titulares deverão ser atendidas observando-se os prazos estabelecidos na Lei de Acesso à Informação (Lei nº 12.527/2011): 20 (vinte) dias, prorrogáveis por mais 10 (dez) dias mediante justificativa expressa, conforme artigo 11, §§ 1º e 2º da referida lei.

4.11.7 A CONTRATADA manterá procedimentos claros para o exercício dos direitos dos titulares, garantindo canais de comunicação acessíveis e resposta adequada às solicitações, em conformidade com os procedimentos da administração pública.

4.11.8 A CONTRATADA deverá adotar medidas técnicas e organizacionais aptas a proteger os dados pessoais contra acessos não autorizados, destruição acidental ou ilícita, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

4.11.9 Medidas de Criptografia e Proteção de Dados:

4.11.9.1 Implementar criptografia para dados em trânsito e em repouso;

4.11.9.2 Utilizar algoritmos de criptografia reconhecidos internacionalmente;

4.11.9.3 Realizar backup seguro dos dados com criptografia adequada.

4.11.10 Controles de Acesso e Autenticação:

4.11.10.1 Implementar controles de acesso baseados no princípio do menor privilégio;

4.11.10.2 Utilizar autenticação multifator para acesso aos sistemas;

4.11.10.3 Manter trilhas de auditoria completas de todos os acessos.

4.11.11 Testes e Monitoramento:

4.11.11.1 Realizar testes periódicos de vulnerabilidade e penetração;

4.11.11.2 Manter planos atualizados de continuidade e recuperação de desastres;

4.11.11.3 Implementar sistema de monitoramento contínuo de segurança.

4.11.12 A CONTRATADA se compromete a implementar o conceito de Privacy by Design, assegurando que a privacidade e a proteção de dados pessoais sejam incorporadas desde a concepção do sistema até seu ciclo final de vida.

4.11.13 A CONTRATADA assegurará que todos os profissionais envolvidos na operação, manutenção e suporte da solução EDR/Antivírus recebam treinamento adequado e contínuo em proteção de dados pessoais, segurança da informação e uso responsável e ético dos dados de telemetria e logs de segurança da CONTRATANTE.

4.11.14 Os dados serão armazenados obrigatoriamente em datacenters localizados em território nacional, sendo vedada a transferência internacional sem autorização formal e prévia do Município.

4.11.15 Havendo necessidade de transferência internacional de dados, devidamente acordada com a CONTRATANTE, a CONTRATADA se compromete a:

4.11.15.1 Observar rigorosamente o disposto nos artigos 33 a 36 da LGPD;

4.11.15.2 Assegurar a adoção de cláusulas contratuais específicas e garantias adequadas;

4.11.15.3 Demonstrar conformidade com os padrões exigidos pela ANPD;

4.11.15.4 Comunicar formalmente à CONTRATANTE sobre a transferência.

4.11.16 A CONTRATADA não poderá comercializar, vender, ceder ou tratar os Dados Pessoais de telemetria e segurança da CONTRATANTE para finalidades secundárias (como marketing, desenvolvimento de outros produtos ou perfilização de titulares), exceto quando expressamente autorizado pela CONTRATANTE, para cumprimento de ordem judicial ou para atendimento de requisições de órgãos de controle.

4.11.17 A CONTRATADA manterá acordo de níveis de serviço específico para incidentes de segurança, estabelecendo prazos claros para resposta, comunicação e mitigação baseados na criticidade do incidente.

4.11.18 Procedimentos para Incidentes de Segurança:

4.11.18.1 Notificar a CONTRATANTE no prazo máximo de 24 (vinte e quatro) horas a contar da ciência do incidente;

4.11.18.2 Apresentar, em até 48 (quarenta e oito) horas, relatório técnico detalhado contendo a descrição do ocorrido, os dados afetados, medidas adotadas e responsáveis pelo tratamento;

4.11.18.3 Colaborar com a CONTRATANTE no cumprimento das obrigações de comunicação à ANPD e aos titulares dos dados, quando aplicável.

4.11.19 Correção de Vulnerabilidade quanto à proteção de dados:

4.11.19.1 As vulnerabilidades críticas deverão ser corrigidas em até 24 horas;

4.11.19.2 As vulnerabilidades altas deverão ser corrigidas em até 72 horas;

4.11.19.3 As vulnerabilidades médias e baixas deverão ser corrigidas conforme cronograma acordado;

4.11.19.4 A CONTRATADA disponibilizará toda a documentação comprobatória das providências adotadas.

4.11.20. A retenção de todos os Dados de Telemetria e Logs de Segurança ficará sob a exclusiva determinação da CONTRATANTE, devendo a CONTRATADA observar o prazo máximo de retenção estabelecido pela Política de Segurança da Informação (PSI) e/ou Regulamentação Específica do Município, salvo ordem judicial ou investigação oficial devidamente registrada.

4.11.21 Procedimentos de Descarte:

4.11.21.1 O descarte dos dados será realizado de forma segura e irreversível;

4.11.21.2 A CONTRATADA fornecerá certificado de eliminação segura dos dados;

4.11.21.3 Ao término do contrato, os dados deverão ser entregues à CONTRATANTE em formato aberto e padrão não proprietário.

4.11.22 Portabilidade de Dados:

4.11.22.1 A CONTRATANTE terá direito à portabilidade integral dos dados a qualquer tempo;

4.11.22.2 Os dados serão entregues em formato estruturado, de uso comum e leitura automatizada;

4.11.22.3 A migração não poderá implicar em perda de funcionalidades ou informações.

4.11.23. Todas as operações de tratamento deverão ser registradas em conformidade com o art. 37 da LGPD, possibilitando rastreabilidade e auditoria integral.

4.11.24 Registros Obrigatórios:

4.11.24.1 Acessos realizados: identificação do usuário, data, horário e finalidade do acesso;

4.11.24.2 Decisões automatizadas: registro de cada alerta de ameaça, detecção ou ação de resposta automatizada (do motor EDR), com taxa de confiabilidade e parâmetros utilizados pela Machine Learning (Inteligência Artificial);

4.11.24.3 Alterações nos dados: histórico de retenção, descarte ou exportação de informações;

4.11.24.4 Incidentes de segurança: logs de tentativas de acesso indevido, falhas ou vulnerabilidades detectadas.

4.11.25 A CONTRATANTE poderá, a qualquer tempo, solicitar documentos e realizar auditorias para verificação do cumprimento da legislação de proteção de dados, com comunicação prévia de 10 (dez) dias úteis.

4.11.26 Termos de Confidencialidade:

4.11.26.1 Todos aqueles que tiverem acesso aos dados deverão firmar termos específicos de compromisso, sigilo e confidencialidade, conforme modelo constante no Anexo SEI 27218734.

4.11.26.2 Os termos constituem instrumento de responsabilização em casos de incidentes ou vazamentos;

4.11.26.3 A violação dos termos sujeitará o infrator às sanções contratuais e legais cabíveis.

4.11.27 As obrigações relacionadas à proteção de dados permanecerão válidas após o término do contrato, especialmente quanto à confidencialidade e eliminação segura dos dados.

4.11.28 Em caso de alterações na legislação de proteção de dados durante a vigência do contrato, a CONTRATADA deverá adequar-se às novas exigências sem ônus adicional para a CONTRATANTE, no prazo máximo de 90 (noventa) dias da publicação da nova norma.

5. MODELO DE EXECUÇÃO DO OBJETO

5.1 Equipe Mínima

5.1.1 A CONTRATADA deverá dimensionar sua equipe, avaliando periodicamente seu desempenho e a qualidade dos serviços no decorrer do contrato.

5.1.2 A CONTRATADA deverá alocar, pelo menos um profissional na equipe com as competências e habilidades que atendam o seguinte critério:

5.1.2.1 Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação na área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas oferecido por instituição reconhecida pelo Ministério da Educação (MEC).

5.1.3 A equipe será responsável pela demanda com atendimento remoto e pela orientação dos profissionais que realizarão atividades presenciais, quando forem necessárias.

5.2 Frequência e Periodicidade da execução dos serviços

5.2.1 A execução dos serviços vinculados a presente contratação, ocorrerão da seguinte forma:

5.2.1.1 O serviço deverá estar disponível em regime 24x7 (vinte e quatro horas por dia, sete dias por semana em qualquer período do ano).

5.2.2 O suporte técnico, realizado remotamente ou *in loco*, deverá estar disponível das 8:00h às 18:00h de segunda-feira à sexta-feira ou, em casos específicos, em outros horários, inclusive finais de semana, feriados e pontos facultativos, desde que acordado entre as partes.

5.2.3 A CONTRATADA deverá providenciar um sobreaviso para ser acionado no período não compreendido no item 5.2.2.

5.2.4 A CONTRATADA deverá disponibilizar suporte técnico a partir da assinatura do contrato.

5.2.5 O suporte técnico deverá permanecer disponível por todo o período de vigência contratual, apto a atender as dúvidas dos usuários administradores da solução, dúvidas e problemas relacionados às atualizações e correções da solução, além de eventuais problemas com o gerenciamento de licenças, relacionados aos produtos adquiridos e mantidos.

5.2.6 Deverão ser informados os contatos do suporte técnico da solução, a ser prestado por meio dos canais: central de atendimento telefônico, plataforma de chamado, e-mail e presencial (caso o problema não possa ser resolvido por meio eletrônico), em dias úteis de segunda-feira à sexta-feira, observando, no mínimo, o horário de 8:00h às 18:00h.

5.2.6.1 A CONTRATADA deverá prestar atendimento, initerruptamente, nos horários especificados acima para o suporte técnico, e resolver qualquer requisição, incidente ou problema com a solução conforme prioridade, nos termos do item 4.4.4.

5.2.7 O atendimento de suporte e assistência técnica deverão ser disponibilizados em língua portuguesa.

5.2.8 Durante todo o período de vigência contratual, a CONTRATADA deverá disponibilizar as novas versões da solução, além de disponibilizar correções, novas tecnologias desenvolvidas e evoluções de segurança, sem ônus ou custo adicional para a CONTRATANTE.

5.2.8.1 A CONTRATADA deverá disponibilizar as novas versões e atualizações da solução no mesmo momento em que elas forem disponibilizadas ao mercado pelo fabricante.

5.2.9 Toda as licenças que compõem a solução devem contar com manutenções corretivas, sem ônus adicional, durante o prazo de vigência da licença de uso, para o caso de vícios, defeitos ou falhas.

5.3 Cronograma de execução dos serviços

5.3.1. A execução da presente contratação será pelo regime de execução indireta por preço unitário.

5.3.2 O início da execução do objeto ocorrerá a partir da assinatura da Ordem de Serviço Eletrônica, a contar da última assinatura da mesma.

5.3.3 A CONTRATADA deverá conduzir uma análise de ambiente (Assessment) da infraestrutura de TI da CONTRATANTE, com o objetivo de validar a compatibilidade da solução com os sistemas operacionais e realizar o dimensionamento ideal de recursos de rede e servidores. O relatório detalhado da análise de ambiente deverá ser entregue à CONTRATANTE em até 10 (dez) dias úteis após a assinatura da Ordem de Serviço Eletrônica.

5.3.4 A CONTRATADA deverá garantir a entrega das chaves de licença (part numbers do software) e a disponibilização para download da solução em um prazo máximo de 15 (quinze) dias úteis a partir da assinatura da Ordem de Serviço Eletrônica.

5.3.4.1 O início da implantação/configuração das licenças e do Console de Gerenciamento Centralizado deverá ocorrer em um prazo máximo de 20 (vinte) dias úteis após a assinatura da Ordem de Serviço Eletrônica.

5.3.4.2 A CONTRATADA terá prazo máximo de 30 (trinta) dias corridos, a contar da entrega das chaves de licença (part numbers do software), para finalizar a entrega dos produtos de software com seus serviços acessórios, incluindo instalação e configuração.

5.3.5 A CONTRATADA deverá entrar em contato com o gestor do contrato para que sejam acordados os meios e ferramentas a serem utilizadas para a entrega do software, códigos de acesso e comprovantes de licenciamento.

5.4 Local de execução dos serviços

5.4.1 O local de execução dos serviços é remoto devido a sua característica (licença de uso de software).

5.4.2 Eventual entrega física de produtos e/ou prestação de serviço in loco deverá ser realizada nas dependências da Diretoria de Tecnologia e Gestão, da Secretaria de Administração e Planejamento da Prefeitura Municipal de Joinville, localizado na Avenida Hermann August Lepper, número 10 - Bairro Saguaçu - CEP 89221-901 - Joinville - SC, das 08:00h às 18:00h.

5.5 Da garantia dos serviços e materiais empregados

5.5.1 A CONTRATADA deverá fornecer garantia conforme aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990, tanto para os produtos quanto para os serviços, de acordo com o Código de Defesa do Consumidor.

5.5.2 A garantia será prestada com vistas a manter os itens fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o CONTRATANTE.

5.5.3 A presente contratação será uma prestação de serviço continuada, considerando isso, a garantia se estende por todo período do Contrato, devendo ser observado o item 7.3 - Níveis Mínimos de Serviço, de acordo com o inciso XII do art. 92 da da Lei 14.133/2021.

5.5.4 Uma vez notificado, a CONTRATADA realizará a reparação ou substituição dos itens que apresentarem vício ou defeito no prazo de até 30 (trinta) dias corridos.

5.5.4.1 O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da CONTRATADA , aceita pelo CONTRATANTE.

5.5.5 O custo referente ao transporte dos itens cobertos pela garantia será de responsabilidade da CONTRATADA .

5.6. Procedimentos de transição e finalização do contrato

5.6.1 Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

6. MODELO DE GESTÃO DO CONTRATO

6.1 Da Gestão

6.1.1 A gestão do contrato será realizada por Comissão de Acompanhamento e Fiscalização conforme previsto na Instrução Normativa n° 03/2024 (SEI 0023970042) da Secretaria de Administração e Planejamento, restando como atores os servidores nomeados para compor a Comissão.

6.1.1.1 A Comissão de Acompanhamento e Fiscalização ou Comissão de Recebimento, será nomeada em até 10 (dez) dias úteis, contados da publicação do Contrato.

6.1.2 Caberá a Comissão de Acompanhamento e Fiscalização designada verificar o cumprimento pela CONTRATADA de todas as condições contratuais.

6.1.3 Define-se como forma de comunicação com a CONTRATADA a formal, nos termos do Decreto nº 64.109, de 18 de dezembro de 2024 (SEI 0023987931), que aprovou a Instrução Normativa n.º 03/2024 (SEI 0023970042), da Secretaria de Administração e Planejamento.

6.1.4 A Comissão de Acompanhamento e Fiscalização tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, quando necessário.

6.1.5 A Comissão de Acompanhamento e Fiscalização deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

6.1.6 Após o interregno de um ano contados a partir da apresentação da proposta e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação do **IPCA - Índice de Preço ao Consumidor Amplo**, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

6.2 Gestor do Contrato

6.2.1 A gestão do contrato será realizada pela Secretaria de Administração e Planejamento.

6.2.2 A fiscalização do contrato será realizada pela Secretaria de Administração e Planejamento, sendo que a Secretaria da Saúde, Secretaria de Educação, Hospital Municipal São José e Departamento de Trânsito de Joinville serão responsáveis pela subfiscalização do contrato.

6.2.3 Os ordenadores da despesa serão a Secretaria de Administração e Planejamento, Secretaria da Saúde, Secretaria de Educação, Hospital Municipal São José e Departamento de Trânsito de Joinville.

6.2.4 A unidade gestora indicada no item 6.2.1, fica responsável em publicar a portaria da Comissão de Gestão e Fiscalização, que tratará em conjunto sobre todos os assuntos relativos à execução da contratação, inclusive solicitações de reequilíbrio, cancelamento, entre outras, que possam a vir a impactar na execução contratual das demais unidades subfiscalizadoras.

6.2.5 A gestão não suprime as funções e competências do ordenador de despesa de cada unidade definido em Lei.

6.2.6 Os contatos da unidade fiscalizadora e das unidades subfiscalizadoras estão disponíveis no site: https://www.joinville.sc.gov.br/estrutura-organizacional/

6.3 Obrigações da CONTRATADA específicas do objeto

6.3.1 Fornecer mão-de-obra especializada, mantendo quadro de pessoal técnico qualificado para realização dos serviços.

6.3.2 Responder por quaisquer danos pessoais ou materiais causados por seus empregados, bem como àqueles provocados em virtude dos serviços executados e da inadequação de materiais e equipamentos empregados.

6.3.3 Será de responsabilidade da CONTRATADA todas as despesas necessárias para a prestação do serviço.

6.3.4 A CONTRATADA deverá arcar, sem ônus para o CONTRATANTE, com o custo do fornecimento de materiais de consumo que são considerados aqueles que se consomem à primeira aplicação, empregados em pequenas quantidades com relação ao valor dos serviços.

6.3.5 Obedecer às normas de segurança e medicina do trabalho para esse tipo de atividade, ficando por sua conta o fornecimento, antes do início da execução dos serviços, dos Equipamentos de Proteção Individual– EPI e coletiva EPC, caso necessário a seus funcionários.

6.3.6 Refazer/ Substituir / Atender nos prazos estimados no subitem 5.5.4 (conforme cada caso), bem conforme procedimento ali disposto, quanto a quaisquer problemas quanto ao(s) equipamento(s) / acessório(s)/ insumo(s) / serviços, que apresentarem defeitos/vícios, ocultos ou não, e/ou que se tornarem impróprios para uso a que são destinados, e/ou, que não correspondam com o Termo de Referência, sem ônus para CONTRATANTE.

6.3.7 Comunicar ao CONTRATANTE toda e qualquer irregularidade encontrada para o cumprimento do contrato.

6.3.8 A CONTRATADA deverá submeter-se às normas e políticas de segurança da CONTRATANTE e assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados à entidade CONTRATANTE, ou a terceiros, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança.

6.3.9 Promover a destinação final ambientalmente adequada e a logística reversa, sempre que a legislação assim o exigir.

6.3.10 Caso seja detectado algum problema no fornecimento ou na prestação do serviço prestado, este será levado formalmente ao conhecimento da CONTRATADA .

6.3.11 A CONTRATADA deverá sanar a irregularidade dentro do prazo que for estabelecido ou apresentar manifestação no prazo estabelecido na notificação emitida.

6.3.12 A CONTRATADA deverá indicar Preposto, representante da CONTRATADA , responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

6.3.13 Cabe a CONTRATADA fornecer juntamente com os equipamentos entregues os respectivos manuais de operação (em mídia e/ou impresso), em Língua Portuguesa, sem qualquer ônus para a CONTRATANTE.

6.3.14 A CONTRATADA responsabilizar-se única e exclusivamente, pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrentes da execução do objeto do presente Termo de Referência e seus anexos, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias. ou seja, por todas as obrigações e responsabilidades, sem qualquer ônus ao CONTRATANTE.

6.3.15 A CONTRATADA se responsabiliza por transportar, seus funcionários, ferramentas e máquinas sempre que o atendimento técnico *in loco* for solicitado, sem ônus para a CONTRATANTE.

6.3.16 A CONTRATADA fica obrigada ao cumprimento de todas as obrigações trabalhistas e previdenciárias em relação aos empregados contratados, inclusive no tocante às normas de saúde e segurança do trabalho, sob pena de aplicação das penalidades previstas no contrato administrativo.

6.4 Obrigações da CONTRATANTE específicas do objeto

6.4.1 Acompanhar e fiscalizar o cumprimento do presente Termo de Referência e do contrato.

6.4.2 Notificar a(s) CONTRATADA(S) quanto a qualquer irregularidade encontrada.

6.4.3 Permitir acesso dos empregados da(s) CONTRATADA(S) às dependências do(s) local(is) de entrega(s), caso necessário.

6.4.4 Prestar as informações e os esclarecimentos que venham a ser solicitados pela(s) CONTRATADA(S), quando necessário.

6.4.5 Comunicar formalmente a(s) CONTRATADA(S) qualquer falha e/ou irregularidade no fornecimento do(s) produto(s), determinando o que for necessário à sua regularização.

6.4.6 Aceitar/rejeitar, no todo ou em parte, o(s) serviços(s) executados pela(s) CONTRATADA(S).

6.4.7 Solicitar a correção dos serviço(s) que apresentarem defeito(s) ou vício(s) durante a verificação de conformidade e/ou no decorrer de sua instalação ou utilização.

6.4.8 Disponibilizar as instalações físicas e os meios materiais, tais como ponto de rede e de energia elétrica, necessários à execução dos serviços objeto do presente Termo de Referência.

6.4.9 Efetuar os pagamentos referentes aos serviços prestados pela CONTRATADA .

6.4.10 Quando do pagamento, efetuar a retenção tributária prevista na legislação aplicável.

6.5 Das sanções

6.5.1 No caso da presente contratação, as sanções administrativas serão as mesmas dispostas na Lei nº 14.133/2021 e no Edital.

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

7.1 Critérios de medição

7.1.1 O(s) serviços(s) será(ão) recebido(s):

7.1.1.1 **Provisoriamente**, no ato da entrega do(s) serviços(s), pela Comissão de Fiscalização e Acompanhamento do Contrato.

7.1.1.2 **Definitivamente**, no prazo máximo de 5 (cinco) dias úteis, contados após o recebimento provisório, a CONTRATANTE realizará o recebimento definitivo, que ocorrerá somente se o(s) serviço(s) estiver(em) conforme quantidade solicitada e em conformidade com as especificações do presente Termo de Referência.

7.1.2 Na hipótese de a verificação a que se refere o subitem 7.1.1.2 não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

7.1.3 O recebimento provisório ou definitivo do(s) serviços(s) não exclui a responsabilidade da(s) CONTRATADA(S) pelos prejuízos resultantes da incorreta execução do(s) futuro(s) Contrato(s).

7.1.4 Se a CONTRATANTE constatar, tanto no recebimento provisório como no definitivo, que o(s) serviço(s) prestado(s) não corresponde(m) ao exigido no presente Termo de Referência, ou em quantidade diversa da solicitada, a CONTRATADA deverá providenciar em 5 (cinco) dias úteis, a substituição/reposição do) serviço visando ao atendimento total das especificações, conforme item 1.2, sem prejuízo da incidência das sanções previstas no contrato, na Lei n°. 14.133/2021 e alterações posteriores e no Código de Defesa do Consumidor (Lei n°. 8.078/90).

7.1.5 O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.2 Critérios do pagamento

7.2.1 O pagamento do valor correspondente à vigência das licenças será efetuado **ANUALMENTE**.

7.2.1.1 O primeiro pagamento ocorrerá após a entrega das licenças, com vigência de 1 (um) ano.

7.2.1.2 Os pagamentos subsequentes serão realizados após a efetivação da renovação anual das licenças e durante o período de vigência do contrato, sendo o mesmo prorrogável na forma do Art. 107 da Lei nº 14.133/2021.

7.2.2 No primeiro ano de contrato o pagamento será efetuado após o **recebimento definitivo do serviço**.

7.2.3 Nos anos subsequentes, o pagamento será realizado a cada anualidade, ou seja, a cada doze meses, contatos a partir do **início do licenciamento**.

7.2.4 O pagamento será por **licença ativa**, após conferência e recebimento definitivo do atendimento das especificações do Termo de Referência.

7.2.5 Sempre que necessário e a critério da CONTRATANTE, poderá ocorrer solicitação para ativação de novas licenças, por meio de Ordem de Serviço.

7.2.6 As licenças adicionais têm vencimento na mesma data de renovação das licenças já ativadas. Exemplo: 100 licenças ativadas no início do contrato vencem no dia DD/MM/AA, após 6 meses de execução contratual são ativadas mais 50 licenças, então estas licenças vencem no mesmo dia (DD/MM/AA).

7.2.7 As licenças adicionais terão seu pagamento proporcional, considerando a quantidade de meses faltantes para término da anualidade. Exemplo: 100 licenças ativadas no início do contrato vencem no dia DD/MM/AA, após 6 meses de execução contratual são ativadas mais 50 licenças, então o pagamento destas licenças é equivalente ao valor de seis meses de uso (da ativação da licença ao término da anualidade).

7.2.8 A cada anualidade, e a critério da CONTRATANTE, poderá ocorrer solicitação para redução de licenças ativas, por meio de Ordem de Serviço, desde que respeitada a quantidade mínima a ser contratada, de acordo com o item 1.2.2.

7.2.9 Para fins de pagamento, a CONTRATADA deverá apresentar a comprovação da regularidade trabalhista, previdenciária e FGTS, além de outros documentos que comprovem a regularidade da CONTRATADA nos termos do artigo 92, inciso XVI da Lei nº 14.133/1993.

7.2.10 Emitir documentos fiscais em observância às regras de retenção dispostas na Instrução Normativa RFB nº 1.234 de 2012, sob pena de não aceitação.

7.2.11 O método de avaliação e conformidade dos serviços prestados, deverão observar os padrões mínimos de qualidade e desempenho apresentados no item 7.3.

7.3 Níveis mínimos de serviço

7.3.1 Para a execução da presente contratação será utilizado como critério de aferição os resultados dos Níveis Mínimos de Serviço (SLA).

7.3.1.1 Os níveis mínimos de serviços se constituem em critérios objetivos e mensuráveis estabelecidos entre a CONTRATADA e o CONTRATANTE com a finalidade de aferir e avaliar a prestação dos serviços contratados.

7.3.1.2 Para mensurar esses fatores são utilizados indicadores relacionados com a natureza e características dos serviços a serem contratados, os quais serão estabelecidas metas quantificáveis a serem cumpridas pela CONTRATADA.

7.3.2 A CONTRATADA será responsável pelo cumprimento, medição e envio das informações dos indicadores estabelecidos durante todo o prazo de vigência do contrato.

7.3.2.1 A medição dos indicadores estabelecidos serão auditados pela CONTRATANTE durante todo o prazo de vigência do contrato.

7.3.2.2 Os indicadores poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados, desde que acordado entre as partes.

7.3.3 Os indicadores de Níveis de Serviço deverão estar de acordo com a tabela abaixo, para cada mês civil e para todos os itens, conforme indicado:

Item	Indicadores de Níveis de Serviço	Descrição	Fórmula de Cálculo	Unidade de Medida	Meta Exigida
1	Percentual de *uptime*	**Disponibilidade do serviço** (Observação: descontados os tempos apurados de	[número total de horas no período de apuração - soma	% (Percentual) de	≥ 99%

		indisponibilidade resultantes de manutenção programada e problema decorrente da infraestrutura de processamento e comunicação disponibilizada pelo CONTRATANTE)	de todas as interrupções do sistema, em horas)] / [número total de horas no período de apuração] * 100	disponibilidade da aplicação	
2	SLA Crítico (P1)	Solicitação de **Nível de Severidade Crítico (P1)**, independente se incidente, preventiva ou corretiva, atendida em até 4 (quatro) horas corridas.	[Quantidade de solicitações P1 com atendimento resolvido em até 4 horas] / [Total de solicitações recebidas no mês e classificada em P1] * 100	% (Percentual) de atendimento no prazo	≥ 90%
3	SLA Alto (P2)	Solicitação de **Nível de Severidade Alto (P2)**, independente se incidente, preventiva ou corretiva, atendida em até 8 (oito) horas corridas.	[Quantidade de solicitações P2 com atendimento resolvido em até 8 horas] / [Total de solicitações recebidas no mês e classificada em P2] * 100	% (Percentual) de atendimento no prazo	≥ 90%
4	SLA Médio (P3)	Solicitação de **Nível de Severidade Médio (P3)**, independente se incidente, preventiva ou corretiva, atendida em até 24 (vibte e quatro) horas corridas.	[Quantidade de solicitações P3 com atendimento resolvido em até 24 horas] / [Total de solicitações recebidas no mês e classificada em P3] * 100	% (Percentual) de atendimento no prazo	≥ 90%
5	SLA Baixo (P4)	Solicitação de **Nível de Severidade Baixo (P4)**, independente se incidente, preventiva ou corretiva, atendida em até 72 (setenta e duas) horas corridas.	[Quantidade de solicitações P4 com atendimento resolvido em até 72 horas] / [Total de solicitações recebidas no mês e classificada em P4] * 100	% (Percentual) de atendimento no prazo	≥ 90%

7.3.4 As inoperâncias e/ou indisponibilidades dos serviços, no todo ou em parte, que não seja de responsabilidade da CONTRATANTE, devem gerar reembolso correspondente aos serviços não prestados proporcionais ao tempo de sua não prestação, com exceção das seguintes situações:

7.3.4.1 Falha na conexão ("link de dados") fornecida pela CONTRATANTE, sem culpa da CONTRATADA.

7.3.4.2 Falhas de fornecimento, de responsabilidade da CONTRATANTE, ou quaisquer indisponibilidades devido má gestão pela CONTRATANTE.

7.3.4.3 Interrupções necessárias para ajustes técnicos ou manutenção programada que serão informadas com antecedência mínima de 72h (setenta e duas horas) e se realizarão, preferencialmente, nos finais de semana, feriados e pontos facultativos ou durante os dias úteis entre 19h00 e 6h00 (fora do horário comercial).

7.3.4.4 Interrupções diárias necessárias para ajustes técnicos ou manutenção, com duração máxima de até 10 (dez) minutos, que serão informadas previamente e se realizarão preferencialmente entre 0h e 6h da manhã.

7.3.4.5 Intervenções emergenciais decorrentes da necessidade de preservar a segurança do ambiente, destinadas a evitar ou fazer cessar quaisquer incidentes ou destinadas a implementar correções de segurança.

7.3.4.6 Suspensão da prestação do serviço contratado por determinação de autoridades competentes ou por descumprimento das cláusulas do contrato.

7.3.4.7 Definição, pela CONTRATANTE, de infraestrutura e serviços de rede insuficientes para atender à sua própria demanda.

7.3.5 A disponibilidade do serviço (percentual de uptime) indicará o percentual de tempo, durante o período de 01 (um) mês de operação (considerando o mês de 30 dias), em que o serviço permanece em condições normais de funcionamento.

7.3.5.1 A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pela Comissão de Fiscalização e Acompanhamento do Contrato, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle da CONTRATADA.

7.3.6 A contagem do tempo para o atendimento inicia-se a partir da hora de abertura do chamado na plataforma disponibilizada pela CONTRATADA.

7.3.6.1 Para fins de entendimento, serão sempre consideradas horas corridas para a atendimento dos chamados, considerando a natureza do objeto.

7.3.7 Além das sanções usuais previstas na legislação e estabelecidas no contrato como penalidades por descumprimento de obrigações em relação a presente contratação, a CONTRATADA estará sujeita às sanções.

7.3.8 No caso de atrasos, inexecução total ou parcial do contrato, a CONTRATADA estará sujeita às seguintes penalidades:

7.3.8.1 Advertência, por escrito, quando praticar irregularidade de pequena monta – aquelas que não impliquem em sanções categorizadas como multa a critério do Município.

7.3.8.2 No caso de 03 (três) advertências consecutivas será aplicado à CONTRATADA uma multa de 5% (cinco por cento) sobre o valor total do contrato.

7.3.8.3 Multa de até 10% (dez por cento) em caso de inexecução parcial sobre o valor total do contrato.

7.3.9 No caso de atraso nos prazos previstos para os serviços descritos nos Níveis de Serviço, a CONTRATADA estará sujeita às seguintes penalidades:

7.3.9.1 Multa de 5% (cinco por cento) sobre o valor total do contrato para cada um dos casos em que não houver atendimento das metas exigidas nos itens 1, 2, 3 e 4 dos níveis mínimos de serviço, acrescida de 0,3% (três décimos por cento) a cada ponto percentual a maior de desconformidade.

7.3.9.2 Multa de 5% (cinco por cento) sobre o valor total do contrato em caso de atraso superior a meta exigida no item 5 dos níveis mínimos de serviço, acrescida de 0,3% (três décimos por cento) a cada dia de atraso na entrega.

7.3.10 A aplicação das sanções poderá ser reavaliada caso a CONTRATADA apresente justificativa técnica plausível e esta seja aceita pelo CONTRATANTE.

7.3.11 Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a CONTRATADA:

7.3.11.1 Não cumpriu as metas exigidas no item7.3.3, considerando-se ainda o item 7.3.4.

7.3.11.2 Deixe de executar, ou não executar com a qualidade mínima exigida as atividades CONTRATADA;

7.3.11.3 Deixe de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

8.1 Forma de seleção e critérios de julgamento da proposta

8.1.1 Trata-se da contratação de empresa especializada na prestação de serviços de antivírus e antimalware com tecnologia EDR (Detecção e Resposta de Endpoint), conforme especificações técnicas, com disponibilização de atualizações, manutenção e suporte técnico com o objetivo de proteger a infraestrutura de tecnologia da informação do órgão.

8.1.1.1 A solução será selecionada com base no critério de **menor preço global**, considerando que a segurança dos dados e a proteção contra ameaças cibernéticas são essenciais para a continuidade e integridade das atividades da Administração Pública.

8.1.2 Como critério de aceitabilidade a proposta apresentada, visto suas peculiaridades específicas, deverá ser o menor preço ofertado.

8.1.3 A escolha do critério fora desta forma definida objetivando-se o atendimento ao interesse público envolvido para a Administração Pública.

8.2 Regime de execução

8.2.1 A execução do presente contrato será pelo regime de execução indireta de empreitada por preço unitário.

8.2.2 O prestador dos serviços será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento MENOR PREÇO GLOBAL.

8.3 Exigências de Habilitação

8.3.1 Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

8.3.1.1 Qualificação Econômico-Financeira:

8.3.1.1.1 Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando;

8.3.1.1.2 Para avaliar a situação financeira do(s) proponente(s) deverá(ão) serem considerados os índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), conforme metodologia a ser detalhada no Edital, e conforme já praticado em outros editais no Município;

8.3.1.1.3 Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido, para fins de habilitação, capital social ou patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da contratação.

8.3.1.2 Qualificação Técnica:

8.3.1.2.1 A licitante deverá apresentar atestados de capacidade técnica, emitidos por pessoa jurídica de direito público ou privado, que comprovem a prestação de serviços de natureza e complexidade técnica similares às exigidas na contratação, com a comprovação de fornecimento de no mínimo 5.000 (cinco mil) licenças/ano;

8.3.1.2.2 Será aceito o somatório de atestados e/ou declarações para comprovar a capacidade técnica;

8.3.1.2.3 Serão aceitos atestados ou outros documentos hábeis emitidos por entidades estrangeiras quando acompanhados de tradução para o português, salvo se comprovada a inidoneidade da entidade emissora;

8.3.1.2.4 Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou filial da licitante;

8.4 Da participação de consórcio

8.4.1 Não será admitida a participação de empresas em consórcio.

8.4.1.1 Entende-se pela vedação da participação de empresas em consórcio, isso porque a formação de consórcio pode gerar risco de dominação de mercado e reduzir o universo da disputa. O consórcio, eventualmente, poderia gerar um acordo entre os interessados em vez da disputa de preços, fulminando com a competitividade que se espera de um procedimento licitatório. Assim, entende-se que a formação de consórcio tenderia a cercear as possibilidades de competição.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1 O custo estimado da contratação possui caráter sigiloso na fase preparatória, com vistas a garantir a lisura da pesquisa de mercado e será tornado público apenas quando da fase externa do procedimento.

9.2 A divulgação do valor pode comprometer a competitividade ao permitir que concorrentes ajustem suas propostas para se alinhar exatamente com o valor divulgado, em vez de oferecerem o melhor serviço pelo menor custo.

9.3 O valor estimado para contratação encontra-se previsto no Estudo Técnico Preliminar que compõe o processo de Requisição de Compras.

9.4 Foram utilizados os parâmetros indicados nos Incisos II e IV do § 1º, do art. 23 da Lei de Licitações n° 14.133/2021.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1 Os valores para a presente contratação estão em conformidade com a previsão orçamentária dos órgãos participantes.

10.2 A previsão dos recursos orçamentários para a contratação estão discriminados junto ao documento "Requisição de Compras" que faz parte do presente processo.

10.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária (LOA) respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11. DA ASSINATURA ELETRÔNICA

11.1 Considerando que assinatura dos instrumentos contratuais são realizados eletronicamente, mediante login e senha, deverão o(s) representante(s) legal(is) do(s) proponente(s) providenciar(em) a sua assinatura eletrônica, de acordo com Instrução Normativa n° 183/2023, regulamentada pelo Decreto Municipal nº 56.185/2023.

11.1.1 O(s) representante(s) legal(is) do(s) interessado(s) em participar da licitação poderá(ão) providenciar seu cadastro, com autenticação de conta através do login único "gov.br" para liberação da assinatura eletrônica, de acordo com o que estabelece a carta de serviços disponível no seguinte link: https://www.joinville.sc.gov.br/servicos/acessar-portal-de-autosservico/

11.2 - Após declarado vencedor o(s) representante(s) legal(is) do(s) proponente(s) deverá(ão) estar com o seu usuário externo certificado para efetuar a assinatura eletrônica, nos termos do Decreto nº 56.185/2023, sob pena de decair do direito de assinar o Contrato e/ou eventuais alterações, sem prejuízo das sanções previstas no edital.

11.2.1 É de responsabilidade exclusiva do(s) representante(s) legal(is) do(s) proponente(s)/interessado(s) a criação de seu cadastro com autenticação de conta através do login único "gov.br" para liberação da assinatura eletrônica.

Documento assinado eletronicamente por **Anna Paula Pinheiro**, **Diretor (a) Executivo (a)**, em 03/12/2025, às 09:49, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Rodrigo Ponick**, **Gerente**, em 03/12/2025, às 09:55, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Grasiele Wandersee Philippe**, **Coordenador(a)**, em 03/12/2025, às 09:58, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Alessandro de Cassio Silva**, **Servidor(a) Público(a)**, em 03/12/2025, às 10:06, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

A autenticidade do documento pode ser conferida no site https://portalsei.joinville.sc.gov.br/ informando o código verificador **27711528** e o código CRC **15AAE426**.

ANEXO SEI Nº 27660850/2025 - SAP.UGC

ANEXO I
ESPECIFICAÇÕES TÉCNICAS

1. REQUISITOS MÍNIMOS GERAIS

1.1 As licenças e os serviços que compõem a solução de segurança de endpoint (Antivírus/EDR) da CONTRATADA deverão atender integralmente aos requisitos mínimos desta especificação técnica, incluindo todas as funcionalidades e módulos necessários, sem a necessidade de aquisições complementares posteriores.

1.2 O fornecimento das licenças está associado à sua completa implantação, configuração da plataforma central de gerenciamento e repasse de conhecimento/treinamento à equipe técnica da CONTRATANTE.

1.3 A CONTRATADA proponente deverá apresentar um comprovante de sua posição no relatório Gartner® Magic Quadrant™ ou Forrester Wave™ para a categoria de "Endpoint Protection Platforms (EPP)" ou "Endpoint Detection and Response (EDR)" do ano mais recente disponível.

1.4 O proponente deve fornecer documentação (preferencialmente de testes públicos e independentes como o MITRE ATT&CK Evaluations) que demonstra uma cobertura de detecção em técnicas críticas (como Evasão de Defesa e Elevação de Privilégios) acima de 95%.

1.5 A Solução deverá ser fornecida pela CONTRATADA como um produto comercial e pronto para uso (Off-the-shelf), incluindo todas as funcionalidades, módulos e documentação prometidas na proposta. Não será aceito qualquer procedimento que configure o desenvolvimento de novas funcionalidades ou módulos no código-fonte da solução após a contratação. Contudo, esta regra não se aplica ao trabalho contínuo e necessário de Inteligência de Segurança Adaptativa, que inclui:

1.5.1 Customização de Regras: Otimização, criação e ajuste de regras de Detecção e Resposta (EDR), como regras de Hunting ou de monitoramento de eventos específicos, para adequação ao ambiente da CONTRATANTE.

1.5.2 Criação de Assinaturas/Vacinas: Criação de assinaturas HIPS ou vacinas personalizadas para proteção contra ameaças Zero Day ou Malwares específicos do ambiente.

1.5.3 Ajustes de Políticas: Configuração de políticas e perfis de segurança para balancear a performance e a eficácia, conforme a necessidade de customização para o novo ambiente.
A customização dessas regras de inteligência e políticas de segurança é inerente ao serviço e deve ser executada pela CONTRATADA sem que isso configure "desenvolvimento de solução".

1.6 A CONTRATADA deverá manter a CONTRATANTE imediatamente informada sobre quaisquer alterações nos endereços IP e Nomes DNS (Fully Qualified Domain Names - FQDN) dos servidores utilizados para atualizações de definições (vacinas). Esta comunicação deverá ser realizada com antecedência mínima de 5 (cinco) dias úteis, sempre que aplicável, ou imediatamente em casos de mudanças emergenciais, a fim de permitir o ajuste nas regras de firewall da prefeitura e garantir a continuidade do serviço.

2. COMPONENTES DA SOLUÇÃO

2.1 Os componentes da solução, bem como os quantitativos, estão definidos no Estudo Técnico Preliminar e no Termo de Referência;

2.2 Todos os itens propostos para aquisição por meio desta contratação, deverão ser ofertados por um único fornecedor, pertencentes a um único fabricante ou marca. Esta exigência tem por objetivo promover a adequada integração entre os equipamentos e softwares, gerenciamento e funcionalidade do projeto.

2.3 Não serão aceitas licenças, versões de software ou soluções de segurança que já estejam em fases de descontinuação, sem suporte ou fim de vida útil (*end-of-sale, end-of-support, end-of-life*) pelo Fabricante na data da Proposta e durante toda a vigência do contrato. Caso, no momento da Proposta, Entrega ou durante a execução contratual, a solução ou suas versões se enquadrem nessas categorias, a CONTRATADA deverá providenciar, sem custos adicionais para a CONTRATANTE, a imediata substituição por uma versão ou solução equivalente ou superior, mediante aprovação prévia da equipe técnica de TI da CONTRATANTE.

2.4 Se qualquer solução fornecida tiver seu suporte encerrado após a ativação, deverá ser substituído por um equivalente ou superior, sem custo para a CONTRATANTE, com até 90 (noventa) dias de antecedência da data do fim do suporte.

2.5 A solução fornecida deve ser totalmente compatível com a infraestrutura existente da CONTRATANTE, garantindo a integração de protocolos, configurações, plataformas e outras funcionalidades necessárias para o funcionamento em conjunto.

2.6 Nenhuma instalação ou configuração poderá exigir aquisições ou adaptações extras que não estejam previstas nesta contratação.

2.7 Não serão aceitas soluções baseadas em software de código aberto (*open source*) genérico ou em sistemas operacionais e softwares que não sejam os padrões oferecidos pelo FABRICANTE para o mercado em geral.

2.8 O uso de fontes abertas, como consultas de inteligência, CVEs, entre outros, não possui relação com este item.

3. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

3.1 REQUISITOS GERAIS

3.1.1 A solução de segurança Antivírus/EDR deve ser provida, obrigatoriamente, de um Console de Gerenciamento Centralizado com instalação em ambiente On-Premise (instalado na infraestrutura física ou virtual da CONTRATANTE).

3.1.1.1 O Console de Gerenciamento deve permitir a administração completa da arquitetura central, incluindo o deployment, a aplicação de políticas, e a coleta de logs dos endpoints em modo exclusivamente on-premises, sem a necessidade de serviços externos de nuvem para seu funcionamento administrativo básico. A dependência de serviços de nuvem para a Inteligência de Ameaças Global (ex: reputação de hash, atualização de vacinas, cloud sandboxing e telemetria avançada) é permitida, desde que a solução mantenha a capacidade de proteção offline e o gerenciamento fundamental seja local..

3.1.1.2 A CONTRATADA deve informar todos os requisitos de hardware e software para a instalação do Console, de maneira à comportar a infraestrutura da CONTRATANTE.

3.1.1.3 A solução deve possibilitar a atualização das bases de dados (vacinas) e engines de segurança para os endpoints diretamente a partir do Console On-Premise, permitindo que máquinas internas se atualizem sem consumir a banda de internet, preferencialmente com o uso de proxies para balanceamento das atualizações.

3.1.1.4 O console deve suportar a integração com o serviço de diretório local da CONTRATANTE (Microsoft Active Directory) para facilitar a implantação, distribuição de agentes e gerenciamento de usuários e grupos.

3.1.1.5 A solução deve oferecer recurso para criação de grupos e subgrupos de máquinas baseado na hierarquia do Active Directory e LDAP e em identificador único de clientes, tal como endereço IP;

3.1.1.6 A CONTRATADA deverá garantir que a equipe técnica da CONTRATANTE tenha Controle Total e Irrestrito sobre o console de gerenciamento centralizado da solução (EPP/EDR) instalado no ambiente on-premise.

3.1.2 A solução de Antivírus deverá gerenciar os agentes nas estações e servidores a partir de um ponto único (Console Central de Gerenciamento), permitindo deste ponto a instalação, administração, monitoramento, atualização e configuração, geração de relatórios, seja de um servidor específico ou de um grupo de servidores ou estações de trabalho, com todos os módulos de um único fornecedor.

3.1.3 O acesso ao Console de Gerenciamento deve ser efetuado via tecnologia Web segura (HTTPS) compatível com os navegadores padrão de mercado em suas últimas versões. Não serão considerados acessos do tipo RDP, VNC, ICA, dentre outras soluções de emulação;

3.1.4 O acesso ao Console deve suportar várias sessões simultâneas.

3.1.5 A solução deverá garantir a aplicação imediata de mudanças de configuração e atualizações de políticas (por exemplo, bloqueios de hash ou ações de resposta EDR) nos agentes. Isso deve ser feito através de um canal de comunicação proprietário que permita a execução de comandos e a aplicação de alterações em tempo real (real-time) e de forma síncrona com o Console de Gerenciamento.

3.1.6 Permitir o agrupamento dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio.

3.1.7 O servidor de gerenciamento deve possuir compatibilidade para instalação nos seguintes sistemas operacionais em todas as versões/distribuições/releases e Hypervisors, em arquitetura x64:

3.1.7.1 Microsoft Windows 10 e versões posteriores;

3.1.7.2 Microsoft Windows Server 2019 e versões posteriores;

3.1.7.3 Debian 11 e versões posteriores;

3.1.7.4 VMware vSphere/ESXi 6.5 e versões posteriores;

3.1.8 Possibilidade de aplicar regras diferenciadas baseando-se na localidade lógica da rede.

3.1.9 Possibilidade de criar grupos separando as regras aplicadas a cada dispositivo.

3.1.10 Possibilidade de instalação dos clientes em estações de trabalho e servidores, podendo estes ser físicos ou virtualizados, via console de gerenciamento, de forma remota, sem intervenção do usuário (modo silencioso). Não será considerado como instalação remota acesso a máquina do usuário usando recursos de terceiros como: vnc, remote desktop, etc.

3.1.11 Caso a solução ofertada pela CONTRATADA não seja da marca Kaspersky (atual solução instalada na Administração Pública Municipal), o produto deverá contemplar funcionalidades para remoção automática do produto da Kaspersky, na versão instalada atualmente de maneira silenciosa, através de login script e sem a necessidade de instalar qualquer software adicional na estação de trabalho;

3.1.12 Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota.

3.1.13 A console de gerenciamento deve apresentar funcionalidade que impeça o usuário de acessar as configurações do cliente gerenciado de modo que não se possa alterar, importar e exportar configurações, abrir a console do cliente, desinstalar ou parar o serviço do cliente.

3.1.14 A console de gerenciamento deve possuir capacidade de criação de contas de usuário com diferentes perfis de acesso (minimamente os níveis de operador e administrador).

3.1.15 A solução deve incorporar RBAC (Role-Based Access Control), permitindo a definição de acessos customizados e granulares para usuários adicionais no console. Essa granularidade deve segregar e limitar acessos a políticas, tarefas e outros objetos do console.

3.1.16 A console de gerenciamento deve possuir log centralizado e conter, no mínimo, as seguintes informações:

a) Nome da ameaça;

b) Nome do arquivo infectado;

c) Caminho da detecção;

d) HASH do arquivo;

e) Data e hora da infecção;

f) Ação tomada;

g) Endereço de IP da máquina;

h) Usuário autenticado na máquina;

i) Origem da ameaça (IP ou hostname da máquina) caso a ameaça tenha se propagado;

3.1.17 A console de gerenciamento deve fornecer, em tempo real, o status atualizado das estações de trabalho, com pelo menos as seguintes informações:

a) Nome da máquina;

b) Endereço IP da máquina;

c) Malwares não removidos;

d) Status da conexão;

e) Data da vacina;

f) Versão do antivírus instalado.

3.1.18 O console de gerenciamento deve prover alertas de segurança via e-mail, com informações de infecção de máquinas e ataques. Suportando no mínimo alertas dos seguintes módulos:

a) Detecção e respostas de Malware;

b) Detecção e respostas de Firewall;

c) Detecções e respostas via EDR;

3.1.19 O console de gerenciamento deve utilizar comunicação criptografada, utilizando de SSL, entre console de gerenciamento e o cliente gerenciado.

3.1.20 Possibilidade de criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento e site do fabricante.

3.1.21 Capacidade de voltar (rollback) para versão de atualização anterior (da solução ou vacina) mediante procedimento específico no console de gerenciamento.

3.1.22 A interface do console de gerenciamento deve ser totalmente em português do Brasil.

3.1.23 O acesso ao console de administração do antivírus deve ter a possibilidade de ser feito com duplo fator de autenticação, configurado dentro do console, onde seja possível ativá-lo sem a necessidade de nenhum add-on.

3.1.24 Deve gerar pacotes de instalação dos clientes, para cada tipo de sistema operacional existente na estrutura da CONTRATANTE, possibilitando a gravação em mídia e a instalação do software em ambientes onde não seja possível a instalação via rede corporativa.

3.1.25 Permitir forçar a instalação do software cliente do antivírus nos computadores, reinstalando em caso de desinstalação ou corrupção do mesmo.

3.1.26 Suportar o gerenciamento de todos os clientes instalados nas máquinas (estações de trabalho, servidores, tablets e smartphones) a partir do servidor do Console de Gerenciamento, oferecendo a possibilidade de configuração centralizada e remota de todas as funcionalidades.

3.1.27 Gerenciar de forma remota as configurações do firewall local de cada máquina com o cliente instalado.

3.1.28 A solução deve oferecer recurso para isolar as máquinas da rede, mantendo apenas comunicação segura com o servidor de gerenciamento.

3.1.29 A solução deve permitir a criação de exceções para o isolamento de rede, permitindo que a solução mantenha comunicação com alguns endereços de IP durante o isolamento.

3.1.30 A solução deve permitir forçar a configuração determinada no servidor para os clientes, protegendo o software cliente de alterações pelos usuários, com senha pré-determinada no console de gerenciamento.

3.1.31 Atualização/sincronização de configurações nos clientes sem a necessidade de reinicialização ou logoff.

3.1.32 A solução deve permitir a criação de tarefas de rastreamento de malwares em períodos pré-determinados e na inicialização do sistema operacional.

3.1.33 Permitir a criação de tarefas de atualização de vacinas e novas versões de software em períodos pré-determinados.

3.1.34 A solução deve possuir ferramentas próprias para centralizar e distribuir atualizações de software e atualizações dos módulos, não será aceito o uso de ferramentas de terceiros;

3.1.35 A solução deve permitir criação das tarefas para uma máquina, um grupo de máquinas e/ou para todas as máquinas.

3.1.36 No console de gerenciamento, a solução deve permitir a criação de relatórios customizados. Não serão aceitos apenas os relatórios pré-configurados da solução.

3.1.37 A solução deve permitir a geração de relatórios, permitindo a customização dos mesmos e a exportação para, pelo menos, os seguintes formatos:

a) CSV;

b) PDF;

3.1.38 A solução deve permitir a geração de relatórios que contenham as seguintes informações:

a) Máquinas com a lista de definições de vírus desatualizada, bem como de todas as máquinas e suas respectivas versões da lista de definições de vírus;

b) Versão do software de proteção instalado em cada máquina;

c) Vírus que mais foram detectados;

d) Máquinas que mais sofreram infecções em um determinado período;

3.1.39 A solução deve permitir o armazenamento em um banco de dados centralizado das informações coletadas nos clientes, sendo no mínimo:

a) Registro de eventos (log);

b) Relatórios de eventos de vírus e status dos clientes;

c) Relatórios de todos os softwares instalados;

d) Relatórios de todos os componentes de hardware encontrados;

e) Relatórios de licenças e seus quantitativos;

3.1.40 A solução deve ter a capacidade de enviar eventos para um servidor SIEM ou Syslog, suportando no mínimo os seguintes formatos:

a) JSON;

b) LEEF;

c) CEF;

3.1.41 A solução deve fornecer, em tempo real, o status atualizado da solução de proteção nas estações de trabalho e servidores;

3.1.42 A solução deve possibilitar a exportação, em formato PDF e CSV, de relatórios que atuem com inventário de hardware e software de todas as estações e servidores ativos na estrutura da console de gerenciamento.

3.1.43 A solução deve permitir a instalação remota do agente e produto de segurança por meio de GPO.

3.1.44 Possuir módulo de gerenciamento de dispositivos móveis Android e iOS.

3.1.45 Possibilitar a instalação da solução de segurança nos dispositivos móveis de maneira manual via QR code, link gerado pela solução de gerenciamento e envio por e-mail

3.1.46 Através da console de gerenciamento a solução deve possibilitar a ativação da opção de bloqueio de exploit nas estações e servidores.

3.1.47 Deverá permitir atualizar o Pacote de Vacinas do servidor central da solução, de forma automática, através da internet, sem que haja intervenção técnica, e, distribuir, também de forma automática, a partir do servidor central, as estações de trabalho e servidores clientes. Não serão admitidas replicações com base em scripts ou replicações feitas usando artifícios técnicos não homologados e amplamente documentados pelo fabricante da solução através dos manuais técnicos ou ainda usando softwares de terceiros.

3.1.48 Atualização em clientes móveis (notebook, laptop, netbook, ultrabook e similares) a partir do site do fabricante da solução.

3.1.49 Capacidade de configurar políticas móveis para quando um computador estiver fora da estrutura de proteção, possa atualizar-se via internet.

3.1.50 A solução deve oferecer a possibilidade de eleição de qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função.

3.1.51 Qualquer atualização de vacinas deve ser possível sem a necessidade de reinicialização do computador ou serviço para aplicá-la.

3.1.52 Deverá permitir a atualização de forma automática através de serviço de Proxy permitindo a configuração de usuário e senha para autenticação no sistema de internet.

3.1.53 Deverá ser possível definir políticas de bloqueio às funções de configuração do software em servidores remotos.

3.1.54 A solução deverá contemplar ferramentas que fazem varreduras periódicas na rede a fim de localizar máquinas que, possivelmente, não estejam com o cliente do antivírus instalado no equipamento.

3.2 CARACTERÍSTICAS DA SOLUÇÃO DE DETECÇÃO E RESPOSTA

3.2.1 A solução deve fornecer prevenção de ameaças, visibilidade e resposta a incidentes.

3.2.2 A solução de detecção e resposta deverá atender sistemas operacionais Windows, Linux e macOS.

3.2.3 A solução deve permitir a identificação de comportamentos anômalos dentro da rede.

3.2.4 A solução deve fornecer informações para poder conduzir investigações e tomar ações corretivas.

3.2.5 A solução deve oferecer minimamente as seguintes informações de apoio para as investigações: explicação técnica do comportamento detectado, possíveis causas maliciosas e benignas e ações recomendadas.

3.2.6 A solução deve possuir recurso de gráfico de investigação para a investigação de incidentes, permitindo que o administrador identifique a correlação de eventos detectados durante o incidente.

3.2.7 O gráfico de investigação da solução deve ser interativo, não fornecendo apenas uma imagem estática dos eventos, mas sim, permitindo a interação do administrador com cada evento detectado, facilitando a investigação do incidente.

3.2.8 As consoles de gerência das soluções EPP e EDR devem ser integradas.

3.2.9 A solução de EDR deverá ser completamente integrada com a solução de segurança de Endpoint para trabalhar de forma conjunta a fim de conter os incidentes de segurança.

3.2.10 A solução de EDR deve possuir a capacidade de filtrar os incidentes, executáveis e scripts para realizar uma varredura mais detalhada dos possíveis incidentes de segurança.

3.2.11 A solução deve permitir a detecção de incidentes com base em indicadores de ataques (IoA), e não somente com base em indicadores de comprometimento (IoC).

3.2.12 A solução deve possuir recurso para realização de busca de indicadores de comprometimento (IOCs).

3.2.13 A solução deve possuir modelos pré-definidos para a busca de IOCs, contendo, pelo menos, os seguintes parâmetros:

a) Detecções;

b) Computadores;

c) Eventos;

d) Executáveis;

e) Processos;

f) Scripts;

3.2.14 Além dos modelos pré-definidos para a busca de IOCs, a solução deve oferecer recurso avançado para realização da busca, utilizando o formato XML.

3.2.15 A solução deve oferecer recursos de Threat Hunting (caça a ameaças), permitindo encontrar, de forma proativa, potenciais ameaças cibernéticas.

3.2.16 A solução deve contar com regras pré-definidas agrupadas por categorias.

3.2.17 A solução deve permitir criar regras próprias de monitoramento.

3.2.18 A solução deve permitir que as regras pré-definidas sejam revertidas para a configuração padrão, revertendo quaisquer alterações feitas pelo administrador da solução.

3.2.19 A solução deve poder identificar indicadores de comprometimento.

3.2.20 Os indicadores de comprometimento da solução de EDR devem estar no formato XML.

3.2.21 Os indicadores de comprometimento da solução de EDR devem combinar comportamento e reputação.

3.2.22 A solução de EDR deve ter a capacidade de detectar ataques do tipo “file-less” característica essa de ataques sem arquivos executáveis.

3.2.23 A solução deve permitir o envio de artefatos ao ambiente de Sandbox, diretamente através do painel de investigação de incidentes.

3.2.24 A solução de EDR deverá permitir modificação dos indicadores de comprometimento conforme a necessidade da CONTRATANTE.

3.2.25 A solução deve permitir visualizar e bloquear módulos com base em múltiplos indicadores, incluindo valor de hash, alterações de registro, alterações de arquivo e conexões de rede.

3.2.26 A solução deve bloquear a execução de módulos maliciosos em todos os computadores da sua rede corporativa.

3.2.27 A solução deve apresentar informações detalhadas sobre os módulos que acabaram de ser executados, incluindo o tempo de execução, o usuário que a executou, o tempo de espera e os dispositivos atacados.

3.2.28 A solução deve permitir o bloqueio da execução de aplicativos não autorizados.

3.2.29 A solução deve permitir a inclusão de hashes em lista de bloqueio preventiva, suportando, pelo menos, os formatos SHA-1 e SHA-256.

3.2.30 A solução deve proporcionar visibilidade total da detecção, e oferecer recursos para realizar a análise de causa raiz do ataque, exibindo a árvore completa de processos, para qualquer cadeia de eventos potencialmente suspeitos.

3.2.31 A solução deve permitir a investigação detalhada dos executáveis incluindo a origem do arquivo, o processo que o arquivo disparou, modificações de registro, conexões de rede.

3.2.32 A solução deve permitir adicionar e remover tags para filtrar objetos mais rapidamente, como computadores, alertas, exclusões, tarefas, executáveis, processos e scripts.

3.2.33 A solução deve mostrar a reputação das ações realizadas por algum executável.

3.2.34 A solução deve oferecer recurso para isolar as máquinas da rede, mantendo apenas comunicação segura com o servidor de gerenciamento.

3.2.35 A solução deve oferecer recurso de acesso remoto via PowerShell em dispositivos Windows, para facilitar o processo de resposta a incidentes.

3.2.36 A solução deverá permitir a exclusão de detecções, combinando diferentes critérios por nome de arquivo.

3.2.37 A solução de EDR deverá mostrar os alertas tanto no console de administração do mecanismo de segurança de Endpoint como em sua interface própria de administração.

3.2.38 A solução deve permitir a priorização da gravidade do alerta por meio de funcionalidade de pontuação, que atribui um valor de gravidade aos eventos e permite que os administradores identifiquem facilmente os computadores com maior risco de um possível incidente.

3.2.39 Acesso a MDR (Managed Detection and Response): A solução deve ser compatível com a contratação de serviços de MDR/SOC do fornecedor ou de terceiros, garantindo a capacidade de envio de logs e telemetria para análise 24/7/365, caso o órgão opte por terceirizar o serviço de Threat Hunting/Incident Response futuramente.

3.2.40 A solução de EDR deve permitir a execução de indicadores de comprometimento em dados modificados, bem como em dados históricos.

3.2.41 Deve mostrar o ID da TÉCNICA MITRE ATT&CK ™ em cada detecção gerada pela solução, bem como fornecer o link direto para acesso à página da técnica correspondente.

3.2.42 Deve ter a capacidade de obter uma análise profunda de detalhes da configuração de cada computador.

3.2.43 A ferramenta deve contar com uma API pública para permitir a integração com ferramentas de terceiros (Ex: SOAR, sistemas de tickets, entre outras).

3.2.44 Deve ter a capacidade de enviar eventos para um servidor SIEM.

3.2.45 Deve oferecer recursos para obter a reputação de hashes através do VirusTotal.

3.2.46 Além do VirusTotal, a solução também deve permitir a integração com outras ferramentas de análise de malware para o envio de hashes.

3.2.47 O agente deve utilizar tecnologias avançadas, como a AMSI (para monitoramento de scripts em PowerShell e VBScript) e inspeção de processos na memória (memory introspection), para neutralizar ameaças antes que elas se manifestem.

3.2.48 Gerenciamento de Vulnerabilidades e Patches (VPM): A solução deve incluir ou se integrar nativamente a um módulo de VPM para detecção, priorização e orquestração de aplicação de patches em sistemas operacionais e aplicativos de terceiros, conforme exigido pelos controles de Prevenção e Proteção (NIST).

3.2.49 Gestão de Desvios de Postura (Configuration Drift): O console deve monitorar e alertar automaticamente sobre desvios críticos nas configurações de segurança dos endpoints (ex: firewall desabilitado, proteções desativadas, alteração de GPOs de segurança) em relação à política base.

3.2.50 Suporte a Arquitetura Zero Trust (ZTA): A solução deve oferecer capacidades nativas de:

a) micro-segmentação de rede baseada em identidade do endpoint; e

b) integração com soluções de Zero Trust Network Access (ZTNA) ou NAC para isolamento e controle de acesso dinâmico.

3.2.51 Risk Scoring (Pontuação de Risco): A solução deve gerar uma pontuação de risco (Risk Score) por endpoint e por usuário, agregando dados de ameaças ativas, vulnerabilidades e desvios de postura de segurança, para facilitar a priorização de incidentes e a gestão de riscos.

4. SOLUÇÃO PARA ESTAÇÕES DE TRABALHO, SERVIDORES E DISPOSITIVOS MÓVEIS

4.1 REQUISITOS GERAIS

4.1.1 A solução ofertada deve suportar sistemas operacionais com arquitetura 32-bits e 64-bits.

4.1.2 Deve ser gerenciado via console de gerenciamento centralizado.

4.1.3 Interface do software cliente deve ser fornecido em português do Brasil.

4.1.4 Os manuais da solução devem ser fornecidos em português do Brasil.

4.1.5 O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade para instalação e desinstalação com os seguintes sistemas operacionais, minimamente, nas seguintes versões:

a) Microsoft Windows 10 e versões posteriores;

b) Microsoft Windows Server 2019 (Server Core e Desktop Experience) e versões posteriores;

c) Debian 11 e versões posteriores;

d) MacOS 11 e versões posteriores;

e) Android 6 e versões posteriores;

f) iOS 9 e versões posteriores;

g) iPadOS 13 e versões posteriores.

4.1.6 Deverá permitir a auto-detecção do sistema operacional para instalação da Solução de Antivírus nas estações de trabalho. Não serão admitidas as soluções que necessitem gerar um pacote de instalação específico para cada versão do Windows.

4.1.7 Deverá permitir instalação e atualização automáticas através de login script Internet/Intranet, unidade de armazenamento removível e através de instalação remota em estações conforme item 4.1.5.

4.1.8 Deverá permitir e estar apto a realizar configuração diferenciada para cada estação de trabalho, grupo de estações, domínio ou grupos de domínios.

4.1.9 Deverá permitir gerar notificações customizáveis para o usuário em caso de detecção de vírus.

4.1.10 Deverá permitir exportar o log para o formato Texto e/ou CSV.

4.1.11 Deverá possuir ferramenta integrada que permita seu uso de forma automatizada para reparação de danos causados por vírus do tipo “Trojans”, sem a necessidade de uma ferramenta externa.

4.1.12 Deverá permitir agendar uma verificação na comunicação entre o servidor e as estações.

4.1.13 Deve otimizar as atualizações por meio de distribuição de carga (caching/peer-to-peer) em locais com baixa velocidade de comunicação com o servidor principal..

4.1.14 Deverá permitir armazenamento de log de ocorrência de vírus local e no servidor.

4.1.15 A lista contendo os sites maliciosos deverá ser atualizada diariamente e automaticamente pela CONTRATADA juntamente com o Pacote de Vacinas.

4.1.16 Deverá permitir ações automática em caso de detecção de código malicioso, armazenando uma cópia do arquivo em quarentena antes da desinfecção;

4.1.17 A solução deverá rastrear em tempo real arquivos durante entrada e saída (gravação e leitura) no equipamento. Durante o rastreamento deverá limpar, apagar ou isolar o arquivo infectado conforme a política definida pelo administrador da Solução de Antivírus.

4.1.18 Deverá permitir ao administrador bloquear os serviços de compartilhamento quando alvo de códigos maliciosos, no momento de uma epidemia, e, após o término desta, restaurar as configurações originais.

4.1.19 Deverá ser possível instalar, também de forma silenciosa, a Solução de Antivírus nas estações de trabalho através de scripts durante o Login na rede.

4.1.20 O cliente deve ter a capacidade de continuar operando, mesmo quando o servidor de gerenciamento não puder ser alcançado pela rede.

4.1.21 O cliente deve ter a capacidade de atualizar a versão do agente através do servidor de gerenciamento.

4.1.22 Quando o servidor de gerenciamento estiver inoperante ou o agente estiver incapaz de comunicar-se com o servidor por razões distintas, o agente deve ser capaz de atualizar vacinas e componentes mediante comunicação com o site do fabricante.

4.1.23 A solução deve possuir recursos para criação de planos de distribuição das atualizações via comunicação segura entre clientes e servidor de gerenciamento.

4.1.24 Deverá permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para todas as estações, para um grupo ou estações específicas.

4.1.25 O cliente gerenciado deve implementar funcionalidade em que as configurações, alteração, desinstalação, desativação do serviço, importação e exportação de configurações possam ser bloqueadas por senha, através do console de modo a evitar que o usuário da estação de trabalho interfira no funcionamento da solução.

4.1.26 Atualização de configurações, sem interação (em background) nos clientes, sem a necessidade de reinicialização ou logoff.

4.1.27 Capacidade de bloquear ameaças que exploram a ausência de correções do Sistema Operacional (patches) fazendo com que as ameaças que se utilizam de vulnerabilidades sejam bloqueadas enquanto a correção oficial não esteja instalada/disponível corretamente, através de análise heurística ou outras de melhor efetividade e/ou somadas a essa;

4.1.28 Caso a solução encontre algum arquivo mal-intencionado (tais como ameaça dia-zero, ameaça persistente), deve possuir capacidade de análise e posterior bloqueio automático.

4.1.29 A função de Escaneamento de vírus deverá ter a possibilidade de configuração de exceções:

a) Excluir da verificação tipos de arquivos tais como .TXT (arquivo de texto simples).

b) Pastas e arquivos pré-determinados através do caminho, bem como hash.

4.1.30 Deve permitir a instalação e desinstalação da solução de proteção remotamente, através do console de gerenciamento centralizado.

4.1.31 Possibilidade de instalação presencial por meio de mídia de instalação fornecida ou gerada através do servidor de antivírus.

4.1.32 Programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, com frequência (no mínimo a cada hora) e horários definidos no console de gerenciamento centralizado:

a)Permitir atualização incremental da lista de definições de vírus;

b)Permitir atualização por endereço do próprio fabricante, como opção além do servidor local;

c)Permitir configuração remota de ordem de preferência de endereços de atualização;

d)Permitir configurar conexão do endpoint com o servidor de gerenciamento por meio de serviço de proxy local;

e)Permitir a atualização da lista de arquivos a serem verificados contra vírus através da lista de definições de vírus;

4.1.33 No sistema operacional Linux, além de proteger e rastrear seus sistemas de arquivos, deve proteger também os arquivos armazenados em compartilhamentos SAMBA/CIFS e os arquivos que de alguma forma estejam disponibilizados para o acesso de clientes Windows em um servidor Linux.

4.1.34 Deve ser capaz de detectar e remover todos os tipos de malwares, incluindo vírus, ransomware, worm, trojan, spyware, rootkit, vírus de macro e códigos maliciosos.

4.1.35 Possuir mecanismo de detecção baseado em ferramentas de análise e detecção como:

a) Machine Learning

b) Instrusion Prevention System

4.1.36 Rastreamento em tempo real para vírus de macro e arquivos criados, copiados, renomeados, movidos ou modificados, inclusive em sessões DOS abertas pelo Windows.

4.1.37 Possuir módulo de proteção em tempo real do sistema de arquivos, o qual deve controlar todos os arquivos no sistema a fim de detectar código malicioso quando os arquivos são abertos, criados ou executados.

4.1.38 Possuir módulo de detecção proativa que forneça proteção contra uma nova ameaça durante a propagação inicial.

4.1.39 A solução deve possuir módulo dedicado para detecção e proteção contra variantes de ransomware globalmente conhecidas, a fim de atuar como um escudo contra este tipo de ameaça.

4.1.40 O módulo dedicado para detecção e proteção contra variantes de ransomware deve contar com recurso de remediação (rollback), permitindo que possíveis arquivos criptografados durante o processo de detecção sejam restaurados ao seu estado original.

4.1.41 O recurso de remediação (rollback) do módulo dedicado para detecção e proteção contra variantes de ransomware deve ser baseado exclusivamente em um motor de Machine Learning, visando melhorar a eficácia do processo de restauração. Não serão aceitas soluções que utilizam apenas o mecanismo Volume Shadow Copy Service (VSS), da Microsoft.

4.1.42 A solução deve ser capaz de fazer a varredura em um estado ocioso para fornecer proteção proativa enquanto o equipamento não está em uso

4.1.43 Deve permitir diferentes configurações de varredura em tempo real, tornando o produto mais performático, principalmente em máquinas com baixo desempenho de hardware.

4.1.44 Deve efetuar o rastreamento em tempo real dos processos em memória, para a captura de vírus executados em memória sem a necessidade de escrita de arquivo.

4.1.45 Deve efetuar a detecção em tempo real e limpeza de programas maliciosos como spywares, ransomware, adwares, jokes, discadores, ferramentas de administração remota e programas quebradores de senha, realizando a remoção desses programas e a restauração de áreas do sistema danificados pelos mesmos, com possibilidade de criar uma lista de exclusão dos programas não desejados, onde a administração seja centralizada pela mesma console de gerenciamento do antivírus.

4.1.46 Deve efetuar o rastreamento manual com interface gráfica, customizável, com opção de limpeza.

4.1.47 Deve efetuar o rastreamento por linha de comando, parametrizável, com opção de limpeza.

4.1.48 Deve permitir a programação de rastreamentos de malwares automaticamente com as seguintes opções:

a) Escopo: todos os drives locais, drives específicos, bem como pastas específicas;

b) Ação: somente alertas, limpar automaticamente, apagar automaticamente ou mover automaticamente para área de segurança;

c) Frequência: diária, semanal e mensal;

d) Exclusões: pastas e arquivos que não devem ser rastreados;

4.1.49 Possuir área de segurança (quarentena) no computador no qual o cliente estiver executando a proteção.

4.1.50 Detecção de anomalias através dos métodos de assinatura, heurística e por comportamento.

4.1.51 Proteção contra ameaças via internet. A solução deve conter pelo menos:

a)Ajuste no nível de sensibilidade da detecção;

b)Lista de exceção.

4.1.52 Detecção em tempo real e possibilidade de bloqueio e remoção de malwares provenientes de downloads realizados no ambiente web.

4.1.53 Permitir que a funcionalidade de rastreamento em tempo real na navegação possa ser desabilitada pelo administrador;

4.1.54 Detecção em tempo real e possibilidade de bloqueio e remoção de malwares no conteúdo e anexos de mensagens de correio eletrônico, pelo antivírus cliente, analisando tráfego e suportando principais clientes.

4.1.55 Permitir que a funcionalidade de rastreamento em tempo real de e-mail possa ser desabilitada pelo administrador.

4.1.56 A solução deve oferecer recurso de controle de dispositivos, tendo a capacidade de controlar, minimamente, os seguintes dispositivos:

a) Pendrive;

b) HD externo;

c) Celulares;

d) Tablets;

e) CD/DVD;

f) Impressora USB;

g) Armazenamento de FireWire;

h) Dispositivo Bluetooth;

i) Leitor de cartão inteligente;

j) Dispositivo de criação de imagem;

k) Modem;

l) Porta LPT/COM;

m) Dispositivo portátil;

4.1.57 O módulo de controle de dispositivos deve estar disponível para estações de trabalho Windows, macOS e Linux, assim como para os servidores suportados.

4.1.58 Ferramenta de firewall bidirecional local no cliente, com possibilidade de configuração, ativação e desativação através da console de gerenciamento centralizada, contendo filtros especificados por aplicação, protocolo, IP, range de IPs, rede, porta e range de portas.

4.1.59 O módulo de firewall local da solução de proteção deverá tratar tráfego de entrada e de saída de forma independente.

4.1.60 A solução deve permitir bloquear a conexão de dispositivos removíveis.

4.1.61 A solução deve gerar registro (log) dos eventos de vírus em arquivo.

4.1.62 A solução deve gerar relatórios, ao menos, de:

a) Eventos de vírus;

b) Status da proteção nos clientes;

c) Status dos updates da proteção;

4.1.63 Gerar notificações de eventos de vírus através de alerta por e-mail, ao menos.

4.1.64 Gerar relatórios incluindo tipos de vírus, nome do vírus e se precisa de atualização do Sistema Operacional.

4.1.65 Possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras interfaces, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total.

4.1.66 Permitir a criação de exceções nos escaneamentos de arquivos.

4.1.67 Permitir o bloqueio de dispositivos com base nos seguintes critérios, minimamente:

a) Fabricante;

b) Modelo;

c) Número de série;

4.1.68 Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URLs acessadas.

4.1.69 A solução deve permitir a configuração de quais portas HTTPs serão escaneadas para verificação de conexões criptografadas.

4.1.70 O Firewall deve oferecer suporte aos protocolos TCP e UDP.

4.1.71 O Firewall deve reconhecer o tráfego DNS, DHCP e WINS com opção de bloqueio.

4.1.72 Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan, Spoofing e botnet.

4.1.73 Deve permitir a criação de assinaturas personalizadas para detecção.

4.1.74 Deve permitir a criação de novas regras personalizadas no módulo de firewall.

4.1.75 Deve permitir criar regras diferenciadas por aplicações.

4.1.76 Deve permitir o bloqueio de ataques baseado na exploração de vulnerabilidades.

4.1.77 Deve possuir integração com navegadores web para prevenção de ataques.

4.1.78 Deve realizar proteção usando mecanismo de reputação on-line, reportando ao console de gerenciamento, informações referentes às ameaças durante a navegação web.

4.1.79 Deve ser compatível, no mínimo, com os navegadores Google Chrome, Mozilla Firefox, Microsoft Edge, Opera e Safari.

4.1.80 A solução deve prover proteção em tempo real contra vírus, trojans, worms, spyware, adwares e outros tipos de códigos maliciosos.

4.1.81 As configurações do anti-malware deverão ser realizadas através da mesma console da solução.

4.1.82 A solução deve permitir a criação de listas de exceções de arquivos e diretórios (arquivos ou diretórios que não serão varridos em tempo real).

4.1.83 A solução deve permitir a verificação das ameaças de maneira manual, agendada e em tempo real, detectando ameaças no nível do Kernel do sistema operacional, fornecendo a possibilidade de detecção de Rootkits.

4.1.84 A solução deve possibilitar que, nas varreduras agendadas, o disparo do processo ocorra por grupos com intervalos de tempo determinados, para reduzir impacto no ambiente.

4.1.85 A solução deve permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar e Ignorar.

4.1.86 A solução deve possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados.

4.1.87 Detecção, análise e reparação de vírus em arquivos compactados, automaticamente, incluindo pelo menos 05 níveis de compactação.

4.1.88 Deve suportar varredura de, no mínimo, os seguintes padrões de compactação:

a) CAB;

b) ZIP;

c) RAR;

d) LHA;

e) ARJ;

f) TAR;

g) GZIP;

4.1.89 A solução deve possuir a capacidade de terminar o processo e serviço da ameaça no momento de detecção.

4.1.90 A solução deve possuir a capacidade de identificação da origem da infecção, para malwares que utilizam compartilhamento de arquivos como forma de propagação, informando nome ou endereço IP da origem com opção de bloqueio da comunicação via rede.

4.1.91 A solução deve permitir bloquear a verificação de malware em recursos mapeados da rede.

4.1.92 A solução deve possuir capacidade de realizar monitoramento em tempo real por heurística correlacionando com a reputação de arquivos.

4.1.93 Não serão aceitas soluções de anti-malware que possuam engine de terceiros.

4.1.94 A solução deve permitir o bloqueio da execução de aplicações baseado em nome e pasta.

4.1.95 A solução deve permitir a detecção de ameaças desconhecidas em memória, por comportamento dos processos e arquivos das aplicações.

4.1.96 A solução deve possuir capacidade de detecção de keyloggers por comportamento dos processos em memória.

4.1.97 A solução deve possuir capacidade de detecção de Trojans e Worms por comportamento dos processos em memória, com opção de níveis distintos de sensibilidade de detecção.

4.1.98 A solução deve realizar inspeção de ameaças em ambiente isolado, com o emprego de ferramentas como:

a) Aprendizado de máquina;

b) Deep Learning;

c) Análise estatística e dinâmica;

d) Detecção baseada em comportamento;

e) Introspecção na memória;

4.1.099 A solução deve ter a capacidade de realizar a detecção do malware por DNA do vírus.

4.1.100 A solução deve ter a capacidade de atualizar os patches do sistema operacional.

4.1.101 A solução deve ser capaz de detectar o uso do Hyper-V e ter uma verificação de malware específica disponível para este hypervisor.

4.1.102 A solução de proteção de servidor deve incluir a detecção e bloqueio de intrusões, adicionando à lista negra os endereços identificados com este comportamento malicioso.

4.1.103 A solução deve possuir otimização de desempenho para infraestruturas mistas (física e virtual), podendo eliminar a duplicação de verificações de arquivos, excluindo arquivos já verificados e limpos.

4.1.104 Deverá prover proteção à navegação dos usuários bloqueando os sites web de alto risco e suspeitos, e/ou sites que estejam infectados por algum tipo de malware, para estações de trabalho dentro ou fora da rede.

4.1.105 Deve possuir a opção "webfilter":

4.1.105.1 Esta opção deve bloquear ou permitir o acesso a sites nos dispositivos com o módulo de proteção instalado.

4.1.105.2 Deve funcionar sem necessidade de instalação de módulo adicional nos hosts.

4.1.105.3 Deve possuir blacklist(lista de bloqueio) e whitelist(lista de liberação) customizável.

4.1.105.4 Proteção contra o acesso a sites(urls) infectados com malware ou conhecidos por phishing sem a necessidade de licença adicional com listagem de sites atualizada via fabricante.

4.1.105.5 A solução deve ser executada no nível de endpoint, bloqueando o acesso ainda no host.

4.1.106 A solução deve permitir gerar relatórios de sites acessados e bloqueados.

4.1.107 A solução deve permitir a personalização das mensagens exibidas quando um ou mais sites forem bloqueados.

4.1.108 A solução deve possuir recurso de verificação de malwares nas mensagens de correio eletrônico, pelo antimalware da estação de trabalho, suportando clientes de e-mail, que utilizem minimamente os seguintes protocolos:

a) POP3;

b) POP3S;

c) IMAP;

d) IMAPS;

4.1.109 A solução deve permitir a configuração de ações personalizadas para detecções realizadas pelo módulo de proteção de e-mail, suportando minimamente as seguintes ações:

a) Mover o e-mail para uma pasta;

b) Excluir o e-mail;

c) Manter o e-mail;

4.1.110 Em equipamentos macOS, a solução deve possuir módulo para proteção de e-mails de entrada e saída.

4.1.111 Para a navegação na internet o produto deve possuir funcionalidade de anti-phishing para proteger os usuários finais de sites web falsos que tentam obter informações confidenciais.

4.1.112 A solução de proteção anti-spam deve realizar as verificações utilizando o protocolo SSL.

4.1.113 O módulo de proteção anti-spam deverá ser nativo e integrado ao Endpoint.

4.2 SOLUÇÃO PARA CRIPTOGRAFIA DE DISCOS

4.2.1 A solução deve ser capaz de criptografar dispositivos Windows, Linux e macOS.

4.2.2 A solução deverá possuir tecnologia própria de criptografia, além de capacidade de gerenciamento do Microsoft BitLocker e FileVault disponibilizado pela Apple para MacOS.

4.2.3 A solução deve possuir compatibilidade com a tecnologia AES-NI, que utiliza o conjunto de instruções dos algoritmos Advanced Encryption Standard (AES), visando tornar o processo de criptografia e descriptografia mais rápido e eficiente.

4.2.4 A solução deve dispor de recurso que permita o administrador ter visibilidade de quais dispositivos possuem o módulo de criptografia instalado, bem como os que ainda não possuem.

4.2.5 A solução deve permitir que o administrador monitore quais dispositivos estão criptografados, atendendo à política de criptografia definida, dispositivos que não estão criptografados, bem como dispositivos que apresentaram algum problema para aplicação da criptografia.

4.2.6 A solução deve ser capaz de criptografar os Endpoints desejados desde o início do sistema operacional.

4.2.7 A solução deve dispor de possibilidade de recuperação de senha para usuários remotos que estejam bloqueados nativamente, ou seja, sem o uso de scripts.

4.2.8 A solução deve poder programar as tarefas de criptografia sobre os Endpoints desejados com a possibilidade de retomar a execução em seu último estado em caso de pausa.

4.2.9 A solução deve ser administrada desde o mesmo console central com as outras soluções descritas neste termo de referência.

4.2.10 A solução deve possuir recurso para criptografar e descriptografar apenas o espaço em disco utilizado.

4.2.11 Possibilitar a opção de criptografar apenas o disco de inicialização, bem como criptografar todos os discos.

4.2.12 A solução deve possuir opções para utilização de TPM (Trusted Platform Module) se disponível, bem como forçar a utilização de TPM (Trusted Platform Module) para aplicação da criptografia de disco.

4.2.13 A solução deve possuir compatibilidade com a tecnologia de autocriptografia OPAL.

4.2.14 A solução deve possuir opções para utilização da tecnologia OPAL se disponível, bem como forçar a utilização de OPAL para aplicação da criptografia de disco.

4.2.15 A solução deve suportar a tecnologia Single Sign-On (SSO), permitindo que o usuário realize uma única autenticação no equipamento. Ao autenticar-se na tela de autenticação da solução, o usuário será automaticamente autenticado no sistema operacional, sem a necessidade de inserir suas credenciais novamente.

4.2.16 A solução deve permitir que o administrador configure os requerimentos mínimos para definição da senha que será utilizada na criptografia. No mínimo, os seguintes requerimentos devem ser configuráveis:

4.2.16.1 Possibilidade de o usuário alterar sua senha sem intervenção do administrador, diretamente através da interface do produto.

4.2.16.2 Caracteres da senha:

- 4.2.16.2.1 Utilização de letras em caixa baixa;
- 4.2.16.2.2 Utilização de letras em caixa alta;
- 4.2.16.2.3 Utilização de números;
- 4.2.16.2.4 Comprimento mínimo de senha;

4.2.16.3 Possibilidade de limitar as tentativas incorretas de utilização da senha de criptografia.

4.2.16.4 Possibilidade de definição do limite máximo de tentativas incorretas de utilização da senha de criptografia.

4.2.16.5 Expiração da senha:

- 4.2.16.5.1 Possibilidade de configurar a expiração da senha utilizada na criptografia.
- 4.2.16.5.2 Tempo de expiração da senha (dias).

4.2.16.6 A solução deve ter a capacidade de enviar um alerta ao usuário, informando-o sobre a expiração da senha, caso a configuração estiver habilitada.

4.2.16.7 A solução deve permitir que o administrador defina com quantos dias de antecedência o alerta deve ser enviado ao usuário.

4.2.17 A solução deve permitir que o administrador instale a solução com uma senha pré-definida, retirando a necessidade que o usuário crie sua própria senha para a criptografia.

4.2.18 Através da console central deve ser possível invalidar a senha de login do usuário e solicitar que mude sua senha de login por meio de uma interface gráfica.

4.2.19 A solução deve permitir o bloqueio da senha de login do usuário, permitindo apenas o acesso através da senha única de recuperação, gerada através da console de gerenciamento.

4.2.20 A solução deve permitir a remoção da senha de login do usuário, fazendo com que, neste caso, a máquina somente possa ser iniciada via ferramenta de recuperação avançada, executada pelo administrador da solução. Caso o equipamento esteja em uso no momento da ação de remoção, este deve ser reinicializado automaticamente para garantir o sucesso da ação.

4.2.21 A solução deve permitir que o administrador desative temporariamente a tela de autenticação através da console de gerenciamento, para realização de manutenção do equipamento, sem que a senha da criptografia seja solicitada, podendo reativá-la automaticamente após a conclusão da manutenção.

4.2.22 A solução deve possibilitar a desativação permanente da tela de autenticação, caso necessário.

4.2.23 Deve possibilitar que o administrador recupere os dados caso o usuário não consiga acessar a máquina com suas credenciais.

4.2.24 A senha de recuperação gerada pela solução deve ser única para cada máquina, ou seja, cada dispositivo criptografado irá possuir sua senha individual de recuperação, gerada automaticamente pela solução.

4.2.25 Deve possibilitar que o administrador gere uma nova senha de recuperação para o dispositivo.

4.2.26 A solução deve oferecer ferramenta de recuperação avançada, para casos em que há a impossibilidade de inicialização correta do dispositivo, devido à falha física ou falha do sistema operacional. Esta ferramenta deve permitir a inicialização da máquina por meio de uma mídia removível (pen drive USB), permitindo que os dados criptografados sejam recuperados após a descriptografia manual do disco.

4.3 SOLUÇÃO PARA GERENCIAMENTO DE VULNERABILIDADES E PATCHES

4.3.1 O módulo de gerenciamento de vulnerabilidades e patches deve estar disponível para estações de trabalho e servidores Windows, macOS e Linux.

4.3.2 Para estações de trabalho Windows, a solução deve minimamente identificar vulnerabilidades no sistema operacional e aplicações de terceiros, além de permitir a correção automática das vulnerabilidades encontradas.

4.3.3 Para servidores Windows, a solução deve minimamente identificar vulnerabilidades no sistema operacional e aplicações de terceiros, além de permitir a correção automática das vulnerabilidades encontradas, corrigindo, no mínimo, as vulnerabilidades de aplicativos de terceiros.

4.3.4 Para estações de trabalho e servidores macOS, a solução deve minimamente identificar vulnerabilidades em aplicações de terceiros, além de permitir a correção automática das vulnerabilidades encontradas.

4.3.5 Para estações de trabalho e servidores Linux, a solução deve minimamente identificar vulnerabilidades no sistema operacional e aplicações de terceiros.

4.3.6 Deve rastrear ativamente as vulnerabilidades dos sistemas operacionais suportados e demais aplicações comuns.

4.3.7 Deve poder configurar intervalo de tempo para escaneamento de vulnerabilidades e atualizações disponíveis, bem como para instalação automática de patches.

4.3.8 A solução deve oferecer opção para escaneamento manual em busca de vulnerabilidades.

4.3.9 A solução deve oferecer opção para correção manual de determinada vulnerabilidade, bem como, opção para correção automatizada.

4.3.10 Para a atualização automática de aplicativos de terceiros, a solução deve oferecer minimamente as seguintes opções de configuração:

4.3.10.1 Corrigir apenas em aplicativos permitidos;

4.3.10.2 Corrigir em todos os aplicativos suportados, exceto os aplicativos excluídos;

4.3.10.3 Aplicar apenas patches que corrigem vulnerabilidades;

4.3.10.4 Aplicar todos os patches;

4.3.10.5 Especificar a pontuação mínima para correção automática:

4.3.10.5.1 Pontuação com base no CVSS;

4.3.10.5.2 Pontuação de risco da solução;

4.3.11 Para a atualização automática de patches do sistema operacional, a solução deve oferecer minimamente as seguintes opções de configuração:

4.3.11.1 Instalar todas as atualizações compatíveis;

4.3.11.2 Instalar apenas atualizações importantes;

4.3.11.3 Instalar apenas atualizações críticas;

4.3.12 A solução deve fornecer, minimamente, as seguintes informações sobre as vulnerabilidades detectadas:

4.3.12.1 Nome do aplicativo;

4.3.12.2 Fornecedor;

4.3.12.3 Versão do aplicativo;

4.3.12.4 Nome do computador;

4.3.12.5 Pontuação de risco;

4.3.12.6 CVE;

4.3.12.7 Categoria (Vulnerabilidade de aplicativo ou sistema operacional);

4.3.12.8 Descrição técnica da vulnerabilidade;

4.3.12.9 Data da primeira aparição na rede;

4.3.12.10 Link de referência do fabricante;

4.3.12.11 CWE;

4.3.12.12 Score CVSS v3:

4.3.12.12.1 String do vetor;

4.3.12.12.2 Pontuação base;

4.3.12.12.3 Pontuação de impacto;

4.3.12.12.4 Pontuação de capacidade de exploração;

4.3.13 A solução deve possuir recurso para consulta de CVEs. Ao inserir um CVE, a solução deve retornar se este CVE já é identificado no banco de dados da solução, e, se foi encontrado em algum equipamento do ambiente.

4.3.14 Deve poder aplicar patches no sistema operacional, bem como em aplicações de terceiros comuns como 7Zip, Foxit, Firefox, Chrome, Java, LibreOffice.

4.3.15 Deve priorizar e filtrar as vulnerabilidades segundo sua pontuação de exposição e gravidade.

4.3.16 Deve permitir a visibilidade de vulnerabilidades em grupos específicos da organização.

4.3.17 Deve possuir controle das exceções para os patches de aplicações selecionadas.

4.3.18 Deve permitir silenciar determinadas vulnerabilidades, fazendo com que estas sejam removidas da visualização do administrador, porém, não inseridas permanentemente em uma lista de exclusão.

4.3.19 Deve proporcionar um inventário atualizado de patches encontrados, disponibilizando, pelo menos, as seguintes informações:

4.3.19.1 Nome do aplicativo;

4.3.19.2 Fornecedor do aplicativo;

4.3.19.3 Versão atual do aplicativo;

4.3.19.4 Versão do patch;

4.3.19.5 Nome do computador;

4.3.19.6 EULA da nova versão do aplicativo;

4.3.19.7 Registro de alterações;

4.3.19.8 Vulnerabilidades corrigidas;

4.3.20 A solução deve exibir logs de escaneamentos e aplicação de patches, permitindo a identificação de erros durante o processo de escaneamento de vulnerabilidades e aplicação de patches, bem como as rotinas realizadas com sucesso.

4.3.21 A solução deve permitir a criação de painéis e relatórios interativos para acompanhamento do módulo de gestão de vulnerabilidades e patches.

4.3.22 A solução deve possuir painéis pré-definidos que mostrem o funcionamento geral do módulo de gestão de vulnerabilidades gerais, e as principais informações encontradas pela solução. No mínimo, as seguintes informações devem ser exibidas:

4.3.22.1 Número total de vulnerabilidades críticas;

4.3.22.2 Número total de vulnerabilidades de risco médio;

4.3.22.3 Número de vulnerabilidades ao longo do tempo, exibindo o número total de vulnerabilidades detectadas nos últimos 7 ou 30 dias;

4.3.22.4 Último escaneamento em busca de vulnerabilidades nos computadores;

4.3.22.5 Computadores mais vulneráveis;

4.3.22.6 Principais computadores com vulnerabilidades de Sistema Operacional;

4.3.22.7 Principais aplicativos vulneráveis;

4.3.22.8 Impacto geral das vulnerabilidades;

4.4 Solução para Prevenção de Perda de Dados (DLP)

4.4.1 Descoberta e Classificação de Dados Sensíveis: Capacidade de escanear o conteúdo nos *endpoints* (*data at rest*) para identificar, classificar e rotular dados confidenciais e PII (*Personally Identifiable Information*).

4.4.2 Prevenção Baseada em Conteúdo (LGPD/PII): A solução deve permitir a criação de regras de DLP que inspecionem o conteúdo em trânsito (*data in motion*) e em uso (*data in use*), utilizando: A. Expressões Regulares (RegEx) para padrões brasileiros (ex: CPF, CNPJ, Cartão de Crédito). B. Dicionários e Palavras-chave pré-definidos e/ou customizáveis. C. *Digital Fingerprinting* ou *Exact Data Matching (EDM)* para detecção de documentos e registros exatos.

4.4.3 Controle de Periféricos (Dispositivos Removíveis): Controle granular do acesso a mídias removíveis (USB Drives, CDs/DVDs, cartões SD) e dispositivos de conectividade sem fio (Bluetooth), permitindo ações como: A. Bloqueio total. B. Bloqueio por usuário/grupo. C. Bloqueio por *Device ID* específico. D. Modo *Read-Only* (somente leitura).

4.4.4 Controle de Canais de Comunicação: Capacidade de inspecionar, monitorar, bloquear ou criptografar o fluxo de dados em canais de comunicação de rede: A. Web Uploads (HTTPS/HTTP). B. Webmail e E-mails (SMTP/POP3). C. Impressoras e Screenshots. D. Serviços de Armazenamento em Nuvem (Ex: Dropbox, Google Drive, OneDrive).

4.4.5 Criptografia Forçada em Mídia Removível: Capacidade de, ao detectar a tentativa de transferência de dados sensíveis para um dispositivo USB, forçar a criptografia do arquivo ou do dispositivo antes que a transferência seja concluída.

4.4.6 Evidências e Auditoria: Geração de logs detalhados de todas as violações (incluindo o arquivo, o canal utilizado, o usuário e a política violada) e captura de evidências forenses (cópia-sombra do arquivo vazado) para fins de investigação e auditoria.

5. OUTROS REQUISITOS GERAIS

5.1 A solução ofertada não deve possuir restrições sobre a quantidade de equipamentos por sistemas operacionais para ativação das licenças. A totalidade das licenças contratadas pode ser ativada completamente em servidores, estações de trabalho, ou dispositivos móveis, respeitando apenas o limite total contratado.

5.2 Todos os módulos ofertados pelo fabricante, devem ser ativados utilizando uma única licença, sem a necessidade de aquisição de módulos separados (add-ons).

5.3 O fabricante deverá ter suporte local em idioma português do Brasil.

5.4 O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines e possuir analista dedicado à pesquisa de ameaças e malwares originados no Brasil. Esta informação deve ser comprovada pelo fabricante por meio de documentação oficial.

5.5 O fabricante deve possuir um laboratório de análise e detecção de malware na América Latina.

5.6 O fabricante deve possuir escritório próprio no Brasil.

5.7 O fabricante deve possuir documentação de apoio da solução em português do Brasil.

5.8 O fabricante deve ser citado nos relatórios do MITRE ATT&CK como contribuinte de informações e técnicas de detecção nos últimos anos.

5.9 O monitoramento e o gerenciamento deverão ser unificados através de uma console centralizada, permitindo a administração de todos os computadores e possibilitando, a critério do administrador da Solução de Antivírus, a integração com o Active Directory da Microsoft.

5.10 Deverá possuir suporte à auditoria, permitindo que cada usuário que efetuar determinados comandos ou ações administrativas terá todas as suas ações sendo registradas para fins de verificação posterior.

5.11 Deverá possuir console de único login, permitindo que um único usuário tenha acesso a todas as consoles e configuração de todos os produtos de segurança.

5.12 A CONTRATADA deverá garantir a continuidade e a plena funcionalidade da Solução de Proteção de Endpoint e EDR/EPP no território nacional. Caso a solução ofertada venha a sofrer restrições por:

a) Restrições Geopolíticas ou Sanções;

b) Impedimento Legal ou Regulatório;

c) Risco à Segurança ou Continuidade Operacional;

d) Ruptura Comercial ou Suporte;

e) Eventos de Força Maior ou catástrofes (naturais ou não);

ou qualquer outros eventos que impeçam ou comprometam o seu uso, o seu suporte, a obtenção de atualizações de vacinas e engines de detecção ou a comunicação com os servidores de Intelligence necessários, a CONTRATADA será obrigada a:

a) Prover Solução Alternativa: Substituir a solução integralmente por uma ferramenta de segurança de endpoint de outro fabricante, com funcionalidades e desempenho equivalentes ou superiores aos requisitos técnicos desta contratação.

b) Assumir Custos: Arcar integralmente com todos os custos envolvidos no processo de substituição, incluindo, mas não se limitando a, novas licenças, serviços de migração (desinstalação, deployment e configuração da nova solução) e treinamentos de reciclagem da equipe técnica da CONTRATANTE.

c) Prazo para Migração: Iniciar a migração, instalação e configuração da solução alternativa no prazo máximo de 30 (trinta) dias corridos após a notificação oficial da restrição.

5.13 A CONTRATADA e a Solução de Segurança de Endpoint ofertada (EPP/EDR) devem garantir a plena e contínua conformidade com toda a legislação brasileira vigente aplicável ao tratamento de dados e segurança da informação. Isso inclui, mas não se limita à Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e ao Marco Civil da Internet (Lei nº 12.965/2014).

5.14 A implantação inicial deve ser conduzida pela CONTRATADA com acompanhamento da equipe técnica da CONTRATANTE. Manutenção e gestão subsequente pela CONTRATANTE com suporte da CONTRATADA.

Documento assinado eletronicamente por **Rodrigo Ponick**, **Gerente**, em 28/11/2025, às 09:56, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Grasiele Wandersee Philippe**, **Coordenador(a)**, em 28/11/2025, às 10:51, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

Documento assinado eletronicamente por **Alessandro de Cassio Silva**, **Servidor(a) Público(a)**, em 28/11/2025, às 10:55, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.

A autenticidade do documento pode ser conferida no site https://portalsei.joinville.sc.gov.br/ informando o código verificador **27660850** e o código CRC **2B784E20**.