PREGÃO ELETRÔNICO Nº 0047/2025
PROCESSO CIASC Nº 0510/2025

ANEXO I – TERMO DE REFERÊNCIA

1. - OBJETO

Renovação e contratação de solução de tecnologia da informação para a proteção de computadores contra software malicioso (malware), composta por sistema de software antivírus, gerenciamento centralizado para ambiente corporativo, e também aquisição de licenças de uma ferramenta de Endpoint Detection and Response (EDR) ou Extended Detection and Response (XDR), visando fortalecer a postura de segurança da informação da instituição. Está incluso serviços de suporte técnico, migração ou atualização e treinamento.

2. - JUSTIFICATIVA

O CIASC é fornecedor de Tecnologia da Informação para diversos clientes do estado e municípios.Para aumentarmos a segurança dos servidores hospedados em nosso Data Center e estações de trabalho, utilizamos a Solução de Segurança conhecida como Antivírus Corporativo desde 2012. Estamos hoje com contratos ativos que fazem uso de licenças que tem seu vencimento em 2025 e precisam ser renovadas. Temos ainda tratativas com outros órgãos do estado que demandam por mais licenças do que dispomos hoje.
O processo será dividido em 2 LOTES:

LOTE 1: Será utilizado para expansão de pedidos de clientes que já utilizam a solução Kaspersky.

LOTE 2: Este contrato será utilizado para captação de clientes para nova solução de EDR/XDR.

3. - ESPECIFICAÇÕES TÉCNICAS

LOTE 1:

Este contrato será utilizado para expansão de pedidos de clientes que já utilizam a solução do fabricante Kaspersky.

As aquisições obedecerão à conveniência e às necessidades do CIASC, dentro do prazo de validade da Ata de Registro de Preços e, quando realizadas, obedecerão a seguinte distribuição quantitativa:

LOTE 1 INICIAL: 1.000 (mil) licenças.

LOTE 1 ADICIONAL: pedidos de no mínimo 100 (cem) licenças.

TOTAL LOTE 1: 20.000 (vinte mil) licenças.

VALIDADE LOTE 1: Período de validade das licenças: 12 (doze) meses a contar da data do fornecimento de cada pedido do lote.

LOTE 1: Características Técnicas: Licença Kaspersky Next EDR Foundations - 12 meses

O CIASC não se obriga a consumir a totalidade do LOTE 1.

LOTE 2:

Este contrato será utilizado para captação de clientes para solução de EDR ou XDR.

As aquisições obedecerão à conveniência e às necessidades do CIASC, dentro do prazo de validade da Ata de Registro de Preços e, quando realizadas, obedecerão a seguinte distribuição quantitativa:

LOTE 2 INICIAL: 100 (cem) licenças para estações de trabalho Windows.

LOTE 2 ADICIONAL: pedidos de no mínimo 100 (cem) licenças.

TOTAL LOTE 2: 20.000 (vinte mil) licenças.

Sendo destas, 1.000 (um mil) licenças para sistemas operacionais Windows Server, 500 (quinhentas) para sistemas operacionais Linux e 18.500 (dezoito mil e quinhentas) licenças para estações Windows.

VALIDADE LOTE 2: Período de validade das licenças: 12 (doze) meses a contar da data do fornecimento de cada pedido do lote.

O CIASC não se obriga a consumir a totalidade do LOTE 2.

Características técnicas do LOTE 2:

3.1. Requisitos Mínimos da Solução de EDR ou XDR

A solução ofertada deverá atender aos seguintes requisitos técnicos mínimos:

3.1.1. Funcionalidades de Detecção e Prevenção

- Proteção Multi-Camadas: Capacidade de proteção contra malware (incluindo ransomware), exploits, ataques sem arquivo (fileless attacks), phishing e ameaças de dia zero.
- Análise Comportamental: Utilização de análise de comportamento para identificar atividades maliciosas e anômalas, mesmo sem assinaturas prévias.
- Machine Learning e Inteligência Artificial: Emprego de ML/IA para detecção avançada de ameaças e redução de falsos positivos.
- Detecção de IoCs (Indicators of Compromise): Capacidade de identificar e alertar sobre IoCs conhecidos e emergentes.
- Prevenção de Exploração de Vulnerabilidades: Proteção contra a exploração de vulnerabilidades em softwares e sistemas operacionais.
- Controle de Aplicações: Capacidade de controlar a execução de aplicações não autorizadas

(whitelisting/blacklisting).

- Inspeção de Memória: Análise de processos em memória para detecção de ameaças residentes.
- Proteção Offline: Garantir proteção contínua mesmo quando o endpoint estiver offline ou desconectado da rede.

3.1.2. Funcionalidades de Resposta e Investigação

- Visibilidade e Telemetria Completa: Coleta e registro detalhado de eventos de endpoint (processos, conexões de rede, modificações de registro, acessos a arquivos, etc.).
- Pesquisa de Ameaças (Threat Hunting): Ferramentas para realizar buscas proativas e investigações em tempo real sobre atividades suspeitas nos endpoints.
- Isolamento de Endpoint: Capacidade de isolar endpoints comprometidos da rede para conter a propagação de ataques.
- Eliminação de Arquivos Maliciosos: Remoção e quarentena de arquivos suspeitos ou maliciosos.
- Interrupção de Processos: Encerramento de processos maliciosos.
- Desfazer Alterações Maliciosas: Reverter alterações feitas por atividades maliciosas no sistema.
- Visualização de Ataques (Attack Storyline/Kill Chain): Apresentação clara e intuitiva da sequência de eventos de um ataque, desde o início até a sua contenção.
- Integração com Threat Intelligence: Consumo de feeds de inteligência de ameaças para enriquecer as detecções e investigações.
- Resposta Automatizada (SOAR-like capabilities): Capacidade de configurar regras para respostas automáticas a eventos específicos de segurança.

3.1.3. Arquitetura e Gerenciamento

- Console Centralizado de Gerenciamento: Interface web intuitiva e centralizada para gerenciamento de todos os endpoints e visualização de alertas.
- Multi-Tenancy: A solução deve permitir a administração de múltiplos clientes ou ambientes de forma isolada e segura dentro da mesma console de gerenciamento, garantindo a segregação de dados e configurações entre eles.
- Escalabilidade: Capacidade de suportar um número crescente de endpoints sem degradação de performance.
- Implantação Flexível: Opções de implantação em nuvem (SaaS), on-premise ou híbrida, conforme a necessidade.
- Agente Leve: Agente de endpoint com baixo impacto no desempenho do sistema e consumo de recursos.
- Compatibilidade de Sistemas Operacionais: Suporte para os principais sistemas operacionais de desktops, servidores e, se aplicável, dispositivos

móveis (Windows, macOS, Linux, Android, iOS). ● Integrações (APIs): Disponibilidade de APIs para integração com outras ferramentas de segurança (SIEM, SOAR, CMDB, etc.).

- Relatórios e Dashboards: Geração de relatórios personalizáveis e dashboards para acompanhamento da postura de segurança e auditoria.
- Controle de Acesso Baseado em Função (RBAC): Definição de perfis de acesso e permissões para diferentes usuários do console de gerenciamento.
- Atualizações automatizadas: Mecanismos de atualização automática do agente e da base de detecção.

3.1.4. Requisitos Específicos para XDR (se aplicável)

Caso a solução ofertada seja XDR, ela deverá, além dos requisitos acima, apresentar a capacidade de integrar e correlacionar telemetria de diversas fontes, tais como:

- Rede: Firewalls, IDS/IPS, proxies, Network Detection and Response (NDR).
- E-mail: Gateways de segurança de e-mail.
- Nuvem: Workloads em nuvem, ambientes de SaaS.
- Identidade: Soluções de identidade e acesso (IAM, AD).
- Dados: Soluções de Data Loss Prevention (DLP).
- Automação: Capacidade de orquestrar respostas entre diferentes domínios de segurança.

3.2. Quantidade de Licenças

As aquisições obedecerão à conveniência e às necessidades do CIASC, dentro do prazo de validade da Ata de Registro de Preços e, quando realizadas, obedecerão a seguinte distribuição quantitativa:

LOTE 2 INICIAL: 100 (cem) licenças para estações de trabalho Windows.

LOTE 2 ADICIONAL: pedidos de no mínimo 100 (cem) licenças.

TOTAL LOTE 2 : 20.000 (vinte mil) licenças.

Sendo destas, 1.000 (um mil) licenças para sistemas operacionais Windows Server, 500 (quinhentas) para sistemas operacionais Linux e 18.500 (dezoito mil e quinhentas) licenças para estações Windows.

VALIDADE LOTE 2: Período de validade das licenças: 12 (doze) meses a contar da data do fornecimento de cada pedido do lote.

O CIASC não se obriga a consumir a totalidade!

3.3. Suporte Técnico e Treinamento O fornecedor deverá oferecer:

- Suporte Técnico Especializado: Disponibilidade de suporte técnico para a solução 8x5, em português, com prazos de atendimento (SLA) para diferentes níveis de criticidade.
- Atualizações e Upgrades: Garantia de acesso a todas as atualizações, patches e novas versões da solução durante o período de contratação.

- Treinamento: Oferecimento de treinamento para a equipe técnica da instituição, abordando a administração, operação e análise da ferramenta.

3.4. Considerações Finais

As funcionalidades devem ser comprovadas por documentos de domínio público disponíveis no site do fabricante.

4. - QUALIFICAÇÃO TÉCNICA

Apenas para o LOTE 2:

A qualificação técnica do licitante será avaliada com base nos seguintes requisitos, que visam garantir que o fornecedor possua a capacidade técnica e operacional necessária para fornecer, implantar e manter a solução de segurança com a qualidade e a eficiência exigidas:

4.1. Qualificação Técnico-Operacional

4.1.1. Para comprovação da Qualificação Técnica Operacional, o licitante deverá apresentar documento emitido pelo fabricante do(s) equipamento(s) ou produto(s) objeto desta licitação, atestando seu **credenciamento oficial** como parceiro autorizado, revenda, distribuidor ou prestador de serviços.

4.1.2. O referido documento deverá indicar, expressamente, que o licitante está apto a comercializar e/ou prestar serviços de instalação e manutenção, com **acesso a suporte técnico e garantia de fábrica**, para o(s) item(ns) objeto da presente licitação.

4.1.3. A comprovação de credenciamento é indispensável para assegurar a originalidade do produto, a validade da garantia de fábrica e o acesso ao suporte técnico especializado, garantindo a qualidade e a segurança do fornecimento.

5. - PRAZOS

LOTE 1 e LOTE 2:

A solução deverá ser entregue e implantada em até 30 dias após a assinatura do contrato.

6. - LOCAL DE ENTREGA ou EXECUÇÃO

Caso a solução seja composta apenas por software sem equipamento físico, as tratativas podem ser via e-mail cosei@ciasc.sc.gov.br.

Caso envolva equipamentos, neste caso, deverão ser entregues na sede do CIASC em Florianópolis, na Rua Murilo Andriani, 327, bairro Itacorubi.

7. - CONDIÇÕES DE ENTREGA/RECEBIMENTO OU EXECUÇÃO

Para o LOTE 1: As entregas estarão contempladas, após comprovado o envio e aplicação das licenças na console de gerenciamento.

Para o LOTE 2: As entregas estarão contempladas, após implementação da solução ofertada, criação de usuários para gerenciamento da solução de EDR/XDR, treinamento para os 08 técnicos da solução, e comprovado o envio e aplicação das licenças na console de gerenciamento.

8. - CRONOGRAMA FISICO-FINANCEIRO

O pagamento será de acordo com os pedidos entregues, sob demanda, realizados dentro da Ata de Registro de Preços, respeitando os limites especificados nesta ata.

9. - RESULTADOS ESPERADOS/ENTREGÁVEIS

Vencedor LOTE 1:

Entrega das licenças da Solução Kaspersky Next EDRFoundations;

Suporte técnico em formato 8x5, com limite de 80 (oitenta) horas para atendimento técnico, e sem limites de abertura de chamados.

Vencedor LOTE 2:

Entrega das licenças da Solução de EDR ou XDR;

Suporte técnico em formato 8x5, com limite de 80 (oitenta) horas anuais para atendimento técnico, e sem limites de abertura de chamados;

Treinamento para 8 (oito) técnicos da CONTRATANTE.

10. - GARANTIA, ASSISTÊNCIA TÉCNICA, SUPORTE TÉCNICO E NÍVEIS DE SERVIÇO

LOTE 1 e LOTE 2:

Suporte técnico e garantia de software durante a vigência do contrato;

Suporte técnico de 80 horas anuais pelo período do contrato, de acordo com a necessidade da CONTRATANTE.

11. - OBRIGAÇÕES DA CONTRATADA

Vencedor LOTE 1:

Entregar as licenças da Solução Kaspersky Next EDR Foundations;

Garantia na Solução da Console de Gerenciamento durante a vigência do contrato;

Prestar suporte técnico em formato 8x5, com limite de 80 (oitenta) horas anuais para atendimento técnico, e sem limites de abertura de chamados.

Vencedor LOTE 2:

Implantar a Solução da Console de Gerenciamento e o licenciamento necessário para funcionamento pelo da solução EDR;

Prestar treinamento para 8 (oito) pessoas;

Entrega das licenças de EDR ou XDR;

Garantia na Solução da Console de Gerenciamento durante a vigência do contrato;

Suporte técnico em formato 8x5, com limite de 80 (oitenta) horas anuais para atendimento técnico, e sem limites de abertura de chamados.

12. - MATRIZ DE RISCO

Risco 01	***Atraso na entrega das licenças***							
Consequências:								
1	*Não cumprimento do contrato com o cliente do CIASC*							
2	*Máquinas ficarão desprotegidas*							
2.1 - AVALIAÇÃO DO RISCO								
Probabilidade	Baixa			Impacto	Moderado			
Nível do Risco	- Risco Crítico			Tolerância do Risco			Aceitável	
Responsabilidade	x	Contratada		Contratante		Compatilhada		
Resposta ao Risco	x	Evitar		Reduzir		Transferir		Aceitar
Estratégia de Resposta ao Risco								
1	*Solicitar as licenças com antecedência*							
2	*Usar a reserva técnica de licenças de clientes que contrataram, mas não utilizaram ainda.*							
Risco 02	***Não entrega das licenças***							
Consequências:								
1	*Não cumprimento do contrato com o cliente do CIASC*							
2	*Máquinas ficarão desprotegidas*							
2.1 - AVALIAÇÃO DO RISCO								
Probabilidade	Baixa			Impacto	Moderado			
Nível do Risco	- Risco Crítico			Tolerância do Risco			Não Aceitável	
Responsabilidade	x	Contratada		Contratante		Compatilhada		
Resposta ao Risco	x	Evitar		Reduzir		Transferir		Aceitar
Estratégia de Resposta ao Risco								

1	*Penalizar a contratada e realizar novo novo processo de contratação*
2	*Usar a reserva técnica de licenças de clientes que contrataram, mas não utilizaram ainda.*
Risco 3	**Entrega das licenças na versão errada**
Consequências:	
1	Não cumprimento do contrato com o cliente do CIASC
2	Máquinas ficarão desprotegidas
2.1 - AVALIAÇÃO DO RISCO	
Probabilidade	Baixa — Impacto: Moderado
Nível do Risco	- Risco Crítico — Tolerância do Risco: Não Aceitável

Responsabilidade	x	Contratada		Contratante		Compatilhada		
Resposta ao Risco	x	Evitar		Reduzir		Transferir		Aceitar

Estratégia de Resposta ao Risco	
1	Usar a reserva técnica de licenças de clientes que contrataram, mas não utilizaram ainda.
2	Informar o fornecesor sobre o erro e solicitar a versão correta
3	aplicar as penalidades previstas, de forma educativa, para evitar novas falhas
Risco 04	**Ficar sem suporte e atualizações**
Consequências:	
1	Máquinas desprotegidas.
2	Não conformidade no contrato com clientes do CIASC.
2.1 - AVALIAÇÃO DO RISCO	
Probabilidade	Muito Baixa — Impacto: Moderado
Nível do Risco	- Risco Crítico — Tolerância do Risco: Não Aceitável

Responsabilidade	x	Contratada		Contratante		Compatilhada		
Resposta ao Risco	x	Evitar		Reduzir		Transferir		Aceitar

Estratégia de Resposta ao Risco	
1	Penalizar a contratada conforme contrato.
2	Solicitar apoio do fabricante.
3	Realizar novo processo de contratação.

gov.br Documento assinado digitalmente
SIDINEI ALEX MASIERO
Data: 26/03/2026 17:01:12-0300
Verifique em https://validar.iti.gov.br