CIASC
CENTRO DE INFORMÁTICA
E AUTOMAÇÃO DO ESTADO DE SANTA CATARINA S.A.

ANEXO II: ESTUDO TÉCNICO PRELIMINAR

1. Equipe de Planejamento

Nome	Cargo/função	E-mail
DIEGO LOPES DA CRUZ	COORDENADOR	diegolc@ciasc.sc.gov.br

2. Descrição do problema a ser resolvido ou da necessidade apresentada

O CIASC atua como fornecedor de Tecnologia da Informação para diversos clientes do estado de Santa Catarina e municípios. Desde 2012, tem utilizado uma Solução de Segurança conhecida como Antivírus Corporativo para aprimorar a segurança dos servidores hospedados em seu Data Center e das estações de trabalho de clientes contratantes. Atualmente, existem contratos ativos com licenças que vencem em 2025 e necessitam de renovação. Além disso, há tratativas em andamento com outros órgãos do estado que demandam um número maior de licenças do que o atualmente disponível. O CIASC possui 20.000 licenças ativas, atendendo a mais de 19.500 estações e servidores entre secretarias de estado e prefeituras. A atual Ata de Registro de Preços será utilizada quase em sua totalidade. A solução em uso tem se mostrado segura e consolidada, sem registro de incidentes de segurança, como vírus, malwares ou ransomwares, nas máquinas cobertas. A necessidade é garantir a continuidade dos serviços de segurança já fornecidos, assegurando a disponibilidade de licenças.

A contratação conta ainda com um segundo lote referente a licenças XDR (Extended Detection and Response). A solução XDR tem o objetivo de atender necessidades de segurança complementares, em uma plataforma unificada que integre e correlacione dados de múltiplas camadas de segurança (endpoints, e-mails, redes, servidores e nuvem), utilizando recursos avançados de automação e inteligência artificial para melhorar a detecção, investigação e resposta a ameaças. A solução XDR deve proporcionar visibilidade de ponta a ponta, reduzir falsos positivos, automatizar respostas a incidentes e otimizar os fluxos de trabalho da equipe de Segurança da Informação, garantindo maior proteção contra ciberataques avançados e conformidade com normas regulatórias.

3. Demonstração da previsão da contratação com o Plano Anual de Compras

Item 455 - Licenças de Antivírus

Item	Unidade	Descrição	Natureza	Quantidade
455	Licença	Licenças de antivirus	Software e licenças	20.000,00

4. **Descrição dos requisitos da potencial contratação**

A contratação será dividida em dois lotes, com requisitos específicos:

• **LOTE 1:** Destinado à expansão de pedidos de clientes que já utilizam a solução Kaspersky.

◦ **Características Técnicas:** A contratação visa a renovação e aquisição de 30.000 Licença "Kaspersky Next EDR Foundations".

• **LOTE 2:** Destinado à captação de clientes para uma nova solução de segurança avançada de endpoint (XDR).

Os requisitos detalhados estão listados no Termo de Referência, destacando-se os seguintes:

Funcionalidades de Detecção e Prevenção: Proteção multicamadas (malware, ransomware, exploits, ataques sem arquivo, phishing, dia zero), análise comportamental, uso de Machine Learning e Inteligência Artificial para detecção avançada e redução de falsos positivos, detecção de IoCs, prevenção de exploração de vulnerabilidades, controle de aplicações (whitelisting/blacklisting), inspeção de memória, e proteção contínua mesmo offline.

Funcionalidades de Resposta e Investigação: Coleta e registro detalhado de eventos de endpoint (processos, conexões de rede, modificações de registro, acessos a arquivos), ferramentas para busca proativa de ameaças (Threat Hunting), isolamento de endpoints comprometidos, remoção e quarentena de arquivos maliciosos, encerramento de processos maliciosos, reversão de alterações maliciosas no sistema, integração com Threat Intelligence, e capacidade de configurar respostas automáticas (SOAR-like capabilities).

Arquitetura e Gerenciamento: Console centralizada de gerenciamento (interface web intuitiva), Multi-Tenancy para administração isolada de múltiplos clientes, escalabilidade, implantação flexível (nuvem, on-premise, híbrida), agente leve com baixo impacto no desempenho, compatibilidade com principais sistemas operacionais (Windows, macOS, Linux, Android, iOS), disponibilidade de APIs para integração com outras ferramentas de segurança (SIEM, SOAR, CMDB), geração de relatórios personalizáveis e dashboards, Controle de Acesso Baseado em Função (RBAC), e mecanismos de atualização automática.

Requisitos Específicos para XDR: Capacidade de integrar e correlacionar telemetria de diversas fontes como rede (Firewalls, IDS/IPS, proxies, NDR), e-mail (gateways de segurança), nuvem (workloads, SaaS), identidade (IAM, AD), dados (DLP) e automação para orquestrar respostas entre diferentes domínios de segurança.

5. **Estimativas das quantidades para contratação, acompanhadas de memórias de cálculo e dos documentos que lhe dão suporte**

A estimativa total é de até **30.000 licenças**. Toda contratação de licenças é realizada vinculada a um contrato de fornecimento das mesmas aos clientes.

O processo será dividido em dois lotes com as seguintes quantidades:

- **LOTE 1 (Licenças Básicas - Kaspersky Next EDR Foundations):**
  - **Quantidade Inicial:** 1.000 (mil) licenças.
  - **Pedidos Adicionais:** de no mínimo 100 (cem) licenças.
  - **Total Lote 1:** 10.000 (dez mil) licenças.
  - Esta quantidade é destinada à expansão de pedidos de clientes que já utilizam a solução Kaspersky.
- **LOTE 2 (Licenças Avançadas - EDR ou XDR):**
  - **Quantidade Inicial:** 1.000 (mil) licenças para estações de trabalho Windows.
  - **Pedidos Adicionais:** de no mínimo 100 (cem) licenças.
  - **Total Lote 2:** 20.000 (vinte mil) licenças.
  - **Distribuição das 20.000 licenças:**
    - 1.000 (mil) licenças para sistemas operacionais Windows Server.
    - 500 (quinhentas) licenças para sistemas operacionais Linux.
    - 18.500 (dezoito mil e quinhentas) licenças para estações Windows.
  - Esta quantidade é destinada à captação de clientes para uma nova solução de EDR ou XDR e adoção em ambiente Data Center.

6. Levantamento mercadológico

Lote 1: Renovação de Licenças Kaspersky Existentes: A Kaspersky é reconhecida como líder em cibersegurança, com prêmios em detecção de malware, prevenção de ataques direcionados e baixo impacto no desempenho do sistema, conforme avaliação da AV-Comparatives. A solução atual, utilizada pelos clientes, oferece proteção robusta contra malwares, ransomwares e outras ameaças, com alta taxa de detecção e integração com plataformas existentes, o que minimiza custos de substituição e treinamento.

A renovação das licenças Kaspersky existentes é necessária para manter a continuidade da proteção já implementada nos ambientes dos clientes do CIASC, evitando interrupções no serviço de segurança cibernética, mudança de solução durante a vigência do contrato com os clientes e garantindo a conformidade com os padrões de proteção estabelecidos. A renovação das licenças existentes permite a continuidade operacional, aproveitamento de dias remanescentes das licenças em uso, facilidade de renovação (realizada remotamente) e manutenção da confiabilidade na solução, já comprovada pelo CIASC e seus clientes.

Lote 2: Contratação de Solução XDR: **A contratação de uma solução de Detecção e Resposta Estendida (XDR) é necessária para complementar o portfólio de segurança do**

CIASC, atendendo à crescente complexidade das ameaças cibernéticas e às demandas por maior visibilidade e resposta integrada em ambientes híbridos e multicloud, com foco na proteção de serviços e ambientes críticos. Instituições como Gartner e Forrester recomendam a adoção de soluções XDR para enfrentar desafios como a conformidade com a LGPD e a proteção de infraestruturas críticas. A solução XDR amplia a proteção além dos endpoints, integrando dados de redes, e-mails, servidores e ambientes de nuvem, com uso de inteligência artificial (IA) e aprendizado de máquina (ML) para reduzir falsos positivos e acelerar respostas a incidentes. A contratação de uma solução XDR, complementa as licenças EDR existentes ao expandir a proteção para camadas adicionais da infraestrutura, garantindo maior resiliência contra ciberataques sofisticados e alinhamento com as tendências de mercado observadas no Brasil.

7. Estimativa do valor da contratação

O valor estimado é de R$ 95,00 por dispositivo/12 meses. O valor total estimado da contratação é de R$ 2.850.000,00 (dois milhões e oitocentos e cinquenta mil reais) para 30.000 licenças, considerando um período de 12 meses.

8. Comparativo das soluções

Tipos de Soluções Disponíveis: EDR e XDR

1. Detecção e Resposta de Endpoint (EDR): Soluções EDR concentram-se na proteção de dispositivos finais (endpoints), como computadores, laptops, servidores e dispositivos móveis. Elas monitoram continuamente as atividades nos endpoints, coletando dados sobre processos, tráfego de rede, comportamento do usuário e eventos do sistema para detectar e responder a ameaças cibernéticas.

Funcionalidades Principais:

- Monitoramento contínuo em tempo real de endpoints.
- Análise comportamental e detecção de ameaças baseadas em indicadores de comprometimento (IoCs) e indicadores de comportamento (IoBs).
- Resposta automatizada, como isolamento de dispositivos comprometidos e remediação de ameaças.
- Ferramentas forenses para investigação detalhada de incidentes.

- Integração com inteligência de ameaças para contextualizar ataques.

2. Detecção e Resposta Estendida (XDR): O XDR é uma evolução do EDR, integrando dados de múltiplas camadas de segurança, como endpoints, redes, e-mails, servidores, workloads em nuvem e aplicações. Utiliza inteligência artificial (IA) e aprendizado de máquina (ML) para correlacionar eventos e oferecer uma abordagem holística de detecção e resposta.

- Funcionalidades Principais:
  - Coleta e correlação de dados de endpoints, redes, e-mails, nuvens e outras fontes.
  - Visibilidade unificada em um console centralizado.
  - Automação avançada para detecção, priorização e resposta a ameaças.
  - Integração com frameworks como MITRE ATT&CK para mapeamento de ataques.
  - Análise de tráfego de rede (NTA) e verificação de segurança em ambientes híbridos e multicloud.

Vantagens e Desvantagens

Solução	Vantagens	Desvantagens
EDR	- Alta proteção para endpoints - Resposta rápida a ameaças - Custo acessível	- Escopo limitado a endpoints - Mais falsos positivos - Exige expertise técnica - Impacto no desempenho de dispositivos
XDR	- Visibilidade holística - Correlação avançada com IA/ML - Resposta automatizada - Ideal para ambientes híbridos - Conformidade com LGPD	- Custo elevado - Integração complexa - Requer infraestrutura madura - Curva de aprendizado

As soluções EDR e XDR são complementares, mas atendem a diferentes níveis de maturidade e necessidades de segurança. O EDR é uma escolha sólida para proteção focada em endpoints, enquanto o XDR oferece uma abordagem mais abrangente, integrando múltiplas camadas de segurança para maior resiliência contra ameaças sofisticadas. A decisão entre EDR e XDR deve considerar o tamanho da organização, a complexidade da infraestrutura de TI, o nível de expertise da equipe de segurança e os requisitos regulatórios.

9. Descrição da solução escolhida

A solução escolhida é a renovação e aquisição de licenças de uma solução de tecnologia da informação para proteção de computadores contra software malicioso (malware), antivírus básico e avançado seguindo a tendência do mercado com soluções de segurança mais modernas e robustas (EDR ou XDR), com gerenciamento centralizado para ambiente corporativo, suporte técnico, migração/atualização e treinamento.

O lote 2 compreende um novo produto a ser incluído no portifólio de segurança do CIASC, com uma solução de segurança avançada e integrada, focado em aplicações e serviços críticos.

Será uma contratação de software e serviços, com despesas vinculadas aos contratos de fornecimento de licenças e suporte.

• **LOTE 1:** Focado na solução Kaspersky Next EDR Foundations para atender a demanda de clientes que já a utilizam.

• **LOTE 2:** Direcionado a uma nova solução de EDR ou XDR, visando a captação de novos clientes, com requisitos técnicos mínimos específicos para detecção, prevenção, resposta, investigação, arquitetura e gerenciamento.

A duração das licenças será de 12 meses a contar da data de fornecimento de cada pedido. A solução engloba proteção contra diversos tipos de ameaças, gerenciamento centralizado para facilitar a administração e visibilidade, e um agente leve para minimizar o impacto no desempenho.

10. Justificativas para o parcelamento ou não da contratação

A contratação será **dividida em dois lotes**. Esta decisão se justifica pela necessidade de atender a duas frentes distintas:

1. **LOTE 1:** Para a expansão e continuidade do serviço para clientes que já utilizam a solução Kaspersky, devido à incompatibilidade operacional entre diferentes fabricantes de antivírus, o que permite a manutenção da solução atual para essa base de clientes.

2. **LOTE 2:** Para a captação de novos clientes e a possibilidade de introduzir uma nova solução de EDR ou XDR, ampliando as opções tecnológicas oferecidas e a competitividade do mercado. Este lote é composto de uma solução mais avançada, atendendo às necessidades específicas de cada grupo de clientes.

11. Contratações correlatas e/ou interdependentes

A contratação de licenças de segurança está diretamente correlacionada à capacidade do CIASC de atuar como fornecedor de Tecnologia da Informação para diversos clientes do estado e municípios, bem como para a segurança de seus próprios servidores e estações de trabalho. A continuidade da prestação de serviços de TI do CIASC aos seus clientes e a proteção de sua própria infraestrutura são interdependentes da disponibilidade e atualização

dessas licenças. Não há outras aquisições de materiais ou reformas explicitamente necessárias mencionadas nos documentos. A capacitação da equipe técnica, por meio de treinamento para 8 pessoas, é uma ação correlata prevista para a efetividade da solução, especialmente no LOTE 2.

12. **Providências a serem adotadas pela Administração previamente à celebração do contrato**

As providências a serem adotadas incluem:

• **Transferência de Conhecimento e Treinamento:** Em caso de o vencedor do LOTE 2 apresentar uma solução diferente da atual, está previsto treinamento para 8 pessoas da equipe técnica do CIASC, repasse de conhecimento e implantação da console centralizada da nova solução.

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

• **Comunicação:** Caso a solução seja composta apenas por software sem equipamento físico, as tratativas de entrega podem ser realizadas via e-mail. Para equipamentos físicos, a entrega será na sede do CIASC no bairro Itacorubi, em Florianópolis.

13. **Possíveis impactos ambientais e respectivas medidas mitigadoras**

As informações fornecidas nos documentos não contêm detalhes sobre possíveis impactos ambientais da contratação ou as respectivas medidas mitigadoras.

14. **Resultados pretendidos**

Os resultados pretendidos com a contratação são:

• A manutenção e ampliação da capacidade técnica de entrega de serviço de detecção de ameaças, tanto básica quanto avançada, nos dispositivos do CIASC, incluindo servidores no Data Center.

• A garantia da continuidade dos serviços de segurança já fornecidos aos clientes do CIASC e a disponibilidade de captação de novos clientes.

• Manter a segurança consolidada, como demonstrado pela ausência de incidentes de segurança (vírus, malwares, ransomwares) nas máquinas que utilizam a solução atual.

• Fortalecer a postura de segurança da informação da instituição e contribuir significativamente para sua resiliência cibernética.

• Para o Lote 1, garantir a entrega das licenças Kaspersky Next Foundations e suporte técnico.

• Para o Lote 2, garantir a entrega das licenças EDR ou XDR, suporte técnico e treinamento para a equipe.

15. **Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina**

Diante da necessidade imperativa de manutenção e renovação das licenças disponíveis para a solução de antivírus dos clientes do CIASC e do Data Center, a aquisição é considerada necessária e adequada nos parâmetros e quantitativos solicitados. A solução proposta atende à demanda e é fundamental para a segurança cibernética e a continuidade dos serviços prestados.

16. Vantajosidade comercial da contratação

A contratação apresenta vantajosidade comercial para o CIASC, que atua como fornecedor de Tecnologia da Informação para diversos clientes do estado e municípios. O registro de preço para a solução de antivírus e segurança de endpoint e servidores permitirá a renovação e o suporte de licenças já instaladas no parque de máquinas dos clientes do CIASC, além de viabilizar a captação de novos clientes para uma nova solução de EDR ou XDR. Ao garantir a continuidade e a expansão da oferta desse serviço essencial de segurança, o CIASC fortalece sua posição no mercado, mantém sua base de clientes e tem potencial para atrair novos contratos, contribuindo diretamente para sua viabilidade econômica e operacional.