CONSELHO DE ARQUITETURA E URBANISMO - SP

Estudo Técnico Preliminar 23/2026

1. Informações Básicas

Número do processo: 00179.000412/2026-55

2. Descrição da necessidade

Aquisição de solução de segurança EDR (Endpoint Detection and Response) para a proteção de endpoints.

O CAU/SP encontra-se exposto a riscos relevantes de segurança da informação, como ataques cibernéticos, ransomware, vazamento de dados e indisponibilidade de serviços.

A contratação de uma solução EDR (Endpoint Detection and Response) visa:

- proteger estações de trabalho e servidores
- detectar ameaças conhecidas e desconhecidas
- responder automaticamente a incidentes
- garantir continuidade dos serviços institucionais

3. Área requisitante

Área Requisitante	Responsável
Coordenação de TIC	Julian Moya Gomez
Coordenação de TIC	Thiago Pereira Machado
Assessoria Chefe de Tecnologia, Inovação e Digital	Laercio Correa Lourenço

4. Necessidades de Negócio

Considerando que o CAU/SP não possui atualmente solução especializada de segurança de endpoints (EDR), identifica-se a necessidade de adoção de mecanismos tecnológicos capazes de elevar o nível de proteção do ambiente computacional corporativo, mitigando riscos operacionais, cibernéticos e institucionais.

A ausência de solução dedicada compromete a capacidade de:

- prevenção, detecção e resposta a ameaças avançadas;
- monitoramento contínuo do ambiente de TI;
- atuação proativa diante de incidentes de segurança;

Nesse contexto, a contratação de solução de segurança de endpoints visa atender às seguintes necessidades de negócio:

- Garantir a segurança da rede corporativa do CAU/SP, protegendo estações de trabalho, servidores e demais dispositivos contra ameaças cibernéticas, incluindo ataques sofisticados e persistentes;
- Preservar a integridade, confidencialidade e disponibilidade das informações institucionais, assegurando a proteção de dados sensíveis e estratégicos;
- Assegurar a continuidade operacional dos serviços institucionais, reduzindo riscos de indisponibilidade decorrentes de incidentes de segurança da informação;
- Elevar o nível de maturidade em segurança da informação, por meio da implementação de solução capaz de realizar monitoramento contínuo, detecção comportamental e resposta automatizada a incidentes;

- Atender às exigências legais e regulatórias, especialmente no que se refere à Lei Geral de Proteção de Dados Pessoais (LGPD), bem como às boas práticas de governança e segurança da informação na Administração Pública;
- Reduzir riscos financeiros, operacionais e reputacionais, decorrentes de possíveis violações de segurança, vazamentos de dados ou interrupções de serviços;
- Possibilitar maior capacidade de gestão e visibilidade do ambiente de endpoints, permitindo atuação centralizada, geração de relatórios e suporte à tomada de decisão estratégica pela área de TI.

5. Necessidades Tecnológicas

Considerando a inexistência de solução especializada de segurança de endpoints no ambiente do CAU/SP, faz-se necessária a adoção de solução tecnológica capaz de prover proteção avançada, monitoramento contínuo e resposta a incidentes de segurança da informação.

A solução a ser contratada deverá contemplar, de forma integrada:

- detecção de ameaças conhecidas e desconhecidas por meio de técnicas como análise comportamental, heurística e aprendizado de máquina;
- monitoramento contínuo dos endpoints, com coleta de telemetria e visibilidade centralizada do ambiente;
- capacidade de resposta a incidentes, incluindo ações remotas e automatizadas;
- gerenciamento centralizado por meio de console unificada, com controle de políticas e geração de relatórios;
- integração com outras ferramentas de segurança da informação, como soluções de SIEM e mecanismos de correlação de eventos;
- operação em ambientes híbridos (nuvem e/ou on-premise), garantindo escalabilidade e alta disponibilidade;
- compatibilidade com os principais sistemas operacionais utilizados pelo CAU/SP.

6. Demais requisitos necessários e suficientes à escolha da solução de TIC

Além das necessidades de negócio e tecnológicas já definidas, a solução de segurança de endpoints a ser contratada pelo CAU/SP deverá atender a requisitos complementares indispensáveis para garantir sua adequada seleção, implantação e operação no ambiente institucional.

Nesse sentido, destacam-se os seguintes requisitos adicionais:

Requisitos de desempenho e eficiência

A solução deverá apresentar baixo impacto no desempenho dos endpoints, garantindo operação eficiente mesmo durante atividades de varredura e monitoramento contínuo, de forma a não comprometer a produtividade dos usuários.

Requisitos de disponibilidade e continuidade

A solução deverá garantir alta disponibilidade dos serviços, com mecanismos de redundância, resiliência e continuidade operacional, especialmente em ambientes baseados em nuvem, assegurando níveis mínimos de serviço (SLA).

Requisitos de segurança da solução

A solução deverá atender a padrões reconhecidos de segurança da informação, incluindo:

- proteção contra tentativas de desativação ou adulteração (autoproteção);
- uso de comunicação segura (ex: criptografia TLS);
- controle de acesso com autenticação forte (ex: MFA);
- registro e auditoria de eventos (logs);

Requisitos de integração e interoperabilidade

A solução deverá possibilitar integração com o ecossistema de segurança existente ou futuro do CAU/SP, incluindo:

- ferramentas de SIEM;
- sistemas de gestão de identidades (AD/LDAP);
- APIs e mecanismos de exportação de dados;

Requisitos de escalabilidade

A solução deverá suportar crescimento do ambiente computacional do CAU/SP, permitindo expansão do número de endpoints monitorados sem degradação de desempenho.

Requisitos de suporte e atualização

A contratação deverá incluir:

- suporte técnico especializado;
- atualizações contínuas da solução (engine, assinaturas e funcionalidades);
- correções de vulnerabilidades;

Requisitos de auditoria e rastreabilidade

A solução deverá garantir:

- registro detalhado de eventos e ações realizadas;
- trilha de auditoria para fins de controle e conformidade;
- possibilidade de exportação de logs para análise externa;

Requisitos de conformidade legal

A solução deverá estar em conformidade com:

- Lei Geral de Proteção de Dados Pessoais (LGPD);
- normas de segurança da informação aplicáveis à Administração Pública;

Requisitos de implantação e operação

A solução deverá:

- permitir implantação remota e centralizada;
- suportar operação offline por período mínimo;
- possibilitar gerenciamento simplificado por equipe interna.

7. Estimativa da demanda - quantidade de bens e serviços

Com base no inventário do parque tecnológico do CAU/SP, estima-se que a solução de segurança deverá atender a 400 (quatrocentos) dispositivos.

8. Levantamento de soluções

SOLUÇÃO 1 – MANUTENÇÃO DO CENÁRIO ATUAL

SOLUÇÃO 2 – AQUISIÇÃO DE ANTIVÍRUS TRADICIONAL

SOLUÇÃO 3 – SOLUÇÃO EDR (ENDPOINT DETECTION AND RESPONSE)

SOLUÇÃO 4 – UTILIZAÇÃO DE FERRAMENTAS OPEN SOURCE

SOLUÇÃO 5 – ADESÃO À ATA DE REGISTRO DE PREÇOS

9. Análise comparativa de soluções

SOLUÇÃO 1 – MANUTENÇÃO DO CENÁRIO ATUAL

Consiste na manutenção do ambiente atual, sem a adoção de solução especializada de segurança de endpoints (EDR), permanecendo apenas com mecanismos básicos de proteção eventualmente existentes.

Análise técnica

- inexistência de monitoramento contínuo de ameaças
- ausência de detecção comportamental
- inexistência de resposta automatizada a incidentes
- baixa visibilidade do ambiente de TI

Riscos

- alta exposição a ataques cibernéticos (ransomware, APTs)
- risco de indisponibilidade de sistemas
- potencial vazamento de dados institucionais
- comprometimento da conformidade com LGPD

Conclusão

Alternativa tecnicamente inadequada, pois não atende às necessidades mínimas de segurança da informação do CAU/SP.

SOLUÇÃO 2 – AQUISIÇÃO DE ANTIVÍRUS TRADICIONAL

Consiste na contratação ou utilização de soluções tradicionais de antivírus (Endpoint Protection Platform – EPP), baseadas predominantemente em assinaturas e detecção reativa.

Análise técnica

- detecção baseada principalmente em assinaturas
- baixa capacidade de identificar ameaças desconhecidas
- ausência ou limitação de recursos de investigação (threat hunting)
- inexistência de resposta automatizada e orquestrada

Limitações

- incapacidade de lidar com ataques modernos (fileless, exploits avançados)
- ausência de visibilidade detalhada (telemetria)
- baixa capacidade de correlação de eventos

Conclusão

Alternativa parcialmente adequada, porém insuficiente para atender às necessidades atuais de segurança do CAU/SP.

SOLUÇÃO 3 – SOLUÇÃO EDR (ENDPOINT DETECTION AND RESPONSE)

Consiste na contratação de solução avançada de segurança de endpoints (EDR), capaz de realizar detecção, investigação e resposta a incidentes de forma integrada e contínua.

Análise técnica

A solução EDR caracteriza-se por:

- detecção de ameaças conhecidas e desconhecidas
- coleta contínua de telemetria
- correlação de eventos de segurança
- investigação de incidentes (RCA e kill chain)
- resposta automatizada e remota

Benefícios

- elevada capacidade de detecção (inclusive ameaças avançadas)
- resposta rápida a incidentes
- visibilidade completa do ambiente
- integração com ferramentas de segurança
- melhoria da governança de TI

Considerações

- maior custo em relação às soluções tradicionais
- necessidade de equipe minimamente capacitada

Conclusão

Alternativa tecnicamente adequada e recomendada, por atender integralmente às necessidades do CAU/SP.

SOLUÇÃO 4 – UTILIZAÇÃO DE FERRAMENTAS OPEN SOURCE

Consiste na adoção de soluções de segurança baseadas em software livre ou gratuito, combinando múltiplas ferramentas para suprir funcionalidades de EDR.

Análise técnica

- necessidade de integração manual de múltiplas ferramentas
- ausência de solução unificada
- dependência de conhecimento técnico avançado

Limitações

- ausência de suporte técnico especializado
- maior tempo de implantação e manutenção
- risco de inconsistência na operação

Conclusão

Alternativa tecnicamente limitada e operacionalmente onerosa, não recomendada para o contexto do CAU/SP.

SOLUÇÃO 5 – ADESÃO À ATA DE REGISTRO DE PREÇOS

Consiste na adesão a ata de registro de preços vigente para contratação de solução de segurança de endpoints.

Análise técnica

- possibilidade de contratação mais célere
- redução do esforço administrativo

Riscos

- solução pode não atender integralmente aos requisitos do CAU/SP
- limitação na customização da solução
- dependência de especificações de outro órgão

Conclusão

Alternativa viável sob o aspecto administrativo, porém dependente de análise de aderência técnica.

Conclusão do Levantamento

A solução de Endpoint Detection and Response (EDR) apresenta-se como a alternativa mais adequada para o CAU/SP, por ser a única capaz de atender de forma integral aos requisitos técnicos, operacionais e de segurança da informação identificados no presente Estudo Técnico Preliminar.

10. Registro de soluções consideradas inviáveis

No processo de levantamento de soluções, foram identificadas alternativas tecnológicas que, embora existentes e aplicáveis em determinados contextos, não se mostraram adequadas para atendimento das necessidades específicas do CAU/SP, considerando os requisitos técnicos, operacionais e de segurança da informação estabelecidos neste Estudo Técnico Preliminar.

Manutenção do cenário atual (não contratação)

A alternativa de manutenção do cenário atual não foi considerada inviável em termos absolutos, porém foi classificada como inadequada, tendo em vista que:

- não atende aos requisitos mínimos de segurança da informação;
- não possibilita monitoramento contínuo e resposta a incidentes;
- mantém o ambiente exposto a riscos elevados;

Assim, embora possível, não é compatível com o nível de proteção requerido pelo CAU/SP.

Utilização de ferramentas open source ou gratuitas

A adoção de soluções open source não é inviável tecnicamente, podendo ser adequada em ambientes com alta maturidade operacional. Entretanto, foi considerada inadequada ao CAU/SP, em razão de:

- elevada complexidade de integração e operação;
- dependência de equipe altamente especializada;
- ausência de suporte corporativo estruturado;

Assim, embora possível, não se mostra adequada ao contexto institucional atual.

Adoção de solução por adesão à ata de registro de preços

A adesão a atas de registro de preços também não é inviável e pode representar alternativa válida em determinados cenários. Contudo, foi considerada inadequada como estratégia principal, pois:

- não foram encontradas atas federais para adesão;
- depende de especificações elaboradas por terceiros;

Dessa forma, sua utilização deve ser condicionada à análise de compatibilidade, não sendo a alternativa mais adequada neste momento.

11. Análise comparativa de custos (TCO)

A análise comparativa de custos foi realizada considerando o Custo Total de Propriedade (TCO) das soluções avaliadas, abrangendo não apenas o custo direto de aquisição, mas também custos indiretos relacionados à implantação, operação, suporte e riscos associados.

Para fins de comparação, foram consideradas as seguintes premissas:

- horizonte de análise: 36 meses (padrão adotado nas contratações analisadas);
- cobertura integral dos endpoints do CAU/SP;
- inclusão de custos diretos e indiretos;
- consideração de riscos operacionais e de segurança;

O custo total das soluções foi avaliado com base nos seguintes elementos:

- custos de licenciamento/subscrição;
- custos de implantação e configuração;
- custos de suporte técnico e atualizações;
- custos operacionais (gestão e administração da solução);
- custos indiretos (treinamento, integração, manutenção);
- custos associados a riscos (incidentes de segurança, indisponibilidade);

Análise por Solução

Manutenção do cenário atual
Custo direto: inexistente
Custo indireto: elevado

Considerações:

- alto risco de incidentes de segurança
- potencial impacto financeiro elevado (ransomware, indisponibilidade)

Conclusão: Menor custo aparente, porém maior custo total (TCO) devido aos riscos envolvidos.

Antivírus tradicional (EPP)
Custo direto: baixo a moderado
Custo indireto: moderado

Considerações:

- necessidade de complementação com outras ferramentas
- baixa eficácia contra ameaças avançadas

Conclusão: Custo inicial reduzido, porém TCO elevado por ineficiência técnica.

Solução EDR

Custo direto: moderado a elevado
Custo indireto: baixo a moderado

Considerações:

- solução integrada (reduz necessidade de múltiplas ferramentas)
- maior eficiência na prevenção e resposta a incidentes
- redução de riscos operacionais

Conclusão: Maior investimento inicial, porém melhor relação custo-benefício no TCO.

Soluções open source
Custo direto: baixo
Custo indireto: elevado

Considerações:

- necessidade de equipe especializada
- alto custo operacional e de manutenção
- maior tempo de implantação

Conclusão: Custo inicial baixo, porém TCO elevado devido à complexidade operacional.

Adesão à ata
Custo direto: variável
Custo indireto: variável

Considerações:

- possível economia administrativa
- risco de indisponibilidade ou inexistência

Conclusão: Viabilidade condicionada, com TCO incerto.

12. Descrição da solução de TIC a ser contratada

A solução de TIC a ser contratada consiste na prestação de serviço continuado de segurança de endpoints, por meio do fornecimento de solução do tipo Endpoint Detection and Response (EDR), incluindo licenciamento/subscrição, implantação, configuração, gerenciamento centralizado, suporte técnico especializado, atualização tecnológica e garantia de funcionamento durante toda a vigência contratual.

A solução deverá prover proteção avançada para estações de trabalho, servidores e demais endpoints do ambiente computacional do CAU/SP, contemplando mecanismos integrados de prevenção, detecção, investigação e resposta a incidentes de segurança da informação, com gerenciamento centralizado por meio de console unificada.

A contratação deverá contemplar, no mínimo, os seguintes componentes e funcionalidades:

- proteção contra malwares, ransomwares, exploits, ameaças fileless, ataques avançados e ameaças desconhecidas;
- detecção baseada em múltiplas camadas, incluindo assinaturas, heurística, análise comportamental e machine learning;
- monitoramento contínuo dos endpoints com coleta de telemetria e correlação de eventos de segurança;
- funcionalidades de Endpoint Detection and Response (EDR), incluindo investigação de incidentes, análise de causa raiz (RCA), reconstrução de cadeia de ataque (kill chain) e threat hunting;
- resposta automatizada e remota a incidentes, incluindo isolamento de dispositivos, bloqueio de ameaças e ações de contenção;
- gerenciamento centralizado por meio de console web unificada;
- integração com serviços de diretório, ferramentas SIEM e APIs de integração;
- controle de aplicações, dispositivos USB, navegação web e políticas de segurança;
- funcionalidades de firewall, prevenção de intrusão (HIPS) e proteção contra alterações indevidas;
- geração de logs, relatórios, dashboards e trilhas de auditoria;
- atualização contínua de assinaturas, motores de detecção e funcionalidades da solução;
- suporte técnico especializado e garantia de atualização tecnológica durante toda a vigência contratual.

A solução deverá possuir compatibilidade com os principais sistemas operacionais utilizados pelo CAU/SP, incluindo ambientes Windows, Linux e macOS, bem como suportar operação em ambientes híbridos, cloud e/ou on-premise, garantindo escalabilidade, disponibilidade e segurança operacional.

A contratação deverá prever, ainda, serviços especializados de implantação e configuração inicial da solução, incluindo apoio técnico para instalação dos agentes, parametrização de políticas, integração com o ambiente corporativo e transferência de conhecimento à equipe técnica do CAU/SP.

A solução deverá operar de forma integrada e centralizada, permitindo gestão simplificada, visibilidade completa do ambiente de endpoints e suporte às atividades de governança, conformidade e resposta a incidentes de segurança da informação.

13. Estimativa de custo total da contratação

Valor (R$): 102.133,33

Inicialmente, a estimativa de custo total da contratação foi elaborada com base em pesquisa de mercado realizada junto a empresas especializadas no fornecimento de soluções de segurança de endpoints do tipo Endpoint Detection and Response (EDR), observando-se os princípios da economicidade, razoabilidade e vantajosidade para a Administração Pública.

Além das propostas comerciais obtidas junto ao mercado, foram também analisados preços praticados em contratações similares realizadas por órgãos da Administração Pública, identificadas por meio de pesquisa no Portal Nacional de Contratações Públicas (PNCP), em processos já homologados envolvendo soluções de segurança de endpoints com características compatíveis ao objeto pretendido pelo CAU/SP.

Pesquisa de Preços

	Quantidade	Valor Unitário	Valor Total
Empresa 1	400	R$ 337,74	R$ 135.096,00
Empresa 2	400	R$ 350,00	R$ 140.000,00
Empresa 3	400	R$ 162,49	R$ 64.996,00
Empresa 4	400	R$ 255,00	R$ 102.000,00
Empresa 5	400	R$ 195,00	R$ 78.000,00
Média		R$ 260,05	R$ 104.018,40

Após a Manifestação Jurídica 071/2026 que compõe o processo, com a recomendação de revisar os valores e os serviços contemplados, segue tabela atualizada com a estimativa de custo total.

Pesquisa de Preços

	Quantidade	Valor Unitário	Valor Total
Empresa 1	400	R$ 299,00	R$ 119.600,00
Empresa 2	400	R$ 255,00	R$ 102.000,00
Empresa 3	400	R$ 212,00	R$ 84.800,00
Média		R$ 255,33	R$ 102.133,33

14. Justificativa técnica da escolha da solução

A escolha da solução de segurança de endpoints do tipo Endpoint Detection and Response (EDR) fundamenta-se na análise comparativa das alternativas disponíveis, considerando os requisitos técnicos, operacionais e de segurança da informação necessários ao atendimento das demandas do CAU/SP.

Conforme demonstrado no levantamento de soluções e na análise de custo total de propriedade (TCO), a solução EDR é a única capaz de atender de forma integral às necessidades identificadas, especialmente no que se refere à proteção contra ameaças cibernéticas avançadas, monitoramento contínuo e resposta a incidentes.

Adequação aos requisitos técnicos

A solução EDR apresenta aderência integral aos requisitos tecnológicos definidos no ETP, destacando-se por:

- capacidade de detecção de ameaças conhecidas e desconhecidas, por meio de técnicas avançadas como análise comportamental e aprendizado de máquina;
- coleta contínua de telemetria e visibilidade ampliada do ambiente de endpoints;
- possibilidade de investigação detalhada de incidentes, incluindo análise de causa raiz e reconstrução de cadeias de ataque;
- execução de ações de resposta automatizada e remota, reduzindo o tempo de contenção de incidentes;

Superioridade em comparação com as demais alternativas

As demais soluções analisadas foram consideradas inadequadas ao contexto do CAU/SP pelos seguintes motivos:

- soluções baseadas apenas em antivírus tradicional não atendem às demandas atuais de segurança, por apresentarem limitações na detecção de ameaças avançadas;
- soluções open source demandam elevado esforço operacional e não oferecem suporte corporativo adequado;
- a manutenção do cenário atual não proporciona nível mínimo de proteção;
- a adesão a atas não garante atendimento aos requisitos técnicos específicos do órgão e depende da imediata disponibilidade de alguma vigente;

Dessa forma, a solução EDR se destaca como a alternativa mais completa e eficiente.

Além disso, a adoção da solução EDR proporciona benefícios relevantes, como:

- aumento da maturidade em segurança da informação;
- redução de riscos operacionais e de incidentes cibernéticos;
- melhoria na capacidade de resposta e mitigação de ameaças;
- centralização da gestão de segurança dos endpoints;
- suporte à tomada de decisão por meio de relatórios e indicadores.

15. Justificativa econômica da escolha da solução

Sob a ótica econômica, a escolha da solução de segurança de endpoints do tipo Endpoint Detection and Response (EDR) mostra-se a mais vantajosa para o CAU/SP, considerando não apenas o custo inicial de contratação, mas principalmente o custo total de propriedade (TCO) ao longo do período de vigência contratual. Embora apresente investimento inicial superior às alternativas mais simples, como antivírus tradicional, a solução EDR proporciona maior eficiência operacional e reduz significativamente os riscos associados a incidentes de segurança da informação.

Adicionalmente, a adoção de uma solução integrada de EDR contribui para a racionalização de custos, ao evitar a necessidade de aquisição e manutenção de múltiplas ferramentas isoladas para suprir funcionalidades distintas. Essa integração reduz custos indiretos relacionados à gestão, operação e suporte, além de otimizar o tempo de resposta a incidentes, minimizando impactos financeiros decorrentes de indisponibilidade de sistemas ou comprometimento de dados institucionais.

Por fim, a solução EDR alinha-se ao princípio da economicidade previsto na Lei nº 14.133/2021, ao proporcionar a melhor relação custo-benefício entre as alternativas avaliadas, considerando o equilíbrio entre investimento, desempenho e mitigação de riscos. Dessa forma, a escolha da solução não se fundamenta no menor preço imediato, mas na seleção da proposta mais vantajosa para a Administração Pública, em termos de eficiência, segurança e sustentabilidade econômica da contratação.

16. Justificativa para o parcelamento ou não

A solução de segurança de endpoints (EDR) a ser contratada não se mostra tecnicamente adequada ao parcelamento, por tratar-se de uma plataforma integrada, cujas funcionalidades são interdependentes e operam de forma unificada por meio de agente e console centralizados. O fracionamento da contratação poderia comprometer a eficiência da solução, gerar incompatibilidades técnicas e dificultar a gestão e a operação do ambiente de segurança da informação.

Adicionalmente, a contratação de forma unificada contribui para a padronização tecnológica, simplificação da gestão contratual e garantia de níveis adequados de serviço, incluindo suporte técnico, atualização contínua e resposta a incidentes. O parcelamento, nesse contexto, poderia resultar em aumento de custos operacionais, sobreposição de funcionalidades e maior complexidade na integração entre diferentes soluções.

Dessa forma, conclui-se que a contratação em item único representa a alternativa mais vantajosa para a Administração, assegurando eficiência, economicidade e melhor desempenho da solução, em consonância com os princípios estabelecidos na Lei nº 14.133/2021.

17. Contratações Correlatas ou Interdepentes

Não existem contratações correlatas ou interdependentes em relação ao objeto deste estudo.

18. Benefícios a serem alcançados com a contratação

A contratação de solução de segurança de endpoints do tipo Endpoint Detection and Response (EDR) proporcionará significativa elevação do nível de maturidade em segurança da informação no âmbito do CAU/SP, permitindo a adoção de mecanismos avançados de detecção, investigação e resposta a incidentes cibernéticos. Com isso, espera-se a redução substancial da exposição a ameaças digitais, contribuindo para a proteção dos ativos tecnológicos e das informações institucionais.

Além disso, a solução possibilitará maior visibilidade e controle sobre o ambiente de TI, por meio de monitoramento contínuo, centralização da gestão e geração de informações estratégicas para tomada de decisão. Esses fatores contribuirão para o aumento da eficiência operacional da área de tecnologia, reduzindo o tempo de resposta a incidentes e melhorando a disponibilidade dos serviços institucionais.

Por fim, a adoção da solução EDR contribuirá para a mitigação de riscos operacionais, financeiros e reputacionais, bem como para o atendimento às exigências legais e normativas relacionadas à proteção de dados e segurança da informação. Dessa forma, a contratação se alinha aos princípios da eficiência, economicidade e continuidade dos serviços públicos, promovendo maior segurança e confiabilidade no ambiente tecnológico do CAU/SP.

19. Providências a serem Adotadas

De acordo com a natureza desta contratação, o CAU/SP deve designar funcionários capacitados para o acompanhamento e condução doprocesso licitatório, e para a verificação do cumprimento dos requisitos técnicos do objeto desta contratação.

20. Planejamento da Contratação

A contratação está prevista no Plano Anual de Contratações 2026.

DFD correspondente no PCA: DFD 183/2025 - SEI 803212

21. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

21.1. Justificativa da Viabilidade

A solução é amplamente comercializada e utilizada em empresas, órgãos e instituições na administração pública.

22. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

JULIAN MOYA GOMEZ

Analista de TIC

Assinou eletronicamente em 12/08/2026 às 09:32:24.

THIAGO PEREIRA MACHADO

Coordenador de TIC

Assinou eletronicamente em 12/08/2026 às 10:46:07.