

CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO - ETP-TIC Nº 6/2026/CRA-SP

PROCESSO Nº 476906.000765/2026-33

Elaboração dos Estudos Técnicos Preliminares - ETP - para a aquisição de serviços. O ETP é um documento constitutivo da primeira etapa do planejamento de uma contratação que caracteriza determinada necessidade, descreve as análises realizadas em termos de requisitos, alternativas, escolhas, resultados pretendidos e demais características, dando base ao anteprojeto, ao termo de referência ou ao projeto básico, caso se conclua pela viabilidade da contratação.

Referência Legal:

- a) Lei nº 14.133 DE 1º/04/2021 e suas alterações;
- b) Decreto nº 3.555, de 08/08/2000;
- c) Decreto nº 10.024, de 20/09/2019;
- d) Decreto nº 9.507, de 21 de setembro de 2018;
- e) Instrução Normativa Nº 58, de 8 de agosto de 2022;
- f) Instrução Normativa Nº 65, de 7 de julho de 2021;
- g) Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022;

1. OBJETO

1.1. O objeto deste Estudo Técnico Preliminar consiste na contratação de **Solução Integrada de Segurança Cibernética e Serviços Especializados de Governança e Auditoria**, visando a proteção dos ativos de informação e adequação com a LGPD no âmbito do CRA-SP, dividida em 03 (três) grupos distintos:

1.1.1. **Grupo 1:** Solução de Segurança de Rede e Endpoint (Firewall de Próxima Geração, ZTNA e MDR) sob o modelo de **Hardware as a Service (HaaS)**, incluindo fornecimento, instalação, configuração e suporte técnico;

1.1.2. **Grupo 2:** Serviços de Consultoria em **Governança, Riscos e Conformidade (GRC)** e Gestão de Segurança da Informação;

1.1.3. **Grupo 3:** Serviços de **Auditoria Técnica e Testes de Invasão (Pentest)**, executados de forma independente para validação dos controles implementados.

2. ÁREA REQUISITANTE

Área Requisitante	Responsável
Tecnologia da Informação	Eduardo Sadayoshi Borghi Kondo Assessor de Tecnologia
Infraestrutura Computacional	Ivan Cesar Machado Narcizo Coordenador de Infraestrutura

3. DESCRIÇÃO DA NECESSIDADE (NEGÓCIO E TECNOLOGIA)

3.1. O CRA-SP é uma autarquia federal, organizada na forma de Conselho de Fiscalização Profissional (CFP) que orienta, disciplina e fiscaliza o exercício profissional da área de Administração, matéria de sua competência.

- 3.2. Como prestador de um serviço público, o CRA-SP desenvolve relevantes atividades dentro de sua jurisdição, ou seja, no estado de São Paulo, por meio da fiscalização do exercício profissional. Como os demais Conselhos de Fiscalização Profissional, sua receita é uma verba pública de caráter tributário, usada exclusivamente para a manutenção de suas atividades essenciais.
- 3.3. O CRA-SP é uma entidade dotada de personalidade jurídica de direito público, com autonomia técnica, administrativa e financeira e não recebe nenhuma subvenção do governo federal, tendo todo seu recurso alicerçado nos tributos pagos pelos administradores.
- 3.4. Conforme acima exposto, para que nossas atividades finalísticas sejam bem cumpridas, faz-se necessária a complementação com atividades meio, ou seja, aquelas que possibilitam e criam condições favoráveis para o funcionamento da Entidade.
- 3.5. O CRA-SP possui atualmente uma infraestrutura de segurança baseada em tecnologias legadas (VPNs tradicionais e firewalls de borda simples), que se mostram insuficientes diante da crescente sofisticação de ataques cibernéticos (Ransomwares, Phishing avançado) e da nova realidade de trabalho híbrido. A necessidade fundamenta-se em:
- 3.5.1. Vulnerabilidade Tecnológica: A ausência de inspeção profunda de tráfego criptografado e de ferramentas de detecção e resposta (MDR) expõe os ativos de informação do Conselho a riscos críticos;
- 3.5.2. Mitigar o risco de interrupção dos serviços essenciais prestados pelo CRA-SP à sociedade devido a incidentes de segurança;
- 3.5.3. Gestão de Identidade e Acesso: Com o aumento do trabalho remoto, o modelo de VPN atual é baseado em confiança implícita na rede. A necessidade é migrar para o conceito de Zero Trust Network Access (ZTNA), onde o acesso é concedido por usuário e dispositivo, e não por rede.
- 3.5.4. A contratação de serviços de GRC justifica-se pela necessidade de atender ao princípio da continuidade do serviço público e às diretrizes de governança do Tribunal de Contas da União (TCU), suprimindo a ausência de um Plano de Continuidade de Negócios (PCN) e de indicadores de desempenho (KPIs) de segurança, elementos essenciais para a prestação de contas (Accountability) exigida pelas Instruções Normativas do Governo Federal e pela LGPD.

4. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

- 4.1. Os serviços a serem contratados se enquadram como comuns, haja vista que seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado, bem como continuados, pois a sua interrupção pode comprometer o devido funcionamento das atividades do CRA-SP.
- 4.2. Segurança de Rede (**Grupo 1**): Fornecimento de solução de Firewall NGFW em modelo Hardware as a Service (HaaS), com capacidade de inspeção profunda de pacotes (DPI) e tráfego SSL/TLS (1.3) sem degradação de performance.
- 4.2.1. Proteção de Endpoint e XDR: Implementação de proteção multicamada baseada em IA/Machine Learning, com capacidade de rollback contra Ransomware e gerenciamento 100% em nuvem.
- 4.2.2. Acesso Seguro (ZTNA): Implementação de arquitetura Zero Trust, substituindo a confiança implícita por verificação contínua de identidade e postura do dispositivo.
- 4.2.3. Monitoramento (MDR): Serviço de detecção e resposta 24x7, com tempos de resposta (SLA) rigorosos para incidentes críticos.
- 4.3. Requisitos de Sustentabilidade (GNCS e PNRS):
- 4.3.1. Logística Reversa: No modelo HaaS (**Grupo 1**), a contratada é responsável pelo descarte ambientalmente adequado de equipamentos obsoletos ou substituídos, conforme a Política Nacional de Resíduos Sólidos.
- 4.3.2. Eficiência Energética: Os appliances físicos fornecidos devem possuir certificações de baixo consumo de energia.
- 4.4. Exigência de atestados de capacidade técnica compatíveis com o objeto e comprovação de que a equipe técnica indicada para a execução dos serviços detém **certificações de nível avançado ou especialista (Professional/Expert)**, emitidas pelos fabricantes das soluções ofertadas.

- 4.5. Requisitos do **Grupo 2: Consultoria em GRC (Governança, Riscos e Conformidade)**
- 4.5.1. Diagnóstico de Maturidade: Realização de "Gap Analysis" baseado na ISO/IEC 27001 e 27002 para identificar o estado atual da segurança da informação no CRA-SP.
- 4.5.2. Gestão de Riscos de TIC: Elaboração de inventário de ativos de TI e Matriz de Riscos, identificando ameaças e definindo planos de mitigação tecnológica.
- 4.5.3. Continuidade de Negócios: Desenvolvimento de Plano de Continuidade de Negócios (PCN) e Recuperação de Desastres (DR), com foco na resiliência da infraestrutura de TI.
- 4.5.4. Sustentação da Conformidade: Apoio técnico para garantir que as novas soluções (**Grupo 1**) operem em conformidade com as políticas de segurança e diretrizes de privacidade já estabelecidas pelo Conselho.
- 4.5.5. Transferência de Conhecimento: Realização de treinamentos gravados e entrega de materiais editáveis para a equipe de TI do CRA-SP.
- 4.5.6. Requisitos do **Grupo 3: Auditoria Técnica e Testes de Invasão (Pentest)**
- 4.5.7. Independência Técnica: **Vedação expressa de contratação da mesma empresa vencedora do Grupo 1, garantindo a segregação de funções e a imparcialidade da auditoria.**
- 4.5.8. Realização semestral de Pentests em infraestrutura de rede e aplicações, utilizando metodologias de exploração manual e ferramentas automatizadas.
- 4.5.9. Entrega de relatórios técnicos e executivos contendo a classificação de criticidade dos achados e recomendações de correção.
- 4.5.10. Teste de Re-validação (Retest): Após o prazo de correção pelas equipes técnicas, a contratada deve realizar novo teste para validar se as vulnerabilidades foram sanadas.

5. LEVANTAMENTO DE MERCADO

- 5.1. Para fins de verificação das soluções disponíveis no mercado atual, foram realizadas pesquisas em sites de compras públicas e junto a fornecedores, com o objetivo de identificar quais tipos de soluções têm sido contratadas por outros órgãos.
- 5.2. Nas contratações similares no Painel de Preços da Administração Pública (PNCP), para padronizar as especificações e obter uma estimativa dos valores contratados pela Administração, foram filtradas as compras realizadas nos últimos 12 (doze) meses;
- 5.3. Relação das contratações similares registradas no Portal Nacional de Contratações Públicas, referentes ao objeto em tela:
- 5.4. Neste sentido, com base no levantamento de mercado, foram analisadas **soluções alternativas para cada grupo**, que inicialmente se mostraram tecnicamente viáveis para entrega da solução pretendida, sendo que elas são:
- 5.4.1. **Grupo 1: Solução de Segurança (SASE/MDR)**
- 5.4.1.1. Aquisição Definitiva de Ativos (CAPEX): Compra direta de firewalls físicos, licenças perpétuas e contratação de equipe própria para monitoramento 24x7.
- 5.4.1.2. Inviabilidade: Esta alternativa foi considerada inviável e ineficiente. O alto investimento inicial (desembolso imediato), somado à rápida obsolescência tecnológica do hardware de segurança, geraria um custo de manutenção elevado. Além disso, a dificuldade de contratar e manter especialistas em segurança cibernética 24x7 no quadro próprio do Conselho tornaria a operação vulnerável.
- 5.4.1.3. Security as a Service e Hardware as a Service (OPEX) - **SOLUÇÃO ESCOLHIDA.**
- 5.4.1.4. Viabilidade/Eficiência: Esta é a solução mais eficiente e viável. Ela permite a atualização tecnológica contínua (o hardware é substituído pela contratada se ficar obsoleto), garante monitoramento especializado 24x7 sem inchar a folha de pagamento e alinha os custos ao uso efetivo.
- 5.4.2. **Grupo 2: Consultoria GRC**

5.4.2.1. Execução direta pela equipe interna.

5.4.2.2. Inviabilidade: Esta alternativa mostra-se **inviável e ineficiente**. Primeiro, pela limitação do quadro de pessoal, que já se encontra sobrecarregado com as demandas operacionais e de sustentação da infraestrutura. Segundo, pela ausência de imparcialidade: o desenvolvimento de uma matriz de riscos por quem opera o dia a dia compromete a fidedignidade do diagnóstico, uma vez que o executante tende a relevar falhas de processo que lhe são familiares. Juridicamente, a falta de uma auditoria/consultoria externa pode ser interpretada como fragilidade nos controles internos da autarquia.

5.4.2.3. Contratação de consultoria externa para diagnóstico, mapeamento de riscos e elaboração do Plano de Continuidade de Negócios (PCN) - **SOLUÇÃO ESCOLHIDA**.

5.4.2.4. Esta solução é a mais adequada, pois permite ao CRA-SP absorver o *know-how* de especialistas que detêm *benchmarks* atualizados do setor público e privado. A visão externa é isenta e crítica, essencial para identificar vulnerabilidades que a "**cegueira operacional**" oculta. Além disso, a entrega baseada em produtos garante que o Conselho receba metodologias prontas e testadas (ISO 27001/27002), acelerando a curva de maturidade institucional em governança sem desviar a equipe interna de suas funções finalísticas.

5.4.3. **Grupo 3: Auditoria e Pentest**

5.4.3.1. Realização do Pentest pela mesma empresa do **grupo 1** ou pela equipe interna.

5.4.3.2. Inviabilidade: Esta alternativa é inviável por conflito de interesses. A autocritica técnica é comprometida pelo viés de confirmação, onde o implementador tende a não reportar falhas em seu próprio trabalho. Juridicamente, a execução por parte da empresa do **grupo 1** configuraria uma grave falha de controle interno, expondo o Conselho a riscos residuais não detectados e possíveis sanções por falta de governança.

5.4.3.3. Contratação de pessoa jurídica distinta das demais contratadas (**grupos 1 e 2**) para realizar auditorias técnicas e testes de invasão - **SOLUÇÃO ESCOLHIDA**.

5.4.3.4. Esta é a única solução tecnicamente aceitável. A independência assegura a imparcialidade necessária para identificar falhas que possam ter sido negligenciadas na implementação. Além disso, atende ao Princípio da Segregação de Funções (Art. 5º da Lei nº 14.133/2021) e às recomendações do TCU (Acórdão 2305/2017-Plenário), que veda que o fiscalizador e o executante sejam a mesma entidade, garantindo a fidedignidade dos resultados apresentados à Administração.

5.5. **Conclusão**

5.5.1. Em face do exposto, as soluções citadas como **ESCOLHIDAS** são as mais adequadas.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

6.1. Arquitetura e Integração: A solução foi desenhada sob o conceito de Defesa em Profundidade, estruturada em três pilares complementares que garantem a resiliência tecnológica do CRA-SP:

6.1.1. Pilar de Proteção e Operação (**Grupo 1**): Implementação de uma arquitetura SASE (Secure Access Service Edge) e Zero Trust. O hardware (Firewalls) é fornecido como serviço (HaaS), garantindo que o Conselho tenha sempre tecnologia de ponta. A operação é reforçada pelo serviço de MDR, que provê monitoramento e resposta a incidentes 24x7, suprimindo a carência de equipa interna para vigilância noturna e de fins de semana.

6.1.2. Pilar de Estratégia e Normatização (**Grupo 2**): A consultoria em GRC atuará na camada intelectual, definindo as políticas, analisando riscos e criando o Plano de Continuidade de Negócios (PCN). Esta camada garante que as ferramentas do **grupo 1** estejam alinhadas aos objetivos estratégicos e de adequação (LGPD) do Conselho.

6.1.3. Pilar de Validação e Auditoria (**Grupo 3**): Através de Pentests semestrais, uma empresa

independente testará a eficácia das defesas implementadas no **Grupo 1** e a aderência aos processos do **Grupo 2**, fechando o ciclo de melhoria contínua (PDCA).

6.2. **Modelo de Entrega e Sustentabilidade:** A solução será entregue predominantemente no modelo de Serviço (OpEx). Esta escolha garante a Sustentabilidade Tecnológica (evitando hardware obsoleto parado em inventário) e a Sustentabilidade Ambiental, uma vez que a logística reversa e o descarte de resíduos eletrônicos ficam a cargo da contratada do **Grupo 1**, conforme o Guia Nacional de Contratações Sustentáveis.

6.3. **Transferência de Conhecimento:** Para garantir que o CRA-SP não sofra de "aprisionamento tecnológico" (vendor lock-in), a solução prevê a transferência de conhecimento técnico através de formações gravadas e entrega de documentação técnica exaustiva.

6.4. **Pertinência Técnica:** Ao descrever a solução como um "todo", justificamos porque é que a contratação não pode ser apenas um "antivírus" ou apenas um "firewall" isolado.

7. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

7.1. Quantidade:

7.1.1. Grupo 1

Item	Descrição	CATSER/PDM	Unidade de Medida	Quantidade
1	Appliance NGFW (Hardware + Licenças + Garantia) 36 meses	350949	Unidade	1
2	Licença Endpoint Protection (EPP/EDR/XDR) 36 meses	350949	Pacote com 250	1
3	Licença ZTNA (Zero Trust) 36 meses	350949	Pacote com 120	1
4	Serviço de Instalação, Configuração e Migração (incluindo execução de Plano de Rollback, se necessário)	26972	Serviço	1
5	Serviço de Suporte Técnico e MDR (Mensal) 36 meses	16918	Serviço	1
6	Treinamento e Transferência de Conhecimento	21172	Horas	16

7.1.2. Grupo 2

Item	Descrição	CATSER/PDM	Unidade de Medida	Quantidade
7	Consultoria em GRC: Elaboração de Diagnóstico de Maturidade, Matriz de Riscos e Plano de Continuidade de Negócios (PCN) com revisão anual. (12 meses) - Ciclo I	13781	Serviço	1
8	Ciclo II – Serviço de Suporte Técnico: início após a conclusão do Ciclo I. (24 meses)	16918	Serviço	1

7.1.3. Grupo 3

Item	Descrição	CATSER/PDM	Unidade de Medida	Quantidade 36 meses
------	-----------	------------	-------------------	---------------------

Item	Descrição	CATSER/PDM	Unidade de Medida	Quantidade 36 meses
9	Auditoria e Pentest: Execução de testes de invasão e auditoria técnica independente a cada 180 dias (semestral) - 36 meses	14168	Ciclo	6

7.2. Memória de Cálculo e Justificativa:

7.2.1. Para o **grupo 1**: O quantitativo de 250 licenças de Endpoint e 120 usuários de ZTNA baseia-se no censo atual de colaboradores (internos e remotos) do CRA-SP, prevendo uma margem de segurança para expansão.

7.2.2. Para o **grupo 2**: A definição de 03 produtos específicos visa garantir a entrega documental e metodológica essencial para a governança do Conselho, conforme as diretrizes da ISO 27001, sem a necessidade de mensuração por horas trabalhadas, focando no resultado, com revisão anual.

7.2.3. A estimativa de 02 ciclos anuais (semestrais) segue as boas práticas de segurança cibernética para autarquias federais, garantindo que as mudanças de infraestrutura realizadas no primeiro semestre sejam validadas e corrigidas no segundo.

7.3. A pesquisa de preços para definição dos valores, que compõem o objeto deste ETP, corresponde a um conjunto de informações, obtidos por meio de diversas fontes de pesquisas, atendendo às exigências da IN SEGES/ME nº 65/2021, **conforme mapa de preços (Doc. SEI nº 3969235)**

7.4. O Valor Total estimado para **12 meses** é de **R\$ 290.912,12 (duzentos e noventa mil novecentos e doze reais e doze centavos)** e para **36 meses** é de **R\$ 817.056,36 (oitocentos e dezessete mil cinquenta e seis reais e trinta e seis centavos)**.

8. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

Estratégia de Divisão do Objeto: A contratação foi dividida em 03 (três) **grupos**, adotando-se o parcelamento como regra para ampliar a competitividade, sem perder a integridade técnica da solução.

8.1. **Justificativa para o Agrupamento no grupo 1 (Solução Integrada):** Embora a Lei nº 14.133/2021 preveja o parcelamento, optou-se tecnicamente pelo agrupamento dos componentes de Firewall (HaaS), Endpoint (XDR) e Serviços Gerenciados (MDR) em um único **grupo**. A fragmentação destes itens geraria:

8.1.1. Risco de Incompatibilidade Técnica: A eficácia da arquitetura baseia-se no conceito de XDR (Extended Detection and Response), que exige a correlação nativa de dados entre a rede e o usuário. Fornecedores diferentes não garantiriam essa integração em tempo real;

8.1.2. Conflito de Responsabilidade (Finger-pointing): Em caso de incidente cibernético, a divisão de responsabilidades entre múltiplos fornecedores dificultaria a resposta rápida, gerando o risco de um fornecedor atribuir a falha ao outro;

8.1.3. Eficiência na Gestão: O monitoramento 24x7 (MDR) precisa ter visibilidade total da ferramenta que ele opera (Firewall/Endpoint) para ser eficaz.

8.2. **Justificativa para o Parcelamento (grupos 1, 2 e 3):** A divisão entre os **grupos** de Operação (**grupo 1**), Governança (**grupo 2**) e Auditoria (**grupo 3**) fundamenta-se em:

8.2.1. Segregação de Funções (Art. 5º da Lei nº 14.133/2021): É imperativo que a empresa responsável pelos testes de invasão e auditoria (**grupo 3**) seja independente da empresa que implementa e opera as defesas (**grupo 1**), garantindo a imparcialidade e a detecção real de falhas;

8.2.2. Especialização de Mercado: Os serviços de Consultoria em GRC (**grupo 2**) exigem competências em processos e normas (ISO 27001), que diferem das competências operacionais de suporte e hardware do **grupo 1**, permitindo que empresas especializadas em cada nicho participem do certame.

9. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

9.1. Não verifica-se contratações correlatas nem interdependentes para a viabilidade e contratação desta demanda.

10. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO

10.1. A contratação supracitada está prevista no planejamento de contratações anual (PCA) de 2026.

10.2. **Identificação do PCA no PNCP:** 43060078000104-0-000001/2026

10.3. **Grupo 1 e 3:** DFD N° 130/2026 - Soluções integradas de segurança de dados - Contratação prevista nº 32/2026

10.4. **Grupo 2:** DFD N° 123/2026 - Consultoria para Ropmap EY - Contratação prevista nº 39/2026

10.5. **Dotação orçamentária:**

10.5.1. 6.2.2.1.1.01.04.04.037 - Serviços de Internet e Data Center

11. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

11.1. Resultados Diretos e Indiretos: A contratação da Solução Integrada de Segurança e Serviços Especializados visa atingir os seguintes benefícios estratégicos para o CRA-SP:

11.1.1. Elevação da Resiliência Cibernética: Redução drástica na probabilidade de sucesso de ataques de Ransomware e vazamento de dados, garantindo a continuidade dos serviços prestados aos administradores registrados.

11.1.2. Eficiência Operacional (MDR): Implementação de vigilância 24x7x365, com tempos de resposta a incidentes (SLA) inferiores a 60 minutos, suprimindo a lacuna de pessoal interno para monitoramento noturno e em finais de semana.

11.1.3. Sustentabilidade Tecnológica e Econômica (HaaS): Eliminação do risco de obsolescência de hardware de segurança, uma vez que a atualização tecnológica está inclusa no serviço, transformando custos variáveis de manutenção (CAPEX) em custos previsíveis (OPEX).

11.1.4. Conformidade Legal e Reputacional: Atendimento pleno aos requisitos da LGPD (Lei nº 13.709/2018) e às recomendações de segurança do TCU, evitando sanções administrativas e protegendo a imagem institucional do Conselho.

11.1.5. Governança e Maturidade (GRC): Institucionalização de processos formais de gestão de riscos e continuidade de negócios, permitindo que as decisões de investimento em TI sejam baseadas em dados e indicadores de maturidade (KPIs).

11.1.6. Independência de Verificação (Pentest): Obtenção de uma visão imparcial e técnica das vulnerabilidades da infraestrutura, permitindo correções preventivas antes que falhas sejam exploradas por agentes maliciosos.

12. PROVIDÊNCIAS A SEREM ADOTADAS

12.1. Será providenciada a definição do(a)(s) servidor(a)(es) que fará(ão) parte da equipe de fiscalização técnica e gestão contratual, previamente ao contrato.

12.2. Não será necessário adequação ao ambiente, pois o CRA-SP já possui infraestrutura física e estações de trabalho, para a futura contratação. Por esse motivo, não será necessário fazer ajustes no ambiente do órgão para que a contratada atenda à necessidade do negócio.

13. DESCREVENDO OS POSSÍVEIS IMPACTOS AMBIENTAIS

13.1. Não há previsão de impactos ambientais já que os rejeitos são coletados em programa específico de destinação de resíduos.

14. DECLARAÇÃO DA VIABILIDADE OU NÃO DA CONTRATAÇÃO

14.1. Diante do exposto, da análise dos documentos que compõem o processo, do histórico referente às contratações solicitadas pelo departamento de Tecnologia da Informação, bem como do valor

orçado para a realização da demanda, considera-se **viável** para o CRA-SP a contratação de **Solução Integrada de Segurança Cibernética e Serviços Especializados de Governança e Auditoria**, visando a proteção dos ativos de informação e adequação com a LGPD no âmbito do CRA-SP.

15. RESPONSÁVEIS

S.Paulo, na data da assinatura digital.

Nome: Ivan Cesar Machado Narcizo - Coordenador de Infraestrutura - (Responsável pela confecção)

Nome: Eduardo Sadayoshi Borghi Kondo - Assessor de Tecnologia



Documento assinado eletronicamente por **Eduardo Sadayoshi Borghi Kondo**, Gerente de Tecnologia, em 09/04/2026, às 16:21, conforme horário oficial de Brasília.



Documento assinado eletronicamente por **Ivan Cesar Machado Narcizo**, Assistente, em 09/04/2026, às 16:26, conforme horário oficial de Brasília.



A autenticidade deste documento pode ser conferida no site sei.cfa.org.br/conferir, informando o código verificador **3968897** e o código CRC **53F7E345**.