



DMI - ESTUDO TÉCNICO PRELIMINAR - AMD 71/2023

Brasília, 27 de janeiro de 2026.

1. DESCRIÇÃO DA NECESSIDADE

1. DESCRIÇÃO GERAL DA NECESSIDADE

Aquisição de licenças de autenticação, com serviços de instalação e configuração, operação assistida, capacitação, com garantia e suporte de 36 meses.

1.1. MOTIVAÇÃO/JUSTIFICATIVA

O Planejamento Estratégico Institucional, aprovado pelo Ato da Mesa Diretora nº 146, de 2022, estabelece objetivos estratégicos para a sustentação e o funcionamento do complexo computacional da CLDF, incorporado ao PDTI 2024/2025, Ato da Mesa Diretora nº 43 de 2024, no Item 6, Inventário de Necessidades Computacionais, com objetivo estratégico OBJ-5 – Prover sustentação computacional - Garantir sustentação e funcionamento do complexo computacional, alinhado ao Plano Setorial 2025: Meta 30 (Sustentação, manutenção e proteção da rede institucional de dados realizadas), Ação 4 (Adquirir licenças de autenticação [SEINF]).

Atualmente a CLDF faz a autenticação dos usuários diretamente no *Active Directory* -AD, com o uso de agentes que repassam as informações de autenticação aos demais dispositivos de controle de acesso, o que acaba limitando as possibilidades disponíveis de autenticação. A aquisição de licenças para autenticação possibilitará o uso de recursos mais avançados de autenticação, principalmente no firewall, permitindo autenticação centralizada e um melhor controle de acesso dos usuários da Casa, de forma mais granular. As licenças garantem, também, que a infraestrutura esteja em conformidade com as novas normas de segurança e privacidade vigentes, alargando as possibilidade de autenticação e sua automatização. Isso aumenta a garantia que apenas pessoas autorizadas por políticas da Casa tenham acesso aos recursos da rede da CLDF. Além disso, a CLDF usa o serviço de autenticação RADIUS (*Remote Authentication Dial-In User Service*), notadamente na rede sem fio, que é um protocolo que protege uma rede habilitando a autenticação centralizada e a autorização de usuários com ligação direta com o AD. Contudo, esse protocolo tem sua atuação limitada, na atual infraestrutura da CLDF, pois se encontra em serviço NPS da Microsoft, à configurações padrões e depende totalmente de configurações feitas pelos administradores da rede, sem nenhum tipo de suporte. A CLDF também possui o serviço de autenticação via Fortiauthenticator, que é mais moderno e seguro que o RADIUS em NPS da Microsoft, mas não possui licenças para todos os usuários da Casa, para eliminar o serviços de RADIUS em NPS da Microsoft para as autenticações dos usuários.

As licenças para tokens permitirão o acesso a dispositivos de TI da Casa por seus administradores, em caso de manutenção, em que haja desligamento do AD e das máquinas virtuais que hospedam os aplicativos de autenticação;

O treinamento e a operação assistida capacitarão os servidores da SEINF a utilizar essas ferramentas

de forma mais eficaz. Servidores atualizados estarão mais preparados para lidar com ameaças e vulnerabilidades;

Embora haja um investimento inicial, a aquisição resultará em economia de recursos e aumento da segurança da rede, pois processos automatizados de autenticação, com servidores capacitados, reduzem erros e desperdício de recursos de segurança.

1.2. PREVISÃO DA CONTRATAÇÃO NO PDTI E NO PCA

Esta contratação está prevista no PDTI 2024/2025: Ato da Mesa Diretora nº 43 de 2024, no Item 6, Inventário de Necessidades Computacionais, com o objetivo estratégico OBJ-5 – Prover sustentação computacional - Garantir sustentação e funcionamento do complexo computacional, alinhado ao Plano Setorial 2025: Meta 30 (Sustentação, manutenção e proteção da rede institucional de dados realizadas), Ação 4 (Adquirir licenças de autenticação [SEINF]).

1.3. NECESSIDADES DE NEGÓCIO

1.3.1. Segurança da Rede: Garantir que somente usuários autorizados tenham acesso à rede sem fio, prevenindo acessos não autorizados que podem comprometer a integridade e a confidencialidade dos dados da CLDF.

1.3.2. Conformidade Regulatória: Muitos órgãos públicos precisam atender a requisitos específicos de conformidade, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, que exige medidas adequadas para proteger dados pessoais. A autenticação robusta ajuda a cumprir esses requisitos.

1.3.3. Controle de Acesso: Implementar políticas de controle de acesso baseadas em identidade, permitindo que apenas usuários autenticados possam acessar determinados recursos, serviços ou informações dentro da rede.

1.3.4. Auditoria e Relatórios: Necessidade de gerar logs e relatórios detalhados sobre quem está acessando a rede e quando, para fins de auditoria, monitoramento e resposta a incidentes de segurança.

1.3.5. Gerenciamento Centralizado: Facilitar o gerenciamento de usuários e políticas de acesso a partir de um ponto centralizado, reduzindo a complexidade operacional e os custos de administração da rede.

1.3.6. Integração com Outras Soluções de Segurança: Possibilidade de integrar o FortiAuthenticator com outros componentes da infraestrutura de segurança, como firewalls, sistemas de detecção de intrusos, e soluções de monitoramento, para criar uma arquitetura de segurança mais robusta.

1.3.7. Eficiência Operacional: Reduzir o tempo e esforço necessários para gerenciar as credenciais e autenticações de usuários, especialmente em um ambiente com um número significativo de servidores, terceirizados e visitantes.

1.3.8. Suporte a Dispositivos Móveis e BYOD - *Bring Your Own Device*: Necessidade de suportar uma variedade de dispositivos, incluindo aqueles trazidos pelos próprios funcionários (BYOD), garantindo que todos sejam autenticados de forma segura.

1.4. NECESSIDADES TECNOLÓGICAS

- 1.4.1. **Segurança Avançada da Rede:** Implementar autenticação forte para garantir que apenas usuários devidamente autorizados acessem a rede sem fio, protegendo contra acessos não autorizados e possíveis ameaças cibernéticas.
- 1.4.2. **Conformidade com Políticas de Segurança e Regulamentações:** Necessidade de aderir a normas de segurança e regulamentações, como a LGPD, que exigem a proteção dos dados através de mecanismos adequados de autenticação e controle de acesso.
- 1.4.3. **Gerenciamento de Identidades e Acessos:** Facilitar a administração centralizada de identidades e acessos dos usuários, permitindo o controle granular sobre quem pode acessar quais recursos e em quais condições.
- 1.4.4. **Monitoramento e Auditoria de Acessos:** Capacidade de monitorar e registrar todos os acessos à rede, gerando logs detalhados que podem ser utilizados para auditorias e para responder rapidamente a incidentes de segurança.
- 1.4.5. **Integração com Infraestrutura de Segurança Existente:** Necessidade de integrar o FortiAuthenticator com outras soluções de segurança, como firewalls e sistemas de prevenção de intrusões, para criar um ecossistema de segurança mais coeso e eficaz.
- 1.4.6. **Automatização e Eficiência Operacional:** Reduzir a carga administrativa e operacional associada ao gerenciamento de autenticações e credenciais, através da automação de processos e da simplificação do gerenciamento de usuários.
- 1.4.7. **Suporte a Ambientes Móveis e BYOD:** Habilitar a autenticação segura de uma ampla gama de dispositivos, incluindo dispositivos móveis e aqueles trazidos por funcionários, garantindo a segurança em um ambiente de rede dinâmico e diversificado.
- 1.4.8. **Escalabilidade e Flexibilidade:** Necessidade de uma solução que possa escalar conforme o número de usuários cresce, e que ofereça flexibilidade para adaptar as políticas de autenticação às necessidades tecnológicas em evolução da CLDF.

1.5. REQUISITOS DE ARQUITETURA TECNOLÓGICA

- 1.5.1. **Compatibilidade com o ambiente de soluções integradas da rede da CLDF,** composto de firewall, switches, servidores de logs, autenticadores e tokens de acesso, todos do fabricante Fortinet.
- 1.5.2. **Aquisição de 25 licenças de tokens para autenticação em dupla camada;**
- 1.5.3. **Aquisição de 3000 licenças de acesso para Fortiauthenticator;**
- 1.5.4. **Suporte, assistência técnica, manutenção e garantia da solução pelo prazo 36 (trinta e seis) meses.** Os prazos normalmente praticados pelo mercado, são 1, 3 e 5 anos, sendo escolhido o prazo de 3 anos por questões orçamentárias e de atualização tecnológica.

1.6. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

- 1.6.1. **Todas as despesas e ônus dos serviços de instalação ocorrerão por conta da CONTRATADA;**
- 1.6.2. **Possuir garantia de funcionamento, assistência técnica e suporte técnico para todos os equipamentos (incluindo softwares) fornecidos, durante o período de 36 (trinta e seis) meses, a partir da emissão do Termo de Recebimento Definitivo pela CLDF;**
- 1.6.3. **A CONTRATADA deverá dispor de central de atendimento para abertura de chamados na modalidade mínima de 24 (vinte e quatro) horas x 7 (sete) dias. Os chamados poderão ser efetuados através de ligação local, ou através de telefone 0800 (ligação gratuita), acesso Web ou e-mail. Os chamados serão ser registrados e ficarão disponíveis para consulta pela CLDF.**

1.7. REQUISITOS DE IMPLANTAÇÃO

1.7.1. Os serviços de instalação, configuração, manutenção, avaliação, bem como intervenções feitas pela CONTRATADA, no ambiente de TI da CLDF, deverão seguir as melhores práticas (forma de execução e apresentação dos resultados) preconizadas pelo ITIL (*Information Technology Infrastructure Library*), como, por exemplo, os aspectos de documentação, manutenção dos níveis de serviço, abertura de ordens de serviço e emissão de relatórios técnicos;

1.7.2. A instalação lógica e configuração deverá ser realizada por profissional detentor de certificação NSE 7 ou superior, ou equivalente;

1.8. REQUISITOS DE GARANTIA E MANUTENÇÃO

1.8.1. A CONTRATADA deve contratar o plano de suporte do fabricante pelo período de 3 anos que funcione em regime 24/7, com atendimento inicial em até 2 horas para chamados, sejam eles críticos ou não críticos, com garantia de troca de hardware defeituoso em até 4 horas;

1.8.2. A CONTRATADA é corresponsável, juntamente ao fabricante, pelo atendimento dos prazos estabelecidos no termo de referência;

1.8.3. No caso de chamados de alta criticidade, assim compreendidos aqueles relacionados a incidentes que causam interrupção em serviços de produção na CLDF, a CONTRATADA deve concluir o atendimento do chamado em até 24 horas;

1.8.4. No caso de chamados de média criticidade, assim compreendidos aqueles relacionados a incidentes ou requisições relacionados a interrupção em serviços não críticos na CLDF, ou a redução dos níveis de serviço de segurança ou disponibilidade, tal como a aplicação de *patches* de segurança ou quando o incidente afetar itens de configuração redundantes, deixando o serviço de contar com redundância até a resolução, a CONTRATADA deve concluir o atendimento do chamado em até 60 horas;

1.8.5. No caso de chamados de baixa criticidade, assim entendidos aqueles não compreendidos nos itens anteriores, a CONTRATADA deve concluir o atendimento do chamado em até 96 horas;

1.8.6. O prazo de garantia contratual dos bens é de, no mínimo, 36 meses junto ao fabricante, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto. A garantia junto ao fabricante não exime a contratada da responsabilidade sobre as condições de garantia. Caso o prazo de garantia contratado inicialmente pela CONTRATADA junto ao fabricante não atenda a esse requisito, deverá, a seu custo, contratar o período suplementar, nos mesmos termos dos demais requisitos do Termo de Referência;

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

1.8.8. A garantia abrange a realização da manutenção corretiva dos bens pela própria CONTRATADA, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

1.8.9. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

1.8.10. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

1.8.11. Uma vez notificada, a CONTRATADA deverá certificar-se que o fabricante atue no chamado no tempo definido nos itens acima, e que, em se demonstrando a necessidade de substituição do equipamento ou de componente, esse seja realizado pelo fabricante ou por autorizado no prazo de até 4 horas, contados a partir da constatação da necessidade de substituição do item, devendo a CONTRATADA atuar na resolução na falha do fabricante.

1.8.12. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado mediante solicitação escrita e justificada da CONTRATADA, aceita pela CONTRATANTE.

1.8.13. Na hipótese do subitem acima, a CONTRATADA deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pela CONTRATANTE, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

1.8.14. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação da CONTRATANTE ou a apresentação de justificativas pela CONTRATADA, fica a CONTRATANTE autorizada a contratar o próprio fabricante ou empresa autorizada diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da CONTRATADA o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

1.8.15. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da CONTRATADA.

1.8.16. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

1.8.17. Todo o suporte que envolva a intervenção em equipamentos físicos ou que possua especial sensibilidade, conforme declarada pela equipe técnica da contratante, deverá ser feita presencialmente pelo fabricante ou remotamente pelo fabricante com acompanhamento presencial pela contratada.

1.8.18. Durante a vigência dos serviços, não pode haver limite de quantidade dos chamados técnicos junto ao fabricante, que poderão ser abertos via telefone, e-mail, sistema web ou chat, caracterizando a abertura do chamado. Caso os planos do fabricante apresentem limites, deverá a contratada arcar com o custo dos chamados realizados acima do limite, durante a vigência do contrato.

1.9. REQUISITOS DE METODOLOGIA DE TRABALHO

1.9.1. O fornecimento dos equipamentos está condicionado ao recebimento pela CONTRATADA de Ordem de Fornecimento de Bens (OFB) ou equivalente emitida pela CONTRATANTE.

1.9.2. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

1.9.3. A CONTRATADA deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento de 24 horas por dia e 7 dias por semana de maneira eletrônica e de 24 horas por dia e 7 dias por semana por semana por via telefônica.

1.9.4. O andamento do fornecimento dos equipamentos deve ser acompanhado pela CONTRATADA, que dará ciência de eventuais acontecimentos à CONTRATANTE.

1.10. REQUISITOS DE SEGURANÇA, SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1.10.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da CLDF (POSID).

1.11. REQUISITOS LEGAIS

1.11.1. O presente processo de contratação deve estar aderente à [Constituição Federal](#), à [Lei nº 14.133/2021](#), ao AMD nº 71/2023 da CLDF, à [Lei nº 13.709/2018](#) (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis.

1.11.2. A CONTRATADA deverá observar as disposições da Lei 13.709/2018, Lei Geral de Proteção de Dados - LGPD, quanto ao tratamento dos dados pessoais que lhe forem confiados, em especial quanto à finalidade e boa-fé na utilização de informações pessoais para consecução dos fins a que se propõe o presente contrato;

1.11.3. A CONTRATADA deverá observar as disposições do Ato da Mesa Diretora nº 85/2022 e suas alterações posteriores, que regulamenta a aplicação Lei nº 13.709/2018 no âmbito da CLDF;

1.11.4. A CONTRATADA está obrigada a guardar o mais completo sigilo por si, por seus empregados ou prepostos, nos termos da Lei Complementar nº 105/2001 e da LGPD, cujos teores declaram ser de seu inteiro conhecimento, em relação aos dados, informações ou documentos de qualquer natureza, exibidos, manuseados ou que por qualquer forma ou modo venham tomar conhecimento ou ter acesso, em razão deste contrato, ficando, na forma da lei, responsáveis pelas consequências da sua divulgação indevida e/ou descuidada ou de sua incorreta utilização, sem prejuízo das penalidades aplicáveis nos termos da lei;

1.11.5. A CLDF figura na qualidade de Controlador dos dados quando fornecidos à CONTRATADA para tratamento, sendo esta enquadrada como Operador dos dados. A CONTRATADA será Controladora dos dados com relação a seus próprios dados e suas atividades de tratamento;

1.11.6. Os dados pessoais tratados e operados serão eliminados após o término contrato, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

1.11.6.1. cumprimento de obrigação legal ou regulatória pelo controlador;

1.11.6.2. estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

1.11.7. Uso exclusivo do Controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

1.11.8. Os casos omissos em relação ao tratamento dos dados pessoais que forem confiados à CONTRATADA, e não puderem ser resolvidos com amparo na LGPD, deverão ser submetidos à Administração do contrato para que decida previamente sobre a questão;

1.11.9. A Câmara Legislativa e aqueles que, sob sua determinação, atuarem na condição de Operadores de tratamento de dados pessoais, devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

1.12. REQUISITOS TEMPORAIS

1.12.1. A entrega dos equipamentos deverá ser efetivada no prazo máximo de 60 (sessenta) dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB) ou equivalente, emitida pela CONTRATANTE, podendo ser prorrogada, excepcionalmente, desde que justificado previamente pela CONTRATADA e autorizado pela CONTRATANTE.

1.13. **DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TI**

1.13.1. Possuir garantia de funcionamento, assistência técnica e suporte técnico para todos os equipamentos (incluídos *softwares*) fornecidos, durante o período de 36 (trinta e seis) meses;

1.13.2. Dispor de central de atendimento para abertura de chamados na modalidade mínima de 24 (vinte e quatro) horas x 7 (sete) dias. Os chamados poderão ser efetuados através de ligação local, ou através de telefone 0800 (ligação gratuita), acesso Web, mensagem/chat digital, ou e-mail. Os chamados serão ser registrados e ficarão disponíveis para consulta pela CLDF;

1.13.3. Possuir contrato de suporte diretamente com o fabricante para atendimento para abertura de chamados na modalidade mínima de 24 (vinte e quatro) horas x 7 (sete) dias, e troca de equipamentos em 4 horas.

1.13.4. Os serviços de instalação, configuração, manutenção, avaliação, bem como intervenções realizadas, no ambiente de TI da CLDF, deverão seguir as melhores práticas (forma de execução e apresentação dos resultados) preconizadas pelo ITIL (*Information Technology Infrastructure Library*), como, por exemplo, os aspectos de documentação, manutenção dos níveis de serviço, abertura de ordens de serviço e emissão de relatórios técnicos;

2. **LEVANTAMENTO DE SOLUÇÕES**

2.1. **NECESSIDADES SIMILARES EM OUTROS ÓRGÃOS OU ENTIDADES DA ADMINISTRAÇÃO PÚBLICA E AS SOLUÇÕES ADOTADAS**

Nesta contratação foram analisadas contratações similares, não só para o alinhamento de expectativas, mas também para elaboração de estimativas preliminares de preço durante a elaboração do PDTI 2024/2025.

2.2. **Alternativas do mercado**

Há vários competidores para o fornecimento de licenças de autenticação. Foram solicitadas quatro propostas para fornecedores disponíveis:

- a) Proposta 1, da empresa WY Tecnologia (2441226)
- b) Proposta 2, da empresa GlobalSec (2441231)
- c) Proposta 3, da empresa WPI (2441240)
- d) Proposta 4, da empresa NCT (2441257)

2.3. **Políticas, modelos e padrões de governo (ex.: ePing, eMag, ePwg, ICP-Brasil, e-ARQ, etc)**

Não aplicável.

2.4. **Necessidades de adequação do ambiente da CLDF para viabilizar a execução contratual (ex.: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc)**

- Necessidade de disponibilização de ambiente para instalação da equipe técnica da CONTRATADA;
- Por já estar integrado à infraestrutura existente na Casa, tanto em relação ao *hardware* quanto ao *software*, não há necessidade de novos Recursos Materiais.

2.5. Modelos de prestação do serviço

Não aplicável.

2.6. Tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes

2.6.1. O FortiAuthenticator, da Fortinet:

É uma solução de autenticação multifator (MFA) e gerenciamento de identidade que oferece recursos como autenticação baseada em tokens, integração com diretórios LDAP, autenticação de convidados e muito mais. Quando se trata de licenciamento, aqui estão algumas informações importantes:

2.6.1.1. Contagem de Usuários:

- O FortiAuthenticator conta como "usuário" qualquer conta criada nele, incluindo usuários locais, usuários remotos e usuários convidados.
- Alguns casos de uso não exigem a criação de uma conta de usuário no FortiAuthenticator e, portanto, não consomem licenças de usuário.
- Apenas as contas no FortiAuthenticator são contabilizadas; o número de dispositivos/endereços MAC/conexões ativas associadas a cada usuário não afeta a contagem.
- Usuários convidados também contam para o limite de licenças, mas geralmente têm duração limitada. Pode-se configurar a exclusão automática de contas de usuários expiradas para liberar licenças novamente.

2.6.1.2. Autenticação Baseada em Máquina:

- Para usos de autenticação baseada em endereço MAC (MAC-Bypass), o FortiAuthenticator verifica o endereço MAC fornecido em relação aos dispositivos MAC armazenados. Isso não consome licenças de usuário.
- No entanto, se estiver usando autenticação EAP-TLS com certificados, isso conta para o limite de licenças. Nesse caso, o próprio computador é contado como um usuário, independentemente de quantos usuários estejam realmente logados no computador.

2.6.2. Licenças do FortiToken Mobile

O FortiToken Mobile é usado para autenticação multifator (Multi Factor Authentication -MFA) e permite que os usuários utilizem senhas de uso único, tokens SMS e autenticação adaptativa. As licenças do FortiToken Mobile são adquiridas para um número específico de tokens móveis e são importadas para o FortiAuthenticator durante a ativação.

2.7. Possibilidade de aquisição na forma de bens ou contratação como serviço

Considerando tratar-se de aquisição de infraestrutura para sustentação da rede computacional da CLDF, a forma de contratação como serviço não se aplica, pois grande parte da rede já foi adquirida.

2.8. Ampliação ou substituição da solução implantada

Como dito na justificativa do projeto há necessidade de ampliação nos quantitativos de licenças, portanto, necessária a aquisição de novas licenças.

2.9. Diferentes métricas de prestação do serviço e de pagamento

Não aplicável.

Com base no levantamento acima, os seguintes cenários ou arranjos podem ser formados para compor as soluções possíveis para atendimento da necessidade:

Id	Descrição da solução (ou cenário)
1	<p>Aquisição de licença para uso temporário/perpétua.</p> <p>Atualmente, a CLDF possui uma solução de autenticação, para atender as necessidades de segurança das redes de dados da CLDF. Para alguns casos é necessário o uso de MFA. Contudo, o número de licenças é insuficiente para todos os usuários da Casa e o número de tokens precisa ser adotado em outros equipamentos da CLDF. A solução 1 é para esse cenário, é adquirir licenças temporárias (3 anos) para atender a necessidades específicas da autenticação. No caso dos tokens o licenciamento é perpetuo. Nesse cenário, a CLDF adquire as licenças diretamente de um revendedor autorizado Fortinet.</p>
2	<p>Subscrição das licenças com implantação e gerenciamento por terceiros</p> <p>Nesse cenário, considerando a mesma necessidade suprcitada, a CLDF assina um serviço de um fornecedor que inclui a implantação e manutenção das licenças. Nessa abordagem, você terceiriza a aquisição e gerenciamento das licenças para um provedor de serviços ou consultor especializado.</p>

3. ANÁLISE COMPARATIVA DAS SOLUÇÕES

Requisitos		Cenários	
		Aquisição de licença para uso temporário/perpétua.	Subscrição das licenças com implantação e gerenciamento por terceiros
Negócio	Continuidade dos serviços de TIC	atende	atende
	Conformidade	atende	atende
	Manutenção e sustentabilidade	atende	atende
	Segurança e privacidade	atende	atende

	Capacidade de prover as necessidades com suporte pelo prazo de 36 meses	atende	atende
Tecnológico	Alta disponibilidade	atende	atende
	Compatibilidade com o ambiente de soluções integradas da CLDF, composto, além do fortiautheticator, firewall, switches, APs e tokens de acesso.	atende	não atende
	Expansão das licenças para prover autenticação em Fortiautheticator virtualizado, FAC-VM, para 3.000 usuários em duas máquinas virtuais (<i>appliances</i>) que compõem um cluster de Fortiautheticator;	atende	não atende
	Licenças de tokens para autenticação em dupla camada;	atende	atende
	Suporte, assistência técnica, manutenção e garantia da solução pelo prazo 36 (trinta e seis) meses.	atende	atende
	Gerenciamento e monitoração	atende	atende
	Escalabilidade e flexibilidade	atende	não atende
	Auditoria e controle	atende	atende
	Atualização tecnológica	atende	atende
Demais	Compatibilidade e integração	atende	não atende
	Níveis de serviço	atende	atende

	Economicidade	atende	não atende
Resultado da Análise		viável	inviável

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS E JUSTIFICATIVA

Com base na análise das duas alternativas para ampliação da solução de autenticação multifator (MFA) na Câmara Legislativa do Distrito Federal (CLDF), conclui-se que a opção pela aquisição direta de licenças temporárias e perpétuas (Solução 1) é a mais adequada e viável. Essa abordagem contempla a compra de licenças temporárias com validade de 36 meses para autenticação via FortiAuthenticator, além de licenças perpétuas para tokens de acesso, adquiridas diretamente de revendedor autorizado Fortinet. A solução atende integralmente aos requisitos técnicos, operacionais e estratégicos da CLDF, garantindo compatibilidade com o ambiente tecnológico já implantado — composto por firewalls, switches, pontos de acesso, FortiAuthenticator e tokens — e permitindo a expansão para até 3.000 usuários em cluster virtualizado (FAC-VM). Além disso, oferece escalabilidade, flexibilidade, suporte técnico, garantia e economicidade, assegurando a continuidade dos serviços de TIC com conformidade e segurança.

Por outro lado, a subscrição das licenças com implantação e gerenciamento por terceiros (Solução 2), embora ofereça comodidade na gestão, apresenta limitações críticas: não garante compatibilidade com o ambiente Fortinet existente, não atende à expansão para autenticação em cluster virtualizado, não oferece flexibilidade para crescimento futuro e representa menor viabilidade econômica. Tais restrições comprometem a integração e a sustentabilidade da solução no contexto da CLDF.

Diante disso, recomenda-se a adoção da Solução 1, por atender plenamente às necessidades institucionais, técnicas e estratégicas da CLDF, sendo a única alternativa viável para garantir segurança, continuidade e eficiência na autenticação dos usuários da Casa.

5. ANÁLISE COMPARATIVA DE CUSTOS DAS SOLUÇÕES VIÁVEIS

5.1. **CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)** - método utilizado para calcular o custo global de um produto ou serviço ao longo de seu ciclo de vida

Solução Viável :					
Propostas/Preço Público					
Item	1	2	3	4	Média

Aquisição de licenças de tokens para autenticação em dupla camada	R\$ 19.100,00	R\$ 20.000,00	R\$ 19.503,00	R\$ 13,450.00	R\$ 18.013,25
Aquisição de licenças de acesso para Fortiauthenticator	R\$ 486.000,00	R\$ 510.000,00	R\$ 489.690,00	R\$ 273,360.00	R\$ 439.762,50
Serviços de instalação e configuração	R\$ 70.186,00	R\$ 79.900,00	R\$ 59.368,12	R\$ 22,000.00	R\$ 57.863,53
Serviços de operação assistida	R\$ 160.426,00	R\$ 155.000,00	R\$ 161.524,50	R\$ 11,900.00	R\$ 122.212,63
Serviços de capacitação	R\$ 60.162,00	R\$ 72.000,00	R\$ 7.475,30	R\$ 117,842.34	R\$ 64.369,91
Custo Total	R\$ 795.874,00	R\$ 836.900,00	R\$ 807.560,92	R\$ 438,552.34	R\$ 719.721,82

Para elaborar a estimativa de custos foram solicitadas cotações de mercado com fornecedores:

- a) Proposta 1, da empresa WY Tecnologia (2441226)
- b) Proposta 2, da empresa GlobalSec (2441231)
- c) Proposta 3, da empresa WPI (2441240)
- d) Proposta 4, da empresa NCT (2441257)

Solução Viável :					
Propostas/Preço Público	1	2	3	4	Média
Item					
	R\$ 795.874,00	R\$ 836.900,00	R\$ 807.560,92	R\$ 438,552.34	R\$ 719.721,82
Custo Total					R\$ 719.721,82

5.2. MAPA COMPARATIVO DOS CUSTOS TOTAIS

Descrição da solução	Estimativa de custos ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
	R\$ 239.907,27	R\$ 239.907,27	R\$ 239.907,27	R\$ R\$ 719.721,82

6. DECLARAÇÃO DE VIABILIDADE

6.1. Declaração de viabilidade da contratação:

O objeto do presente ETP é viável

6.2. Justificativa da solução escolhida:

A solução escolhida — aquisição de licenças temporárias e perpétuas diretamente de revendedor autorizado — é justificada por sua plena compatibilidade com o ambiente tecnológico da CLDF, capacidade de expansão para até 3.000 usuários em cluster virtualizado, escalabilidade, flexibilidade e melhor relação custo-benefício. Além de atender integralmente aos requisitos de segurança, conformidade e continuidade dos serviços de TIC, essa abordagem garante autonomia na gestão da autenticação multifator, suporte técnico e garantia por 36 meses, tornando-se a alternativa mais viável e eficiente frente às necessidades institucionais.

7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

O cálculo realizado foi baseado na análise integrada dos acessos de usuários via protocolo RADIUS e na quantidade de usuários ativos registrados no Active Directory da CLDF. Essa abordagem permitiu estimar o número de usuários que demandam autenticação para o acesso WiFi e multifator (MFA) no acesso administrativo ao firewall da CLDF, em caso de indisponibilidade da infraestrutura do ambiente virtualizado da CLDF, em consonância ao apontado na Nota Técnica 1 SEI nº 0964033;.

O levantamento dos acessos via RADIUS refletiu o volume de autenticações realizadas nos sistemas corporativos, especialmente em serviços que exigem validação segura, como VPN, Wi-Fi corporativo e acesso remoto, conforme Relatório Ativos e Usuários (2365741). Já a consulta ao Active Directory, realizada no Estudo Técnico Preliminar - ETP 1195996 do Processo 00001-00005433/2023-28 (Informática:Aquisição de soluções e serviços em tecnologia da informação), no item 7.1.1 "Dados para avaliar o quantitativo de licenças", forneceu o total de contas de usuários atualmente habilitadas e com potencial de uso dos recursos de rede e sistemas internos.

Ao cruzar essas duas fontes — acessos reais e base de usuários ativos — foi possível identificar o universo de usuários que necessitam de licenciamento para autenticação, considerando tanto o uso atual quanto a projeção de crescimento em estimativa. Essa metodologia garante que o dimensionamento das licenças seja adequado, evitando tanto a subutilização quanto a insuficiência de recursos, e assegura a continuidade dos serviços com segurança, escalabilidade e conformidade com as políticas de TIC da CLDF.

8. DESCRIÇÃO DA SOLUÇÃO DE TI A SER CONTRATADA

Aquisição de licenças de autenticação, com serviços de instalação e configuração, operação assistida, capacitação, com garantia e suporte de 36 meses.

9. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Aquisição de licenças de autenticação, com serviços de instalação e configuração, operação assistida, capacitação, com garantia e suporte de 36 meses.

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	Aquisição de licenças de tokens para autenticação em dupla camada	25	R\$ 720,53	R\$ 18.013,25
2	Aquisição de licenças de acesso para Fortiauthenticator	3000	R\$ 146,59	R\$ 439.762,50
3	Serviços de instalação e configuração	1	R\$ 57.863,53	R\$ 57.863,53
4	Serviços de operação assistida	1	R\$ 122.212,63	R\$ 122.212,63
5	Serviços de capacitação	6	R\$ 10.728,32	R\$ 64.369,91
Total				R\$ 719.721,82

10. RESPONSÁVEIS**EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO**

INTEGRANTE	NOME	MATRÍCULA	LOTAÇÃO	RAMAL
Requisitante	FÁBIO VIRGILIO DE SOUZA NEVES	23.554	SEINF	8321
Técnico	AIMBERE GIANNACCINI	18.327	SEINF	8321
Técnico	PAULO ANDRÉ VALADÃO DE BRITO	12.481	SEINF	8321

NOME DA ÁREA TÉCNICA DE TI	NOME DO CHEFE OU SUBSTITUTO	MATRÍCULA	RAMAL
SEINF	PEDRO CUNHA REGO CELESTIN	22.858	8344

11. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições do AMD nº 71, de 2023.

WALERIO OLIVEIRA CAMPORES
Diretor da DMI

Conforme [AMD nº 71, de 2023](#), art. 12, § 2º, o Estudo Técnico Preliminar da Contratação será assinado pelos Integrantes Técnico e Requisitante da contratação e pelo Chefe da respectiva Área Técnica de TI e aprovado pelo Chefe da Área de TI. Caso o Chefe da Área Técnica de TI ou o Chefe da Área de TI venha a compor a Equipe de Planejamento da Contratação, a autoridade que assinará o Estudo Técnico Preliminar da Contratação juntamente com os Integrantes Técnico e Requisitante será aquela diretamente superior ao respectivo Chefe, conforme § 3º.



Documento assinado eletronicamente por **AIMBERE GIANNACCINI - Matr. 18327, Fiscal Técnico(a)**, em 02/02/2026, às 16:39, conforme Art. 30, do Ato da Mesa Diretora nº 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.



Documento assinado eletronicamente por **WALERIO OLIVEIRA CAMPORES - Matr. 24872, Diretor(a) de Modernização e Inovação Digital**, em 02/02/2026, às 16:44, conforme Art. 30, do Ato da Mesa Diretora nº 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.



Documento assinado eletronicamente por **PAULO ANDRE VALADAO DE BRITO - Matr. 12481, Fiscal Técnico(a)**, em 03/02/2026, às 10:52, conforme Art. 30, do Ato da Mesa Diretora nº 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.



Documento assinado eletronicamente por **PEDRO CUNHA REGO CELESTIN - Matr. 22858, Chefe do Setor de Infraestrutura de Tecnologia da Informação**, em 06/02/2026, às 14:26, conforme Art. 30, do Ato da Mesa Diretora nº 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.



Documento assinado eletronicamente por **FABIO VIRGILIO DE SOUZA NEVES - Matr. 24554, Consultor(a) Técnico-Legislativo**, em 06/02/2026, às 14:37, conforme Art. 30, do Ato da Mesa Diretora nº 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.



A autenticidade do documento pode ser conferida no site:

http://sei.cl.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Código Verificador: **2506961** Código CRC: **6B232728**.

Praça Municipal, Quadra 2, Lote 5, 2º andar, Sala 2.15– CEP 70094-902– Brasília-DF– Telefone: (61)3348-8321
www.cl.df.gov.br - seinf@cl.df.gov.br

00001-00025785/2024-81

2506961v3