DMI - ESTUDO TÉCNICO PRELIMINAR - AMD 71/2023

Brasília, 06 de outubro de 2025.

1. DESCRIÇÃO DA NECESSIDADE

1. DESCRIÇÃO GERAL DA NECESSIDADE

Aquisição de solução de gerenciamento de contas e de acessos privilegiados, com serviços de instalação e configuração, operação assistida, capacitação, com garantia e suporte de 36 meses.

1.1. MOTIVAÇÃO/JUSTIFICATIVA

A segurança da informação compreende um conjunto de ações e estratégias para proteger sistemas, programas, equipamentos e redes de invasões. Seu objetivo central é proteger dados valiosos de possíveis violações ou ataques. Os pilares da segurança da informação incluem confidencialidade, integridade e disponibilidade. Além disso, suas funções envolvem prevenção, detecção e resposta a incidentes. A segurança da informação é crucial para proteger informações sensíveis e evitar danos à organização e à imagem institucional. Houve um aumento contínuo de incidentes de segurança na infraestrutura da CLDF, especialmente após a pandemia e a adoção do trabalho remoto. O crescente aumento de incidentes se deve à complexidade do ambiente corporativo e ao uso crescente de técnicas de invasão. Contudo, a própria evolução dos sistemas de segurança, contra essas invasões, tendem a conter os incidentes de segurança. Em relação aos incidentes de segurança, destacam-se os acessos privilegiados não autorizados. O Gerenciamento de Acesso Privilegiado (*Privileged Access Management* - PAM) é uma solução de segurança que protege identidades com acesso especial, além dos usuários normais. Ele controla e protege o uso de credenciais de alto privilégio, garantindo armazenamento seguro, segregação de acessos e rastreabilidade. O PAM é essencial para prevenir o roubo de credenciais e garantir a conformidade. O princípio do menor privilégio é uma estratégia de segurança que se baseia na ideia de conceder autorizações apenas quando realmente necessárias. Essas soluções restringem os direitos de acesso e permissões aos usuários, garantindo que um usuário legítimo tenha somente o acesso correto. Isso aumenta a visibilidade, o gerenciamento e o controle sobre as atividades administrativas. O gerenciamento de sessões permite que a comunicação entre usuários normais e ativos privilegiados seja intermediada por um proxy/gateway de conexão. Isso inclui a gravação de sessões e a auditoria de todas as operações realizadas com credenciais privilegiadas.

A contratação de uma solução de Gerenciamento de Acesso Privilegiado (PAM) com vigência de 36 meses representa uma medida estratégica alinhada às melhores práticas de segurança da informação e à continuidade operacional da Administração Pública. Em um cenário de crescente sofisticação de ameaças cibernéticas, a adoção de uma solução robusta e consolidada por um período mais longo garante:

- Estabilidade e maturidade na implementação: Soluções PAM exigem tempo para integração com os diversos sistemas da organização, treinamento de equipes e amadurecimento dos processos de controle de acesso. Um contrato de 36 meses permite consolidar essas etapas sem interrupções ou riscos de descontinuidade.
- Eficiência econômica e previsibilidade orçamentária: A contratação por prazo estendido permite negociar condições comerciais mais vantajosas, protegendo a Administração contra oscilações cambiais e inflacionárias. Isso reduz o custo total de propriedade (TCO) e evita gastos recorrentes com renovações ou novas licitações.
- Fortalecimento da postura de segurança: A permanência de uma solução PAM por três anos assegura a continuidade das políticas de segurança, auditoria e conformidade com normativas como LGPD e ISO 27001, sem a vulnerabilidade de transições tecnológicas frequentes.
- Fomento à inovação interna: Ao garantir uma base tecnológica estável, a Administração pode direcionar esforços para inovação nos processos internos, sem o ônus de reavaliar constantemente a infraestrutura de segurança.

Até o momento, a CLDF não possui uma solução dedicada para essa funcionalidade, provendo acessos privilegiados por meio de contas e permissões basicamente baseadas em grupos específicos no serviço de diretório ou em acesso local. Esse controle possui uma estratégia fraca, pois se baseia em uma autenticação semelhante à de um usuário padrão, de forma descentralizada e com baixa rastreabilidade, razão pela qual é necessário fazer a evolução para uma solução de gerenciamento de acesso privilegiado (PAM).

1.2. PREVISÃO DA CONTRATAÇÃO NO PDTI E NO PCA

Esta contratação está prevista no PDTI 2023/2024: PDTI 2023/2024, Ato da Mesa Diretora nº 144 de 2022, Ação Estratégica 12.4.3 com o macro-objetivo estratégico: OBJ-5 – Manter os recursos computacionais em pleno funcionamento e alinhado ao Plano Setorial 2024: #Nec 5.1.9, Meta 25 (Realizadas sustentação, manutenção e proteção da rede institucional de dados), Ação 3 (Solução de segurança para controle de credenciais privilegiadas locais e remotas) [SEINF].

1.3. NECESSIDADES DE NEGÓCIO

1.3.1. Controle de Acesso a Contas Privilegiadas: As contas privilegiadas (como administradores de sistemas, bancos de dados ou dispositivos de rede) têm amplo acesso a recursos sensíveis. Uma solução de PAM deve garantir que apenas usuários autorizados possam acessar essas contas e que o acesso seja monitorado;

1.3.2. Monitoramento e Auditoria:O PAM deve registrar todas as atividades realizadas por contas privilegiadas. Isso permite auditorias detalhadas, detecção de comportamento suspeito e investigações em caso de incidentes.

1.3.3. Acesso Just-in-Time (JIT):A solução de PAM deve fornecer acesso temporário e sob demanda a contas privilegiadas. Isso reduz o risco de acesso contínuo e não autorizado.

1.3.4. Segurança Zero Trust:O PAM deve aplicar o princípio de confiança zero, garantindo que todas as solicitações de acesso sejam verificadas, independentemente da origem.

1.3.5. Automação e Escala:A solução de PAM deve ser escalável para gerenciar milhões de contas privilegiadas e automatizar tarefas como rotação de senhas e aprovações.

1.3.6. Integração com Ferramentas Nativas e Infraestrutura Baseada em Nuvem:A solução de PAM deve se integrar facilmente com outras ferramentas e infraestrutura existentes, incluindo serviços em nuvem.

1.4. NECESSIDADES TECNOLÓGICAS

1.4.1. Controle Granular de Acesso: Uma solução PAM deve permitir a definição precisa de quem pode acessar quais recursos privilegiados. Isso inclui políticas de acesso baseadas em funções, grupos e atributos específicos.

1.4.2. Autenticação Forte e Integração Multifator (MFA): O PAM deve exigir autenticação robusta para contas privilegiadas. Isso inclui integração com MFA, certificados digitais ou outros métodos de autenticação avançada.

1.4.3. Gerenciamento de Senhas e Rotação Automática: A solução PAM deve facilitar a rotação regular de senhas para contas privilegiadas. Isso reduz o risco de senhas comprometidas.

1.4.4. Monitoramento e Auditoria Contínuos: A capacidade de registrar e auditar todas as atividades relacionadas a contas privilegiadas é essencial. Isso inclui logs detalhados, alertas e análises de comportamento.

1.4.5. O PAM deve suportar um grande número de contas privilegiadas e garantir desempenho adequado.

1.4.6. Segurança de Sessão e Gravação de Comandos: A solução PAM deve ser capaz de gravar sessões de acesso privilegiado para fins de auditoria e investigação.

1.4.7. 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. Implementação rápida e simples: A solução deve permitir uma implantação rápida e sem complicações, minimizando a janela de vulnerabilidade durante o processo de integração.

1.5.2. Centralização de acesso: A solução deve centralizar e gerenciar acessos de forma segura, oferecendo um controle granular e imediato sobre os acessos privilegiados.

1.5.3. Complementaridade com IAM: A solução deve ser compatível com soluções de Gestão de Identidades e Acessos (IAM), permitindo uma integração eficaz entre as duas, notadamente com o *Active Directory* usado na CLDF.

1.5.4. Visibilidade e controle centralizados: A plataforma de gerenciamento deve oferecer visibilidade centralizada e controle de privilégios através de uma única interface.

1.5.5. Auditoria e relatórios abrangentes: A solução deve fornecer auditoria e relatórios detalhados das atividades de usuários em sistemas críticos.

1.5.6. Segurança robusta: A solução deve proteger credenciais privilegiadas em cofres criptografados, aplicar o princípio do privilégio mínimo e monitorar cada ação privilegiada em tempo real.

1.6. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

1.6.1. Todas as despesas e ônus dos serviços de instalação e configuração de todos os componentes da solução ocorrerão por conta da CONTRATADA;

1.6.2. Possuir garantia de funcionamento, assistência técnica e suporte técnico para todos os componentes da solução (incluídos 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 certificado pelo fabricante nos requisitos da solução;

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/atualização de quaisquer componentes da solução 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 custeio, 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 componentes da solução 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 todos os componentes da solução, a quantidade e a localidade na qual os componentes 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 componentes da solução dever 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 das licenças 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 artefatos (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 em órgãos públicos, não só para o alinhamento de expectativas, mas também para elaboração de estimativas preliminares de preço durante a elaboração do PDTI 2023/2024. Nesse aspecto, apesar de não terem mais validade temporal atual, destacam-se os contratos celebrados, vigentes até 2024, por BASA, ANEEL, SEST/SENAT e METRO-DF.

Órgão	Pregão
BASA	004/2023
ANEEL	15/2023
SEST/SENAT	69/2023
METRO-DF	02/2023

2.2. Alternativas do mercado

Há vários competidores para o fornecimento de solução PAM. Foram solicitadas cinco propostas para fornecedores disponíveis:

a) Proposta 1, da empresa 7Secure Doc SEI 2166134
b) Proposta 2, da empresa Fasthelp Doc SEI 2166133
c) Proposta 3, da empresa Cloud4Sec Doc SEI 2170259
d) Proposta 4, da empresa NCT Doc SEI 2172546
e) Proposta 5, da empresa Disruptec Doc SEI 2173845

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;
- Como será 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

O Gerenciamento de Acesso Privilegiado (PAM) é um conjunto de ferramentas que protegem e controlam contas, credenciais e comandos com acesso técnico elevado, utilizados para administrar ou configurar sistemas e aplicações. Essas ferramentas podem ser disponibilizadas como software, SaaS ou dispositivos físicos, e são aplicáveis tanto a usuários humanos (administradores, operadores) quanto a máquinas (sistemas e aplicações).

Segundo o Gartner, as soluções PAM se dividem em quatro categorias principais:

1. Gerenciamento de contas e sessões privilegiadas (PASM): Cofre de credenciais e controle de sessões.
2. Gerenciamento de elevação e delegação de privilégios (PEDM): Agentes locais que filtram comandos e elevam privilégios em Windows, macOS e Unix/Linux.
3. Gerenciamento de segredos: Cofres especializados para credenciais de software e cargas de trabalho.
4. Gerenciamento de permissões em infraestrutura de nuvem (CIEM): Controle de direitos em ambientes de provedores de nuvem.

O acesso privilegiado vai além do acesso comum de usuários e permite alterações críticas em sistemas e dados corporativos, representando riscos significativos. Por isso, o uso de ferramentas PAM é essencial para garantir segurança, conformidade e controle.

De modo geral, após análise de fornecedores e clientes, melhores situados no Gartner, as ferramentas do mercado provem as seguintes

funcionalidades, que foram consolidadas e avaliadas pela equipe de planejamento da contratação no momento da definição dos requisitos técnicos:

- Gestão de credenciais privilegiadas: capacidade de administrar credenciais e segredos, incluindo a geração, validação, rotação e revogação de indivíduos, credenciais e sistemas, por meio de consoles e APIs;
- Gestão de sessões privilegiadas: capacidade de estabelecer, gerenciar, gravar e reproduzir sessões privilegiadas, incluindo monitoramento em tempo real, filtragem de comandos e logs;
- Gestão de segredos: capacidade de gerenciar segredos como senhas, tokens, chaves SSH, entre outros, para máquinas, aplicações, serviços, scripts, processos e containers;
- Descoberta de contas: capacidade de descobrir, identificar e classificar contas privilegiadas por meio de varreduras pontuais e periódicas, incluindo sistemas e serviços;
- Automação de tarefas privilegiadas: capacidade de executar tarefas automáticas relativas a operações orquestradas e executadas em um conjunto de sistemas, incluindo o uso de extensões e bibliotecas para operações pré-configuradas;
- Elevação e delegação de privilégios: capacidade de controlar comandos em nível de execução, de modo que privilégios sejam concedidos somente quando autorizados e necessários, por meio de agentes instalados em sistemas operacionais;

Os três principais fabricantes de PAM segundo o Gartner são BeyondTrust, CyberArk, e Delinea. A BeyondTrust é lider de mercado e se destaca pela flexibilidade e controle granular em endpoints, oferecendo agentes locais para Windows, Linux e macOS, além de acesso remoto seguro. A CyberArk divide a liderança com a BeyondTrust, com soluções equivalentes para gerenciamento de contas privilegiadas. Já a Delinea, apesar de não ser lider, ainda consta no quadrante mágico, foca na simplicidade e agilidade, com uma plataforma mais baseada em navegador para fazer o gerenciamento de credenciais e acessos privilegiados.

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

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

2.8. Ampliação ou substituição da solução implantada

Não aplicável

2.9. Diferentes métricas de prestação do serviço e de pagamento

Não aplicável.

Com base no levantamento acima, as soluções de gerenciamento de acesso privilegiado (Privileged Access Management – PAM) concentram as tecnologias de segurança cibernética capazes de exercer o controle sobre acessos privilegiados e permissões para usuários, contas, processos e sistemas na forma de aquisição da solução, não tendo sido achado nenhuma contratação pública do objeto como serviço, no que tange o cerne da segurança institucional, sendo enfatizado, que o órgão público que faz a gestão do PAM.

Id	Descrição da solução (ou cenário)
1	Aquisição de solução de gerenciamento de contas e de acessos privilegiados Atualmente, a CLDF não possui uma solução de PAM
2	Contratação de solução de gerenciamento de contas e de acessos privilegiados como serviço, em ambiente terceirizado Atualmente, a CLDF não possui uma solução de PAM

3. ANÁLISE COMPARATIVA DAS SOLUÇÕES

Requisitos		Cenários	
		Aquisição de solução de gerenciamento de contas e de acessos privilegiados	Contratação de solução de gerenciamento de contas e de acessos privilegiados como serviço, em ambiente terceirizado
Negócio	Continuidade dos serviços de TIC	atende	atende
	Conformidade	atende	atende
	Manutenção e sustentabilidade	atende	atende
	Segurança e privacidade	atende	não atende
	Capacidade de prover as necessidades com suporte pelo prazo de 36 meses	atende	atende
	Alta disponibilidade	atende	atende
	Compatibilidade com o ambiente de soluções integradas da CLDF. A solução deve ser gerenciada pelos servidores da SEINF, em interface única, tornando a gestão do ambiente menos custosa em termos de pessoal, bem como com níveis reduzidos de riscos	atende	não atende

Tecnológico	Gestão de credenciais privilegiadas, gestão de sessões privilegiadas e gestão de segredos.	atende	atende
	Descoberta de contas, automação de tarefas privilegiadas e elevação e delegação de privilégios	atende	atende
	Gerenciamento e monitoração	atende	atende
	Escalabilidade e flexibilidade	atende	atende
	Auditoria e controle	atende	não atende
	Atualização tecnológica	atende	atende
Demais	Compatibilidade e integração	atende	atende
	Níveis de serviço	atende	atende
	Economicidade	atende	não foram encontrados preços públicos
Resultado da Análise		viável	não viável

4. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS E JUSTIFICATIVA

A contratação de uma solução de Gerenciamento de Acesso Privilegiado (PAM) como serviço, em ambiente terceirizado, não se mostra adequada para a CLDF, considerando os princípios de segurança da informação, governança de TI e conformidade regulatória aplicáveis ao setor público.

De acordo com as diretrizes da ISO/IEC 27001, a segurança da informação deve ser tratada como um pilar estratégico, especialmente em instituições governamentais. A terceirização de serviços críticos de segurança, como o gerenciamento de credenciais privilegiadas, pode introduzir riscos adicionais, incluindo a exposição indevida de dados sensíveis, perda de visibilidade sobre atividades privilegiadas e comprometimento da integridade dos controles internos.

A ISO/IEC 27002, que trata de controles específicos, recomenda que o gerenciamento de acessos privilegiados seja realizado com rigor, incluindo monitoramento contínuo, segregação de funções e aplicação do princípio do menor privilégio. A adoção de PAM como serviço pode dificultar a implementação plena desses controles, sobretudo quando o ambiente é gerido por terceiros.

Além disso, conforme orientações do NIST SP 800-53, é essencial que o controle de acesso se estenda não apenas aos servidores institucionais, mas também aos colaboradores terceirizados, garantindo que todos os usuários com privilégios elevados estejam sujeitos às mesmas políticas de segurança, auditoria e rastreabilidade.

Do ponto de vista da governança de TI no setor público, conforme preconizado pelo TCU, descritos na Estratégia Digital do TCU Consolidada (TCU, 2022), é recomendável que os órgãos públicos mantenham autonomia sobre seus ativos críticos, especialmente aqueles relacionados à segurança da informação, infraestrutura tecnológica e sistemas de missão institucional. A contratação de PAM como serviço pode comprometer essa autonomia, dificultando a adaptação às exigências legais, como a Lei Geral de Proteção de Dados (LGPD), e a conformidade com normativas específicas da administração pública.

Por fim, não foram identificadas contratações similares por outros órgãos públicos que sirvam como referência para estimativa de valores ou boas práticas, o que reforça a necessidade de cautela e análise aprofundada antes da adoção de tal modelo.

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 : Aquisição de solução de gerenciamento de contas e de acessos privilegiados										
Propostas/Preço Público										
Item	1	2	3	4	5	MEDIANA (para o cálculo dos valores discrepantes)	MÍNIMO (-50%)	MÁXIMO (+50%)	MEDIANA FINAL	MÉDIA FINAL

Solução de gerenciamento de contas e de acessos privilegiados (módulo de gerenciamento de contas e de sessões privilegiados, módulo de gerenciamento de elevação e delegação de privilégios e módulo de acesso seguro)	R$ 2.222.000,00	R$ 2.179.314,00	R$ 2.181.517,00	R$ 2.350.000,00	R$ 2.470.100,00	R$ 2.222.000,00	R$ 1.111.000,00	R$ 3.333.000,00	R$ 2.222.000,00	R$ 2.280.586,20
Serviço de instalação e configuração	R$ 121.500,00	R$ 140.000,00	R$ 130.432,00	R$ 122.000,00	R$ 170.350,00	R$ 130.432,00	R$ 65.216,00	R$ 195.648,00	R$ 130.432,00	R$ 136.856,40
Serviço de operação assistida	R$ 27.000,00	R$ 30.000,00	R$ 25.268,20	R$ 34.250,00	R$ 43.800,00	R$ 30.000,00	R$ 5.000,00	R$ 45.000,00	R$ 30.000,00	R$ 32.063,64
Serviço de capacitação	R$ 129.500,00	R$ 140.017,00	R$ 130.315,00	R$ 123.450,00	R$ 155.070,00	R$130.315,00	R$ 65.157,50	R$ 195.472,50	R$ 130.315,00	R$ 135.670,40
Custo Total										

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

a) Proposta 1, da empresa 7Secure- Valor R$ R$ 2.500.000,00 - Doc SEI 2166134
b) Proposta 2, da empresa Fasthelp R$ 2.489.331,00 - Doc SEI 2166133
c) Proposta 3, da empresa Cloud4Sec Valor R$ R$ 2.467.532,20 Doc SEI 2170259
d) Proposta 4, da empresa NCT Valor RR 2.629.700,00 Doc SEI 2172546
e) Proposta 5, da empresa Disruptec Valor R$ 2.839.320,00 Doc SEI 2173845

Também foram analisadas contratações similares em outros órgãos públicos válidos, conforme a seguir:

e) Preço público, Ministério da Comunicações Pregão 90003/2024 - Valor proporcional * Doc SEI 2172550 combinado com Doc SEI 2172556. O contrato expirou em abril de 2025, contudo temos um valor de refência de R$ 2.164.935,00, sem o item de serviço de instalação e configuração, que na média fica próximo do valor alcançado pela propostas comerciais.

* Foi readequado com um valor proporcional, na proposta Doc SEI 2172550 para o item "2" para 250 dipositivos em vez de 400, e no item "4" para 6 alunos em vez de 5, com duas turmas. Tanto para o item "2" como o "3" foram ajustados para 36 meses em vez de 12 meses. Ambos da proposta supracitada.

5.2. MAPA COMPARATIVO DOS CUSTOS TOTAIS

Descrição da solução	Estimativa de custos ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
Aquisição de solução de gerenciamento de contas e de acessos privilegiados	R$ 2.512.747,00	R$ 0,00	R$ 0,00	R$ 2.512.747,00

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 escolha de uma solução de gerenciamento de contas e de acessos privilegiados (PAM), *on-premise*, gerida internamente pelo próprio órgão, é a mais adequada que a contratação como serviço por várias razões.

Entre as principais razões, a segurança da informação é uma prioridade máxima para qualquer entidade governamental. Assim, ao manter a solução de PAM internamente, garante que o órgão tenha controle total sobre as políticas de segurança e a gestão de acessos, minimizando os riscos de vazamento de dados sensíveis e de comprometimento da segurança, mais vuneráveis na contratação como serviço.

Além disso, a gestão interna permite que o órgão aplique e monitore rigorosamente todas as políticas de segurança, tanto para funcionários internos quanto para funcionários terceirizados. Isso assegura que todos os acessos privilegiados sejam gerenciados de acordo com as diretrizes específicas do órgão, sem depender de terceiros.

Outro ponto crucial é a conformidade com regulamentações e normas de segurança específicas do setor público. A gestão interna de uma solução de PAM facilita a garantia de que todas as exigências legais e normativas sejam cumpridas, uma vez que o órgão mantém controle direto sobre todos os processos de segurança.

A resposta rápida e eficaz a incidentes de segurança é outro benefício significativo da gestão interna. Em um ambiente *on-premise*, a comunicação e

a coordenação são mais ágeis, permitindo que o órgão reaja prontamente a ameaças e vulnerabilidades, protegendo melhor suas informações sensíveis.

Além disso, a solução, nessa modalidade, pode ser customizada para atender às necessidades específicas do órgão, proporcionando maior flexibilidade e adaptabilidade. Isso é particularmente importante em um ambiente público legislativo, onde as exigências de segurança podem ser únicas e complexas.

Por fim, a gestão interna de uma solução de PAM promove a capacitação e o desenvolvimento de habilidades dos funcionários do órgão, fortalecendo a equipe de segurança e aumentando a resiliência contra ameaças cibernéticas.

Por estas razões, a escolha é pela de Solução 1 - Aquisição de solução de gerenciamento de contas e de acessos privilegiados

7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

No estudo das soluções disponíveis no mercado, concluiu-se que os principais fornecedores baseiam seus produtos e serviços em função do quantitativo de dispositivos gerenciados e/ou na quantidade de usuários com acessos privilegiados. Tais métricas dimensionam a quantidade e a capacidade dos servidores ofertados, os licenciamentos de softwares associados e os níveis de serviço contratados.

Como dito anteriormente, a solução pretendida servirá como interface de segurança, que atuará como blindagem para todo e qualquer acesso administrativo de TI. Logo, foi realizado levantamento do parque computacional de forma a considerar todos os ativos corporativos e todos os usuários que possuam algum nível de acesso privilegiado. No levantamento foram detalhados quantitativos, sistemas operacionais, contas, serviços, agentes, entre outros fatores, que mostraram necessários para estimar objetivamente a demanda. Através dos relatórios, SEI (2365741) e SEI (2365755), combinado com o 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" , com os dados do Portal da Transparência CLDF, foi possivel identificar esses quantitativos e identificar o universo de usuários que necessitam de licenciamento para uso de credenciais, em acessos a aplicações, inclusive as mais críticas, conforme Quadros abaixos dos anos de 2018 até 2023.

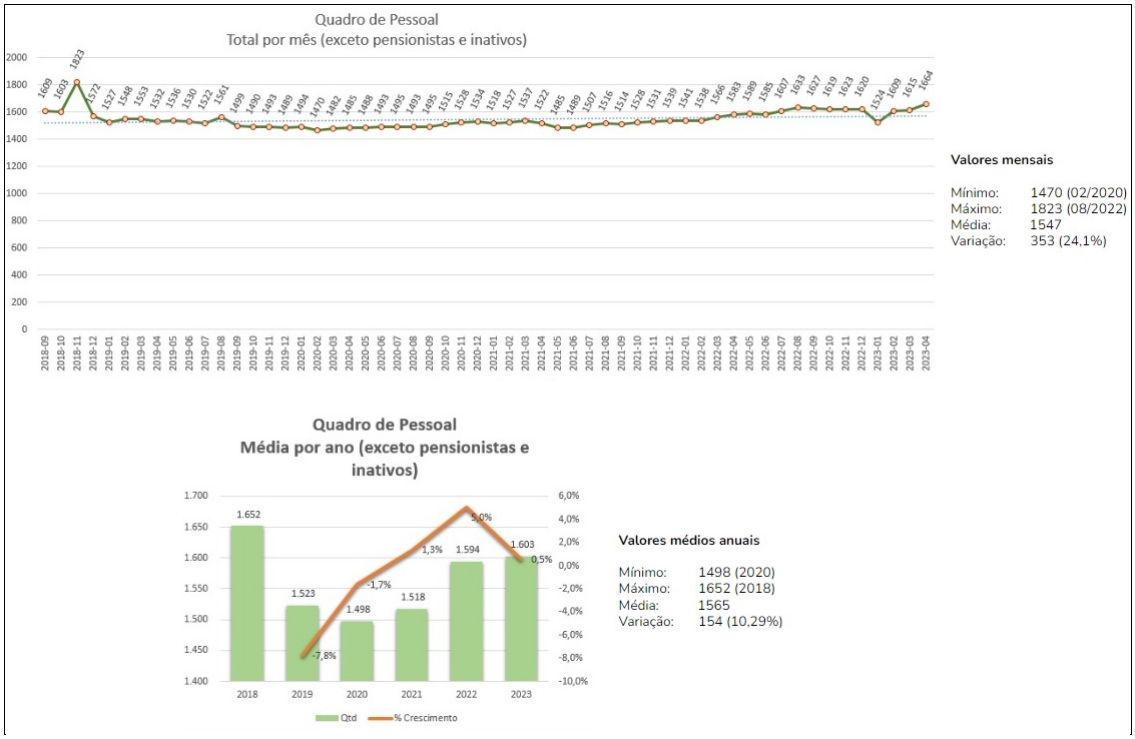

Imagem 7.1 - Quadro de pessoal (Fonte: compilado dos dados do Portal da Transparência da CLDF)

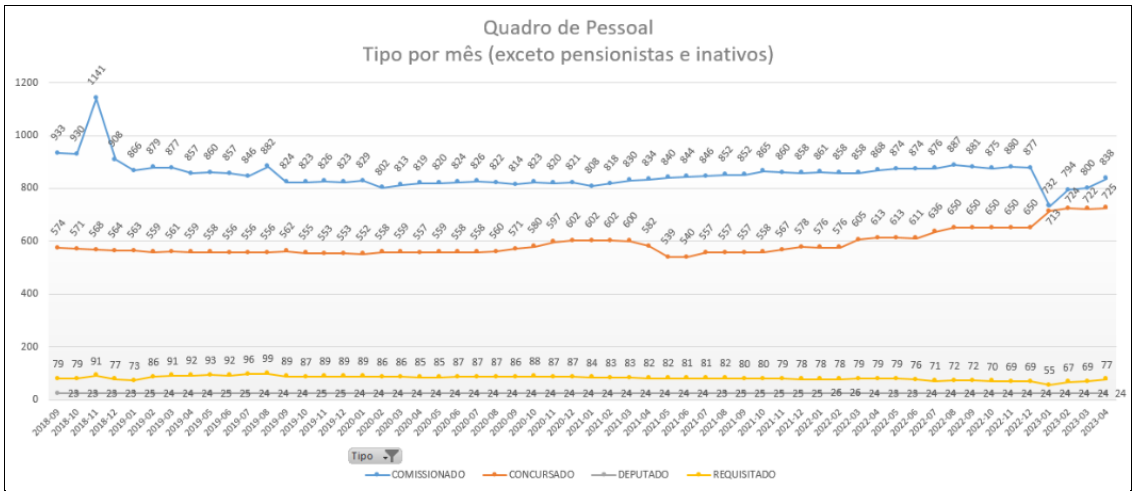

Imagem 7.2 - Quadro de pessoal por tipo de servidor (Fonte: compilado dos dados do Portal da Transparência da CLDF)

Para o ano de 2025, manteve-se a tendência indicada no ETP supracitado, na projeção de crescimento em estimativa apontada no mesmo estudo e mantida a representação conforme dados Quantitativo de pessoal - Portal da Transparência - CLDF. "https://www.cl.df.gov.br/web/portal-transparencia/quantitativo-de-pessoal", em que, para setembro/2025, de modo geral, há 937 comissionados, 782 concursados, 24 deputados e 94 requisitados.

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.

Assim, conforme os relatórios supracitados, a solução pretendida foi projetada para prover credenciais e acessos privilegiados para, pelo menos, 250 (duzentos e cinqueta) dispositivos e 1.000 (um mil) aplicações, atendendo ao mesmo tempo, pelo menos, 1.500 (um mil e quinhentos) usuários privilegiados. Da mesma maneira, com as informações do Relatório SO e VMs (2365755), deverá incluir o fornecimento de agentes locais para 50 (cinquenta) servidores Microsoft Windows e 200 (duzentos) servidores Unix/Linux. Essa definição detalhada promove a possibilidade de participação e a competição entre os diversos fabricantes, independente da forma de comercialização de softwares, levando-se em conta os aspectos de economicidade, eficácia, eficiência e padronização.

8. DESCRIÇÃO DA SOLUÇÃO DE TI A SER CONTRATADA

Aquisição de solução de gerenciamento de contas e de acessos privilegiados, 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 solução de gerenciamento de contas e de acessos privilegiados, com serviços de instalação e configuração, operação assistida, capacitação, com garantia e suporte de 36 meses.

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	Solução de gerenciamento de contas e de acessos privilegiados	1	R$ 2.222.000,00	R$ 2.222.000,00
2	Serviço de instalação e configuração	1	R$ 130.432,00	R$ 130.432,00
3	Serviço de operação assistida	1	R$ 30.000,00	R$ 30.000,00
4	Serviço de capacitação	1	R$ 130.315,00	R$ 130.315,00
Total				**R$2.512.747,00**

DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da CLDF.
Programa de Trabalho: 01.126.8204.2557.2627 - GESTÃO DA INFORMAÇÃO E DOS SISTEMA DE T.I. - CLDF.
Elemento de Despesa: 33.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica.

10. RESPONSÁVEIS

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO				
INTEGRANTE	**NOME**	**MATRÍCULA**	**LOTAÇÃO**	**RAMAL**
Requisitante	FÁBIO VIRGÍLIO DE SOUZA NEVES	24554	SEINF	8321
Técnico	AIMBERE GIANNACCINI	18327	SEINF	8321

NOME DA ÁREA TÉCNICA DE TI	NOME DO CHEFE OU SUBSTITUTO	MATRÍCULA	RAMAL
SEINF	AIRTON BORDIN JUNIOR	23994	8344

11. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

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

WALÉRIO OLIVEIRA CAMPORÊS

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 **FABIO VIRGILIO DE SOUZA NEVES - Matr. 24554**, **Consultor(a) Técnico-Legislativo**, em 24/11/2025, às 18:24, conforme Art. 30, do Ato da Mesa Diretora n° 51, de 2025, publicado no Diário da Câmara Legislativa do Distrito Federal nº 62, de 27 de março de 2025.

Documento assinado eletronicamente por **AIMBERE GIANNACCINI - Matr. 18327**, **Integrante Técnico**, em 24/11/2025, às 18:26, conforme Art. 30, do Ato da Mesa Diretora n° 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 25/11/2025, às 17:48, conforme Art. 30, do Ato da Mesa Diretora n° 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: **2356310** Código CRC: **7B6E1D45**.