Governo do Distrito Federal
Secretaria de Estado de Economia do Distrito Federal
Unidade de Segurança, Centro de Dados e Mensageria
Coordenação de Centro de Dados

Estudo Técnico Preliminar - SEEC/SETIC/SUBINFRA/USCD/COCED

1 - DESCRIÇÃO DO OBJETO
Este Estudo Técnico Preliminar com o objetivo de avaliar alternativas para a implantação de uma solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web e mobile contemplando serviços de suporte especializado, treinamento, manutenção preventiva e corretiva com atualização e upgrades de versões, pelo período de 36 (trinta e seis) meses

2 - DESCRIÇÃO DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO Art. 18 da Lei. 14.133, § 1º, I. **Atendimento ao Art. 57 e inciso I do art. 60 do DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023** **Art. 11 , Inciso I. IN SGD/ME n.º 94 de 23 de dezembro de 2022**
A Secretaria Executiva de Tecnologia da Informação e Comunicação (SETIC) é responsável pelo apoio técnico em TIC. Ela atua como provedora de serviços para a SEEC/DF, órgão central de planejamento e gestão do Governo do Distrito Federal entre outros.. Mas não é só, além de gerenciar os recursos técnicos correlatos à Pasta, a SETIC exerce um importante papel na Gestão Estratégica, atuando como principal proponente das ações estruturantes de TIC, bem como fomentando iniciativas de implantação e difusão de mecanismos de Governança e Gestão de TIC para todo Complexo Administrativo do GDF. Nesse sentido, ao tratarmos da infraestrutura necessária para dar sustentação às soluções tecnológicas, a SETIC dispõe do Centro de Dados Corporativo do DF (CeTIC), ambiente tecnológico composto por soluções integradas de hardware e software, para hospedagem dos sistemas, contemplando seu processamento e armazenamento de dados em larga escala, para todos os órgãos e entidades da Administração Direta e Indireta do Distrito Federal, inclusive na modalidade em nuvem, como a GDFCloud.

Dentre os sistemas, soluções e aplicações sustentadas pela SETIC), destacam-se:

Serviços para o cidadão:

- Aplicativo Economia/DF: Este aplicativo provavelmente oferece funcionalidades relacionadas a serviços econômicos e financeiros no Distrito Federal, como informações sobre impostos, taxas, contribuições e outros serviços financeiros relevantes para os cidadãos e empresas.
- Aplicativo e-GDF: Este aplicativo deve ser uma plataforma centralizada para o acesso a serviços governamentais digitais. Ele pode incluir funcionalidades como consulta de documentos, solicitação de serviços, acesso a informações institucionais, entre outros.
- Agendamento: Este serviço pode estar relacionado ao agendamento online de serviços públicos, permitindo aos cidadãos reservar horários para atendimentos em diferentes departamentos do governo de forma mais eficiente e conveniente.
- Portal de Serviços da Receita do DF: Este portal é provavelmente dedicado a serviços relacionados à receita do Distrito Federal, como declaração e pagamento de impostos, consulta de débitos, emissão de certidões negativas, entre outros.
- AgênciaNet: Este serviço pode estar relacionado ao atendimento virtual de diversas agências governamentais, oferecendo uma variedade de serviços e informações online.
- Receita Web: Este serviços oferecendo uma variedade de serviços e informações online voltados para receita.
- Sisconep Cidadão: Plataforma de controle e acompanhamento de emendas parlamentares, projetos e orçamentos, permitindo aos cidadãos acompanhar a alocação e o uso de recursos públicos.
- Nota Legal: Este serviço esta relacionado a um programa de incentivo fiscal, no qual os cidadãos acumulam créditos ao solicitar a inclusão do CPF em notas fiscais durante compras, podendo utilizar esses créditos para abatimento em impostos ou recebimento de reembolsos.

Serviços para apoio aos processo de negócio do Governo do Distrito Federal, destacam-se aplicativos como:

- Sistema Eletrônico de Informação (SEI): Ferramenta para gestão de documentos e processos eletrônicos, focada em agilizar a tramitação interna e reduzir o uso de papel.
- Sistema Integral de Gestão Governamental (SIGGO): Plataforma para integrar e gerenciar as informações financeiras, orçamentárias e contábeis do governo.
- Sistema de Gestão Tributária e Financeira (SITAF): Sistema para administrar aspectos tributários e financeiros, melhorando a eficiência na coleta e gestão de receitas.
- Sistema de Atividades da Administração Tributária (SIGEST): Ferramenta específica para otimizar as operações da administração tributária.

- Novos Sistema de Gestão de Pessoas (SIGEPE): Solução para gerenciar todos os aspectos relacionados aos recursos humanos, incluindo folha de pagamento e benefícios.
- Sistema de Gestão de Recursos Humanos (SIGRH): Sistema para a administração e o controle das atividades de recursos humanos.
- Sistema de Recadastramento dos Servidores do GDF (RECAD): Plataforma para o recadastramento periódico dos servidores públicos, visando atualizar e validar suas informações.
- Sistema de Atendimento de Perícia Médica (SIAPMED): Sistema destinado à gestão e ao agendamento de perícias médicas para servidores.
- Sistema de Cobranças da Receita (SICOB): Ferramenta para otimizar o processo de cobrança de receitas tributárias e não tributárias.
- Sistema de Gestão do Patrimônio (SISGEPAT): Sistema para controle e gestão dos bens patrimoniais do governo.
- Sistema de Capitalização de Recursos (SISCAP): Plataforma para a gestão de fundos e recursos capitalizados pelo governo.
- Sistema de Patrimônio Público (SPP): Ferramenta para a administração dos bens públicos, focando na transparência e eficiência.
- Sistema de Controle de Emendas Parlamentares (SISCONEP): Sistema para gerir e monitorar a aplicação de emendas parlamentares.
- Sistema de Elaboração e Gestão de PDTICS: Ferramenta para a elaboração e gestão de planos diretores de TI.
- Gestão de Rubricas: Sistema para gerenciar rubricas orçamentárias e financeiras.

Dada a relevância dos serviços e soluções suportadas pela SETIC, bem como o significativo volume de dados custodiados e processados pelo parque computacional, recai a justificativa para investir recursos na busca de uma Solução de inspeção e segurança de credenciais em rede e aplicações web, dada a urgência na implementação de ferramentas e soluções que possam minimizar os pontos de falha de segurança dos sistemas em custódia, hospedados e processados pela SETIC) garantindo assim a performance e disponibilidade das aplicações e sistemas, reduzindo a possibilidade de indisponibilidade de acesso aos serviços, bem como promovendo maior rastreabilidade quanto às tentativas de ataques efetuados dentro do ambiente computacional.

Nesse contexto, devido ao aumento significativo do número de ataques cibernéticos, potencializados pela “onda” crescente do uso de soluções de tecnologia e aplicações de TI, tem-se observado um significativo avanço do setor governamental, no sentido de direcionar esforços para a criação de diretrizes, atos normativos e legais, bem como o investimento de recursos relacionados ao tema Governança e Gestão de TI.

Espera-se que a solução a ser contratada seja capaz de gerar relatórios que suportem a efetividade dos controles de segurança, assim como, por meio de seus recursos e funcionalidades possibilite a auditoria de informações de acessos tanto de administradores quanto dos usuários, trazendo uma visão global e detalhada das permissões de acesso, modificações não necessárias aos recursos, arquivos ou caixas de correio, acessos indevidos em aplicações, detectando atividades não autorizadas de processamento de informações, monitorando a autenticação de aplicações, identificando riscos bom

base na análise comportamental dos usuários, bem como demais recursos e funcionalidades que serão estudadas e analisadas por meio do Estudo Técnico Preliminar.

A demanda encontra ainda o amparo nas atribuições legais da SETIC, na medida em que a solução que será futuramente contratada permitirá apoiar o desenvolvimento de projetos de TIC corporativa voltados às melhores práticas de gestão de tecnologia da informação, inovação institucional, racionalização dos processos de trabalho e automatização de serviços públicos, bem como a melhoria na Gestão e Governança da Instituição, propiciando a manutenção da imagem institucional, bem como a garantia da confiança da população com a instituição e com os serviços ofertados.

Com base em todo o contexto, a demanda justifica-se em razão da necessidade de se desenvolver estratégias que possam inibir a tentativa de busca e vazamento de informações que possam comprometer a segurança de dados dos órgãos, secretarias e Autarquias no âmbito da administração pública, bem como reduzir riscos de ataques ao ambiente computacional.

Importante ressaltar que as informações tratadas por essa Instituição são ativos valiosos para a eficiente prestação dos serviços públicos, é por este motivo que se busca, através da presente demanda, desenvolver ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, assegurando a qualidade dos serviços públicos esperados pela população, garantindo a segurança com relação à guarda de "dados sensíveis" pelo governo, através da adoção de medidas rigorosas de segurança para acesso dessas informações.

Por fim, busca-se estar em conformidade com as normas e padrões de segurança da informação trazidos pela Lei Geral de Proteção de Dados LGPD, aos preceitos legais que regem a responsabilidade sobre os dados gerados, armazenados, tratados e trafegados em ambiente dessa administração.

Deste modo, resta justificada a necessidade do presente estudo, para avaliar as alternativas e requisitos para implantação de uma solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web contemplando serviços de suporte especializado, operação assistida, treinamento, manutenção preventiva e corretiva com atualização e upgrades de versões.

A futura contratação se dará por meio de Ata de Registro de Preços – ARP, pois o objeto deste processo poderá ser adquirido de forma parcelada, permitindo uma evolução gradual do projeto com base no volume de licenças necessárias. Portanto, a escolha da futura contratação por ARP se justifica tanto do ponto de vista técnico quanto do ponto de vista legal, conforme previsão expressa no inciso II, do Artigo 190, Decreto nº. 44.330/2023.

Importante destacar que o Sistema de Registro de Preços poderá ser adotado nas hipóteses em que: I - pelas características do bem ou do serviço, haja necessidade de contratações frequentes; II - for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa; III - for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo; IV - quando, pela natureza do objeto ou situação fática, não for possível definir previamente o quantitativo a ser demandado pela Administração; V - exista expectativa de crédito orçamentário futuro.

O Registro de Preços apresenta-se como ferramenta comprovadamente eficiente na busca por melhores preços, mantendo-os registrados para uma futura aquisição, conforme a necessidade e disponibilidade de recursos orçamentários, atendendo assim a necessidade de controle e racionalização do gasto público.

Assim, a adoção dessa prática tem como um de seus objetivos o princípio da economicidade, que em termos práticos significa ganhos reais na economia de recursos financeiros, uma vez que a contratação será de larga escala, e por isso a tendência dos preços é diminuir.

Em relação a eventuais adesões por órgãos não participantes, conforme determina o Art. 22. do Decreto Distrital nª 39.103/18, desde que devidamente justificada a vantagem, a ARP, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública que não

tenha participado do certame licitatório, mediante anuência do órgão gerenciador.

Outros entes da Administração Pública poderão, igualmente, utilizar-se da ARP, como caronas, desde que observadas as condições estabelecidas no referido Decreto.

> "§ 2º Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o órgão gerenciador e órgãos participantes.
>
> § 3º As aquisições ou contratações adicionais a que se refere este artigo não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.
>
> § 4º O instrumento convocatório deverá prever que o quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao quíntuplo do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

A ata de registro de preços terá validade de 12 meses, possibilitando a eventual aquisição da SETIC dentro do prazo limite definido pela legislação aplicável.

Reforçamos a importância crítica de investir em soluções tecnológicas de proteção contra-ataques a credenciais, especialmente no contexto atual de crescente ameaça cibernética e vazamento de dados sensíveis. É fundamental reconhecermos que os ataques visando comprometer credenciais de usuários representam uma das principais ameaças enfrentadas pelas organizações governamentais e empresas em todo o mundo.

Uma solução tecnológica dedicada à proteção contra-ataques a credenciais é vital para fortalecer as defesas cibernéticas da SUTIC e mitigar o risco de ataques bem-sucedidos, como o incidente ocorrido no ano de 2023 conforme processo 04033-00015950/2023-25, no qual milhões de dados pessoais foram vazados, resultando em um boletim de ocorrência registrado". Esse incidente ressalta a necessidade urgente de implementar medidas proativas para proteger informações sensíveis e garantir a integridade dos dados.

Uma solução tecnológica especializada nesse campo oferecerá diversos benefícios significativos. Em primeiro lugar, a solução pode detectar e bloquear tentativas de comprometimento de credenciais em tempo real, identificando padrões de acesso suspeitos e atividades maliciosas. Cabe ainda citar que o uso de técnicas avançadas de dissuasão de atividades maliciosas aumentará substancialmente a segurança das credenciais dos usuários, tornando as aplicações web menos vulneráveis a ataques de força bruta.

A redução do risco de ataques bem-sucedidos terá um impacto positivo direto na integridade operacional e na continuidade dos serviços governamentais, garantindo a continuidade no cumprimento de nossa missão institucional de forma eficaz e segura.

Em síntese, a aquisição de uma solução tecnológica de proteção contra-ataques a credenciais é estratégica e essencial para fortalecer nossas defesas cibernéticas, mitigar o risco de ataques bem-sucedidos e proteger os dados sensíveis dos cidadãos. Tal solução não apenas contribuirá na prevenção de incidentes de vazamento de dados, mas também aprimorará a postura de segurança cibernética institucional como um todo, possibilitando enfrentar as crescentes ameaças cibernéticas com eficácia e resiliência.

3 - ALINHAMENTO EM RELAÇÃO AOS OBJETIVOS ESTRATÉGICOS - PDTI Art. 18 da Lei. 14.133, § 1º, II.

Atendimento ao Art. 58 DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023.

PDTI/SEEC 2023-2026 – (130739035) Art. 2 , Inciso XXV. IN SGD/ME n.º 94 de 23 de dezembro de 2022

.

ITEM	INICIATIVAS ESTRATÉGICAS SEPLAD/DF	OBJETIVOS ESTRATÉGICOS	ÁREA RESPONSÁVEL	EXECUTIVA RESPOSÁVEL
16	Implantação de Soluções de Segurança para o CeTIC-DF e Rede GDFNet.	CONSOLIDAR A TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO COMO PILAR ESTRATÉGICO ESSENCIAL AS ATIVIDADES DO GDF	INOVA UMARC	SECONTI

OBJETIVO ESTRATÉGICO 1 (OE1): GESTÃO DOS SERVIÇOS DE TIC BASEADA NAS MELHORES PRÁTICAS	
INICIATIVAS ESTRATÉGICAS REFERENTES AO OE1	IE3 - Estabelecimento de norma de segurança da informação interna, em conformidade com a PoSIC-DF. IE6 - Melhoria contínua da infraestrutura de TIC. IE8 - Investimento no aumento da produtividade e otimização dos recursos de TIC
OBJETIVO ESTRATÉGICO 2 (OE2): ELEVAÇÃO DA MATURIDADE DA GOVERNANÇA DE TIC	
INICIATIVAS ESTRATÉGICAS REFERENTES AO OE2	IE11 - Planejamento dos investimentos em hardware e software IE12 - Planejamento das contratações de soluções de TIC baseado nas melhores práticas. IE14 - Gestão eficiente dos ativos de TIC.

3.1 - NECESSIDADE DE TIC.

O Plano Diretor de Tecnologia da Informação da Secretaria de Estado de Economia do Distrito Federal é um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação para atendimento às necessidades tecnológicas e de informação do órgão. A necessidade da contratação em tela consta do **PDTI/SEEC 2023-2026 – (130739035)** sob a classificação de **Macro Requisitos Tecnológicos da Solução de TIC.**

ID.	NECESSIDADE DE TIC.
SUTIC INFRA 11	Solução de Segurança Integrada.
SUTIC INFRA 33	Serviços Preventivos de Segurança da Informação e apoio a Análise Forense, sob demanda.
SUTIC-INFRA 36	Contratação de solução de inspeção e análise de comportamento dos usuários em servidores Windows e Active Directory.
SUTIC INFRA 43	Plataforma de monitoramento e segurança cibernética (cibersegurança).

4 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES.

4.1 - Requisitos da Contratação Art. 18 da Lei. 14.133, § 1º - III.

Atendimento ao inciso II, art. 60 - DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023

Art. 11 , Inciso I. IN SGD/ME n.º 94 de 23 de dezembro de 2022

1.	Solução de Gerenciamento de Identidade e Acesso (IAM): Ferramenta que ofereça controle efetivo sobre o acesso a sistemas e dados, com suporte a autenticação multifatorial e gerenciamento de privilégios.
2.	Painel integrado de eventos de inspeção e segurança de credenciais.

3.	Proteção contra Ameaças Avançadas (ATP): Capacidade de detectar e responder a ameaças avançadas, especialmente em ambientes web e mobile.
4.	**S**olução de inspeção e segurança de credenciais em ambiente de rede
5.	Solução de inspeção e segurança de credencias em aplicações web.
6.	Monitoramento Contínuo e Análise de Comportamento do Usuário: Solução para monitorar comportamentos anormais de usuários e entidades, com suporte para aprendizado de máquina e análise heurística.
7.	Serviços de Suporte Especializado e Treinamento: Inclusão de serviços de suporte técnico especializado, com treinamento para a equipe interna na operação e manutenção da solução.
8.	Serviços técnicos especializados de Operação assistida por todo o período contratado
9.	Serviço de Implantação e Configuração.
10.	Manutenção Preventiva e Corretiva com Atualizações e Upgrades: Garantia de atualizações regulares, incluindo medidas preventivas e corretivas, e upgrades para novas versões da solução para assegurar a máxima eficácia e conformidade com as normativas vigentes.
11.	Segurança de Dados: A solução deve estar em conformidade com a legislação brasileira, especialmente a Lei 14.133/2021, e padrões de segurança e privacidade de dados, como a LGPD (Lei Geral de Proteção de Dados).
12.	Integração com Sistemas Existentes: Capacidade de integração com infraestrutura e sistemas existentes, tanto em ambientes on-premises quanto em nuvem.
13.	Relatórios e Auditorias: Ferramentas para geração de relatórios detalhados e recursos de auditoria, para facilitar a supervisão e o cumprimento de regulamentos.

4.2 - Estimativas das quantidades para a contratação Art. 18 da Lei. 14.133, § 1º - IV.

Atendimento ao inciso V, art. 60 - DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023

Para o dimensionamento adequado da solução, a Equipe de Planejamento conduziu um levantamento estimativo das credenciais, aplicações e outras informações relevantes que impactam diretamente na quantidade a ser licitada. Considerando que se trata de uma futura ata de registro de preços

e diante da impossibilidade de prever com precisão o número de usuários externos durante a vigência do contrato, apresentamos abaixo as quantidades projetadas para o período contratual.

Quantidade total de credenciais por aplicação web (cenário atual):

APLICAÇÃO WEB	CREDENCIAIS
SIGGO	2.193
SITAF	82.000
SISGEPAT	3.702
AGENCIANET	38.118
RECEITAWEB	2.530
SIGEST	2.439
NOTA LEGAL / PSV	1.533.617
SEI	257.297
TOTAL	**1.921.896**

A definição do quantitativo de 1.921.896 licenças de segurança, conforme detalhado na tabela acima, baseou-se numa análise criteriosa dos acessos aos sistemas críticos administrados pela Secretaria Executiva de Tecnologia da Informação e Comunicação (SETIC). Esta análise envolveu a revisão da quantidade de usuários ativos, a frequência de acesso e as necessidades específicas de monitoramento e auditoria de cada sistema.

Projeta-se o seguinte quantitativo a ser contratado:

- 500.000 (quinhentos mil) credenciais de usuários de aplicações web;
  - 500.000 (quinhentos mil) credenciais de usuários x 4 (pacotes)= 2.000.000 (dois milhões de credenciais).
- 15.000.000 (quinze milhões) de eventos de autenticação a cada 30 dias.
- Quando a mesma credencial for utilizada em mais de uma aplicação, deverá ser contabilizada apenas uma credencial.

Itens para solução:

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE ESTIMADA
1	Pacote de licença de uso para solução baseada em software para inspeção e segurança de credenciais em rede e aplicações WEB pelo período de 36 (trinta e seis) meses.	Licença de uso	4
2	Pacote de serviço de Implantação e Configuração	Serviço Unitário	4
3	Pacote de serviço técnico especializado de operação assistida.	Serviço Unitário	4
4	Treinamento	Serviço (Turma)	1

4.3. DA DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS TÉCNICOS DA DEMANDA

Art. 18 da Lei. 14.133, § 1º - VII, VIII e XII.

Atendimento ao inciso II, art. 60 - DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023

REQUISITOS DE SEGURANÇA.

1. A Contratada deverá conhecer todas as normas, políticas e procedimentos de segurança estabelecidos pela SUTIC para execução do Contrato.
2. Não será permitido, salvo justificado, que o ambiente seguro seja acessado por pessoas além daquelas necessárias para a prestação de serviços do objeto contratado.
3. O acesso dos profissionais da Contratada às dependências da SUTIC estará sujeito às suas normas referentes à identificação (crachá funcional), trajes, trânsito e permanência em suas dependências.
4. A Contratada responsabilizar-se-á integral e solidariamente pelos atos praticados de seus empregados e/ou prestadores de serviço nas dependências da SUTIC ou mesmo fora delas, que venham a causar danos ou colocar em risco o patrimônio dessa administração.

REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS.

REQUISITOS SOCIAIS.

1. Na execução de tarefas no ambiente da SUTIC, os funcionários da Contratada deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio

público. Deverão ainda portar identificação pessoal, conforme as normas internas da Instituição.

REQUISITOS AMBIENTAIS,

1. Os serviços prestados pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e material consumidos, bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela SUTIC.
2. A Contratada deverá atender, quando da execução do objeto do contrato, os critérios de sustentabilidade ambiental previstos na legislação pertinente, quando couber.
3. As configurações de hardware e software deverão ser executadas visando alto desempenho com o uso racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos.

A solução de inspeção e segurança de credenciais em rede e aplicações web e mobile considera que as licenças de software, para esse tipo de solução, não são por usuário, mas por credenciais a serem geridas e deverá atender, no mínimo, aos seguintes requisitos técnicos:

ITEM 1 - LICENÇA DE USO PARA SOLUÇÃO BASEADA EM SOFTWARE PARA INSPEÇÃO E SEGURANÇA DE CREDENCIAIS EM REDE E APLICAÇÕES WEB PELO PERÍODO DE 36 (TRINTA E SEIS) MESES.

Disponibilizar licenciamento com as seguintes capacidades mínimas de proteção e inspeção

Para cada pacote de inspeção e segurança de credenciais em rede e aplicações web, será licenciado as seguintes quantidades:

500.000 (quinhentos mil) credenciais de usuários de aplicações web;

15.000.000 (quinze milhões) de eventos de autenticação a cada 30 dias.

Quando a mesma credencial for utilizada em mais de uma aplicação, deverá ser contabilizada apenas uma credencial

REQUISITOS FUNCIONAIS PARA INSPEÇÃO E PROTEÇÃO DE CREDENCIAIS EM APLICAÇÕES WEB:

Comunicar-se através de API HTTP REST ou UDP com a aplicação web protegida, calculando e fornecendo em tempo real um score de risco e o nível de risco que este score representa, para cada evento de autenticação que ocorre em uma dada aplicação.

Assegurar a comunicação entre a solução e a aplicação web protegida através de criptografia de chaves simétricas.

Possibilitar a criação e configuração de políticas de risco, possuindo no mínimo 4 níveis de risco parametrizáveis a serem definidos em cada política.

Fornecer para cada autenticação analisada o score de risco processado acompanhado da ação (permitir, notificar, desafiar ou bloquear) indicada para o nível de risco do evento em questão, de acordo com a política definida.

Possibilitar o agrupamento de credencias, de modo que uma credencial possa estar associada a mais de uma aplicação web protegida.

Possibilitar a definição de mais de uma fonte de autenticação para uma única aplicação web protegida.

Não exigir tokens, dispositivos móveis, códigos ou outras informações adicionais para o processamento de eventos.

Ser capaz de processar e fornecer o score de risco tanto para autenticações com a credencial e senha corretos como para autenticações com credencial e/ou senha incorretos.

Possuir uma base de inteligência de segurança para ser utilizada na mensuração do risco dos acessos, construída com informações próprias e públicas (OSINT), de modo a identificar IPs de má reputação e/ou utilizados para serviço de proxy.

Realizar a mensuração de risco no processo de autenticação sem armazenar e sem ter acesso a senha da credencial em questão, em nenhuma hipótese.

Construir padrão de comportamento de uma credencial com base no histórico de seu uso, composto minimamente por navegador, dispositivo, localização geográfica (cidade e país), sistema operacional, identificador do provedor de internet.

Identificar desvios no padrão de comportamento de uma credencial, possibilitando o envio de notificações, apresentação de desafios (token, captcha ou similares) e bloqueio de acesso, a depender da política de risco definida.

Realizar a mensuração de risco de todos os acessos levando em consideração o padrão de comportamento da credencial e a base de inteligência de segurança.

Todos os eventos processados e armazenados pela solução deverão ser georreferenciados de acordo com o endereço IP de origem, contendo minimamente país, cidade, latitude e longitude.

Permitir a notificação de usuários com base em política de risco, através do disparo via SMTP de e-mail, possibilitando a redação de mensagem personalizada em editor HTML, contendo detalhes do evento em questão como cidade de acesso, data e hora, ip de origem, navegador e um link para que o usuário responda se reconhece o acesso ou não.

Inserir no padrão de comportamento da credencial novas informações quando o usuário confirma através da notificação recebida a veracidade do acesso.

Possibilitar o envio de e-mail para administrador quando um usuário nega a veracidade de um acesso através da notificação recebida.

Ser capaz de bloquear o processo de autenticação de usuários com base no score de risco do evento, mesmo quando a credencial e a senha forem corretamente imputadas no ato da autenticação.

Identificar ataques do tipo “força bruta”, elevando de forma automática e proporcional o score de risco do IP de origem do acesso com base no número de tentativas de autenticações fracassadas em um curto intervalo de tempo.

A reputação das origens detectadas como geradores de ataques de força bruta deverá decair após determinado tempo, e o tempo de decaimento da reputação deverá aumentar em função da recorrência de tentativas de ataques de força bruta.

Enviar eventos, cifrados nativamente com chave simétrica, via webhook para URL a ser configurada em interface gráfica, com base na política de risco definida.

Elevar o score de risco de uma credencial ao detectar mudança geográfica de longa distância.

Identificar os top 10 usuários que representam maior atividade de risco acumulado em um intervalo de tempo escolhido, informando o nome do usuário (credencial) e score de risco acumulado.

Segmentar os eventos processados por credencial, possibilitando navegar por todos os eventos de uma dada credencial, informando no mínimo os seguintes detalhes de cada evento: Cidade, coordenadas geográficas, nome do navegador utilizado, nome do dispositivo utilizado no acesso, endereço ip de origem, score de risco e resultado da ação com base na política definida, código identificador do ISP (internet service provider) e descritivo com análise do evento.

Possuir gráfico que represente os eventos de uma credencial específica em um intervalo de tempo escolhido, distinguindo-os pelos níveis de risco definidos em política.

Possuir dashboard para visualização de eventos no formato de representação de mapa geográfico que possibilite distinguir diferentes níveis de risco, detalhando informações como cidade, usuário, score de risco do evento, data e hora do evento.

Possuir dashboard para visualização do risco organizacional em um intervalo de tempo escolhido, segmentado por aplicação protegida ou não, distinguindo o volume de eventos que representam o risco mitigado, o risco em mitigação (pendente) e o risco assumido.

Possuir dashboard para identificação de ataques, contendo minimamente as seguintes estatísticas:

Endereços IPs com maior incidência de credenciais únicas autenticadas com sucesso e com falha na autenticação;

Credenciais com maior incidência de acessos originados em cidades distintas autenticadas com sucesso e com falha na autenticação;

Credenciais com maior incidência de eventos de autenticação com sucesso e com falha na autenticação;

Endereços IPs com maior número de eventos de autenticação com sucesso e com falha na autenticação;

Cidades com maior número de eventos;

Países com maior número de eventos;

Gráfico com quantidade de eventos classificados por resposta da política de risco em razão do tempo;

Possuir integração com soluções do tipo “single-sign-on”, disponibilizando no mínimo, de forma nativa, o RH-SSO.

Possuir integração com Open-ssh;

Possuir integração nativa com a autenticação de tecnologias de mercado, sendo minimamente wordpress, openssh, cloudflare, moodle e keycloak.

Ser capaz de processar eventos originados em IPv4 e IPv6.

Possuir identificador único para todos os eventos processados pela solução.

Possuir mecanismo de processamento e armazenamento de eventos baseado em tecnologias escaláveis.

Disponibilizar console web responsiva para toda operação da solução.

Possuir mecanismo de dissuasão de ataques de força-bruta baseado em desafio criptográfico a ser decifrado pelo navegador cliente, sem necessidade de interação dos usuários da aplicação protegida.

O nível de dificuldade do desafio criptográfico deverá ser parametrizável.

REQUISITOS FUNCIONAIS PARA INSPEÇÃO E PROTEÇÃO DE CREDENCIAIS DE REDE:

A solução deverá aprender o comportamento padrão dos usuários e dos recursos monitorados baseando-se nos eventos de auditoria coletados para identificar e alertar desvios e anomalidades nesses comportamentos;

A solução deverá ser capaz de identificar tanto desvios quantitativos de comportamento como desvios qualitativos. Ou seja, deve ser capaz de identificar um aumento na quantidade de eventos gerados, assim como identificar acesso a dados que o usuário não costuma acessar;

A solução deverá permitir a configuração de alertas customizados para que um usuário, uma pasta, um período ou uma ação específica seja alertada caso ocorra ação que os envolva.

A solução deverá permitir a configuração de alertas em protocolos de integração com outras soluções como SNMP e Syslog.

A solução deverá permitir que os alertas sejam enviados por e-mail;

A solução deverá permitir que os alertas disparem a execução de respostas ou ações pré-configuradas ou através da execução de scripts.

A solução deverá contemplar a assinatura de uma base de conhecimentos do fornecedor de alertas pré-configurados de eventos suspeitos tais como: Ataques de sequestro de dados (ransomware); Detecção de ferramentas nocivas ao ambiente; Ações com acessos negados; Ações de escalações de privilégios; Excesso de tentativas de autenticação ou contas bloqueadas; Atividades suspeitas em dados parados e/ou inativos; Alterações anormais em GPO; Ataques de golden ticket; Ataques de injeção de códigos maliciosos; Ataques de decoberta de contas com NTLM e Kerkeros; Ataques de força bruta;

Os alertas deverão ser apresentados também em dashboard web que apresente: quantidade de alertas e suas severidades em determinado período, usuários mais alertados em determinado período, tipos de comportamentos suspeitos que mais ocorreram, máquinas que foram mais utilizadas para as ações suspeitas, classificação dos alertas dentro de um cenário de ataque cibernético;

O dashboard deverá apresentar todos os eventos que motivaram o alerta para que o time de segurança possa fazer investigação forense;

A solução deverá exibir no dashboard todos os eventos ocorridos que motivaram a ferramenta a gerar o alerta. A lista desses eventos deve ser customizável podendo ser filtradas, exibidas ou ocultadas colunas e agregada por valores das colunas exibidas.

O dashboard deverá possuir página com KPIs de compliance e segurança dos servidores e recursos monitorados e a partir desses KPIs, deve ser possível abrir a lista com informações detalhadas.

A solução deverá permitir integração com ferramentas de SIEM e outras soluções de gerenciamento de ativos.

Ser capaz de processar eventos de até 125 (cento e vinte e cinco) credenciais de rede (domínio).

REQUISITOS FUNCIONAIS DO PAINEL INTEGRADO DE EVENTOS INSPEÇÃO E SEGURANÇA DE CREDENCIAIS:

Possuir mecanismo nativo para gestão de usuários que podem acessar o painel de visualização, incluindo minimamente integração nativa com os seguintes sistemas de diretório de usuários: Active Directory e Keycloak/RH-SSO.

Criptografar com chave simétrica toda a comunicação com as fontes geradoras de eventos.

Ao armazenar eventos em base de dados, anonimizar minimamente o campo que contem a informação de nome de usuário, seja este um CPF, matrícula, e-mail ou uma string qualquer (ex: nome.sobrenome).

As informações disponibilizadas no painel de visualização deverão estar sempre orientadas a um intervalo de datas.

Fornecer estatísticas dos eventos de segurança originados nas aplicações web e de rede protegidas pela solução.

Fornecer minimamente as seguintes estatísticas:

Usuários que mais geram eventos de segurança no ambiente Microsoft e nas aplicações web;

Endereços IPs que mais geram eventos de segurança no ambiente de rede e nas aplicações web;

Incidentes de segurança mais frequentes;

Permitir visualizar detalhes de cada evento de segurança coletado.

Permitir filtrar eventos por usuário (credencial);

Permitir filtrar eventos por endereço IP de origem;

ITEM 2 - DOS SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO

Por implantação e configuração entende-se a instalação da quantidade de pacotes de licenças das soluções adquiridas, que compõem o objeto no ambiente computacional da SETIC/DF, bem como a ativação das respectivas licenças das ferramentas que compõem o referido objeto, pelo período de vigência e quantitativo requeridos no edital.

O serviço deverá ser executado mediante abertura de ordem de serviço, emitida em até 10 (dez) dias após a assinatura do contrato.

A CONTRATADA deverá apresentar Plano de Implantação e Configuração, detalhando requisitos, etapas, matriz de responsabilidade e prazos para execução das atividades.

O prazo para conclusão do processo de implantação e configuração da solução é de até 15 (quinze) dias úteis após a data de emissão da ordem de serviço.

Para fins de comprovação da execução do serviço de implantação e configuração, a contratada deverá elaborar e entregar relatório técnico com evidências do cumprimento do plano de implantação, bem como a comprovação da disponibilidade das licenças nos prazos e quantidades que serão especificados no edital e seus anexos.

ITEM 3 - DO SERVIÇO TÉCNICO DE OPERAÇÃO ASSISTIDA

O serviço técnico especializado de operação assistida será de execução mensal.

Para cada licença adquirida, será contratado 1 (um) serviço técnico especializado de operação assistida.

Poderá ser contratado um ou mais serviço técnico especializado de operação assistida, de acordo com a quantidade de pacotes de licenças adquiridas pelo contratante.

O serviço de operação assistida servirá para que a contratada, através de equipe própria e comprovadamente especializada na solução, execute serviços inerentes as rotinas técnicas operacionais dos softwares fornecidos.

O serviço de operação assistida deverá ser executado remotamente ou, quando solicitado, pontualmente presencial.

A execução dos serviços será mensal, pelo período de 36 (trinta e seis) meses indicado no quadro de itens do presente termo de referência, tendo seu início definido conforme cronograma do presente termo de referência;

As seguintes atividades técnicas operacionais compõem o serviço de operação assistida:

a. Troubleshooting;
b. Apoio na investigação de incidentes, quando solicitado pela CONTRATANTE;
c. Backup de configurações;
d. Análise, validação e aprovação de políticas, quando necessário;
e. Criação, alteração e configuração de novas políticas, de acordo com o solicitado pela CONTRATANTE;
f. Confecção de relatórios mensais com indicadores e atividades realizadas;

Para realização dos Serviços de Apoio e Suporte Técnico Especializados a CONTRATADA deverá disponibilizar profissionais certificados pelo fabricante da solução, cuja comprovação deverá ser apresentada no momento da assinatura do contrato;

O Serviço de operação assistida será mensurado como um serviço mensal e deverá ser atestado através de relatório técnico emitido pela CONTRATADA e encaminhado juntamente com a da Nota Fiscal Eletrônica de Serviços a partir do 1º (primeiro) dia do mês subsequente à prestação do serviço;

ITEM 4 - DOS REQUISITOS DE TREINAMENTO

A Contratada deverá prestar serviços de treinamento aos funcionários indicados pela SETIC/DF , com as características descritas a seguir:

Uma turma para até 10 (dez), participantes com carga horária mínima de 10 (dez) horas;

As datas de aplicação dos treinamentos deverão ser fixadas de comum acordo com o SETIC;

O conteúdo do treinamento deverá abranger:

Apresentação da arquitetura da solução;

Visão geral de funcionamento de cada solução;

Todo o material didático deverá ser repassado de forma impressa e em mídia para os alunos;

O treinamento deverá ocorrer no formato remoto ou, a critério da SETIC/DF, no formato presencial, ficando a mesma responsável por montar o ambiente adequado para realização do treinamento, isto é, todo o espaço necessário assim como toda infraestrutura computacional e de rede necessária;

Caberá à empresa contratada instalar a plataforma e demais softwares que compõem a solução ou possibilitar o acesso para o treinamento;

Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da empresa contratada, incluindo os gastos com instrutores, alimentação, estadia e o seu deslocamento;

Para fins de comprovação da execução dos Serviços de Treinamento, a contratada deverá entregar:

Lista de presença dos participantes do treinamento;

Certificado de execução do treinamento para cada participante ao término do treinamento.

DOS REQUISITOS DE SUPORTE TÉCNICO

Os serviços de suporte técnico aqui descritos serão prestados pelo período de 36 (trinta e seis) meses a partir da ativação das licenças.

A garantia dos produtos adquiridos, bem como o livre acesso a atualizações e patches, será de 36 (trinta e seis) meses, a partir da data do recebimento das licenças da solução.

A garantia contemplará atendimento técnico quanto à configuração inicial e solução de problemas (*bugs*) envolvendo o produto ofertado, bem como a atualização dos softwares.

O atendimento aos chamados de suporte técnico será prestado na modalidade remota.

Para solicitações de atendimento/abertura de chamados a CONTRATADA deverá dispor de portal web e linha telefônica local ou 0800.

Para os chamados de severidade 1 (um), o atendimento deverá ser em regime de disponibilidade 24x7x365.

Para os chamados de severidade 2 (dois), 3 (três) e 4 (quatro) o suporte deverá ser prestado das 8H as 18 h, de segunda-feira a sexta-feira, exceto feriados nacionais, conforme quadro a seguir:

Severidade	Descrição	Tempo para Início do Atendimento
Crítica	Chamados referentes a situações de emergência ou problema crítico,	No máximo 2 (duas) horas após a

	caracterizados pela existência de ambiente paralisado	abertura do chamado
Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	No máximo 4 (quatro) horas após a abertura do chamado
Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja necessidade de substituição de componentes	No máximo 12 (doze) horas após a abertura do chamado
Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto	No máximo 24 (vinte e quatro) horas após a abertura do chamado

Os chamados de suporte deverão ser classificados de acordo com a sua criticidade e terão prazos de atendimento e solução especificados conforme acordo de nível de serviço definido neste termo de referência;

Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento;

Mensalmente deverá ser entregue pela contratada um relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período com no mínimo as seguintes informações: número do contrato, período de referência, número de acionamento, localidade, severidade, descrição da ocorrência, nome do responsável pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, data e hora da solução e descrição da resolução adotada.

4.6 - DA MENSURAÇÃO DOS SERVIÇOS E PAGAMENTO

Os serviços da futura contratação serão mensurados e pagos através dos seguintes critérios:

1.	As licenças de uso do software serão mensuradas e pagas integralmente, em parcela única, por todo o período do contrato.
2.	Os serviços de Instalação e Configuração do software serão mensurados e pagos como atividade única, tendo sua verificação a partir da estabilização da Solução no ambiente da SETIC/DF e da disponibilização das licenças.
3.	O serviço técnico especializado de operação assistida será pago mensalmente, tendo sua verificação a partir do relatório de estabilidade e integridade da Solução no ambiente da SETIC/DF.
4.	O Treinamento será mensurado a partir de turmas, a serem demandadas por intermédio de agendamento a ser realizado de forma programada junto a empresa contratada, pagos integralmente após a realização dos serviços.

4.7 - DO CRONOGRAMA DE EXECUÇÃO

A execução do projeto se dará conforme o cronograma abaixo indicado:

Requisitos de Projeto e Implementação

A solução de TIC deverá ser plenamente implementada pela Contratada no ambiente da SETIC em no máximo 120 (cento e vinte) dias corridos, a partir da assinatura da Ordem de Fornecimento ou Ordem de Serviço.

Instalação e ativação das licenças a partir do primeiro mês de contrato, (Item 1) bem como o início do serviço de Implantação e Configuração e serviços técnicos especializados de operação assistida e (Itens 2 e 3). Respeitadas as indicações da seção Mensuração dos serviços.

Serviços de Treinamento (item 4) terão sua execução e início a partir do segundo mês de contrato, respeitadas as indicações da seção Mensuração dos serviços.

		MÊS												
ITEM	**DESCRIÇÃO**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**...36**
1	Pacote de licença de uso para solução baseada em software para inspeção e													

	segurança de credenciais em rede e aplicações WEB, pelo período de 365 (trinta e seis) meses.													
2	Serviço de Implantação e Configuração													
3	Serviço especializado de operação assistida													
4	Treinamento													

5 - ESTRATÉGIAS DE TRANSIÇÃO CONTRATUAL E INDEPENDÊNCIA TECNOLÓGICA

De modo preventivo e estratégico, nos meses que antecederem o final do período de vigência contratual, devem ser consideradas as tratativas necessárias para a continuidade do projeto, uma vez que se trata de contratação de alta complexidade ou mesmo verificar alternativas para suprir as necessidades da SETIC/DF.

Na transição contratual, deverão ser consideradas a entrega de versões finais dos produtos alvos da contratação (Transferência de conhecimentos):

1.	Uma vez que os processos e procedimentos são de propriedade da Secretaria de Estado da Segurança Pública (SETIC) a CONTRATANTE deverá prover todos os documentos, relatório, estudos gerados e eventuais bases de dados ao longo da execução contratual.
2.	A Contratada, no último mês da vigência do contrato, deverá fazer o repasse de conhecimento do serviço para a Contratante.

A Contratada deverá detalhar e repassar, conforme orientação e interesse da SETIC, toda a documentação utilizada bem como o conhecimento adquirido na implementação e prestação dos serviços, sem qualquer ônus adicional.

Deverá ainda, registrar em repositório específico, o conhecimento adquirido na resolução de incidentes, procedimentos operacionais e requisições para as situações em que ainda não há informação na Base de Conhecimento de como fazê-lo.

A Contratada deverá assinar um termo de confidencialidade em que reconhecerá que, em razão da prestação de serviços ao SETIC, tem acesso a informações que pertencem ao SETIC, que devem ser tratadas como sigilosas.

A contratada fica proibida de veicular ou comercializar produtos gerados, relativos ao objeto da prestação dos serviços, sem a prévia autorização do CONTRATANTE.

7 – DEMANDAS DOS POTENCIAIS GESTORES	
1.	Flexibilidade na gestão de políticas de acesso, permitindo personalização com base em funções, requisitos específicos da organização e mudanças nas necessidades de segurança.
2.	Recursos avançados de detecção de ameaças, incluindo análise de comportamento do usuário e inteligência contra ameaças, para identificar e responder proativamente a atividades maliciosas.
3.	Atualizações automáticas e manutenção simplificada para garantir que a proteção esteja sempre atualizada contra as últimas ameaças.
4.	A adaptação da solução para ambientes móveis, garantindo que a segurança de credenciais seja estendida a dispositivos móveis e aplicativos web.
5.	Continuidade dos negócios, incluindo planos de recuperação e capacidade de manter operações críticas mesmo em situações de emergência.
6.	Relatórios detalhados e capacidades de auditoria para facilitar a análise forense, bem como atender a requisitos de conformidade e relatórios gerenciais.
7.	Capacidade de monitorar as atividades de credenciamento em tempo real, com alertas proativos para atividades suspeitas ou violações de segurança.

8 – BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

8.1 – Bem/Serviço

Quantidade total de credenciais por aplicação web (cenário atual):

APLICAÇÃO WEB	CREDENCIAIS

SIGGO	2.193
SITAF	82.000
SISGEPAT	3.702
AGENCIANET	38.118
RECEITAWEB	2.530
SIGEST	2.439
NOTA LEGAL / PSV	1.533.617
SEI	257.297
TOTAL	**1.921.896**

Itens para solução:

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE ESTIMADA
1	Pacote de licença de uso para solução baseada em software para inspeção e segurança de credenciais em rede e aplicações WEB pelo período de 36 (trinta e seis) meses.	Licença de uso	4
2	Pacote de serviço de Implantação e Configuração	Serviço Unitário	4
3	Pacote de serviço técnico especializado de operação assistida.	Serviço Unitário	4
4	Treinamento	Serviço (Turma)	1

9 – DAS ALTERNATIVAS E LEVANTAMENTO DE MERCADO

Atendimento ao inciso III, art. 60 - DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023

O levantamento de mercado consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar, podendo, entre outras opções:

a) ser consideradas contratações similares feitas por outros órgãos e entidades públicas, bem como por organizações privadas, no contexto nacional ou internacional, com objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendam às necessidades da Administração.

b) ser realizada audiência e/ou consulta pública, preferencialmente na forma eletrônica, para coleta de contribuições.

Em relação a alínea “b” acima - Não aplicável ao caso concreto, haja vista que foi possível obter resultados a partir de processos análogos publicados pela administração pública.

c) em caso de possibilidade de compra, locação de bens ou do acesso a bens, ser avaliados os custos e os benefícios de cada opção para escolha da alternativa mais vantajosa, prospectando-se arranjos inovadores em sede de economia circular.

Em relação a alínea “c” acima - Não aplicável ao caso concreto, haja vista que foi possível obter resultados a partir de processos análogos publicados pela administração pública que permitiram concluir que o modelo de licenciamento de uso (licença de uso) é o mais aderente a realidade do projeto, haja vista contemplar os serviços de manutenção e suporte evolutivo da solução ao longo do período do contrato, bem como as mudanças tecnológicas que não viabilizam a contratação de uma licença permanente.

d) ser consideradas outras opções logísticas menos onerosas à Administração, tais como chamamentos públicos de doação e permutas.

Em relação a alínea “d” acima - Não aplicável ao caso concreto, haja vista que trata-se de uma solução de software (serviço)

CENÁRIOS / ANÁLISE DE SOLUÇÕES

Em relação as alternativas à presente contratação, podemos destacar as seguintes opções levantadas pela equipe técnica:

Cenário 1.	Utilização de plataformas e/ou softwares livres para atendimento da demanda indicada.
Cenário 2.	Contratação de fábrica de software para desenvolvimento de solução proprietária para atendimento à demanda indicada.
Cenário 3.	Contratação de empresa especializada em fornecimento de solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web, contemplando todos os serviços necessários.

Cenário 1: Utilização de plataformas e/ou softwares livres para atendimento da demanda indicada:

Quadro demonstrativo das desvantagens para Utilização de plataformas e/ou softwares livres - Cenário 1

Desvantagens Técnica		
1.	Suporte Técnico Limitado	Plataformas e softwares livres podem ter suporte técnico limitado em comparação com soluções comerciais. Isso pode resultar em desafios quando se trata de solucionar problemas complexos ou obter assistência especializada.
2.	Menos Recursos de Segurança Avançados	Algumas soluções de segurança comerciais podem oferecer recursos avançados de detecção de ameaças e prevenção que podem estar ausentes em plataformas de código aberto.
3.	Integração Complexa	A integração com outros sistemas e ferramentas pode ser mais complexa, pois as soluções de código aberto podem ter menos compatibilidade com padrões industriais ou APIs específicas
Desvantagens Segurança		
1.	Atualizações e Correções Limitadas	A disponibilidade de atualizações de segurança e correções pode não ser tão rápida ou abrangente como em soluções comerciais. Isso pode deixar a organização mais vulnerável a ameaças conhecidas.
2.	Menor Envolvimento da Comunidade	Nem todos os projetos de código aberto têm uma comunidade ativa de desenvolvedores e usuários. Dependendo do projeto, pode haver menos esforço de desenvolvimento e suporte.
3.	Riscos de Código Malicioso	Como o código é aberto, é possível que usuários mal-intencionados explorem vulnerabilidades ou incluam código malicioso. Isso exige uma revisão rigorosa do código e medidas de segurança adicionais.
Desvantagens Financeiras		
1.	Custos Ocultos de Implementação e Manutenção	Embora o software em si possa ser gratuito, os custos associados à implementação, treinamento, manutenção e suporte técnico podem se acumular, tornando-se significativos.
2.	Necessidade de Especialistas Internos	Plataformas de código aberto podem exigir especialistas internos para personalização, configuração e manutenção. Isso pode

		aumentar os custos de pessoal.
Desvantagens de Compatibilidade		
1.	Compatibilidade com Aplicações Específicas	Em alguns casos, pode haver desafios na compatibilidade com aplicações específicas ou requisitos exclusivos da organização, especialmente se essas aplicações forem construídas para trabalhar com soluções comerciais específicas
2.	Falta de Padronização	A falta de padronização em algumas soluções de código aberto pode levar a problemas de interoperabilidade, especialmente quando diferentes projetos adotam abordagens diferentes.
3.	Treinamento Específico Necessário	O treinamento da equipe pode ser mais específico e especializado quando se utiliza uma solução de código aberto, pois as interfaces e processos podem diferir significativamente das soluções comerciais mais comuns.
Desvantagens de Documentação		
1.	Documentação Incompleta ou Desatualizada	A documentação associada a algumas soluções de código aberto pode ser incompleta, desatualizada ou menos abrangente, o que pode dificultar o entendimento e a utilização eficaz da solução.
2.	Menos Ferramentas de Gestão	Algumas soluções de código aberto podem ter menos ferramentas de gerenciamento e monitoramento integradas, o que pode exigir o desenvolvimento ou a implementação de ferramentas adicionais.

Cenário 2: Contratação de fábrica de software para desenvolvimento de solução proprietária para atendimento à demanda indicada:

Quadro demonstrativo das desvantagens para Contratação de fábrica de software para desenvolvimento de solução - Cenário 2

Desvantagens Financeiras		
1.	Custos Iniciais Elevados	O custo inicial para a contratação de uma fábrica de software pode ser significativo, incluindo taxas de desenvolvimento, licenciamento de software e outros custos associados.

2.	Custos de Manutenção Contínua	Custos contínuos para manutenção, suporte e atualizações podem aumentar ao longo do tempo, especialmente se houver necessidade de modificações ou correções frequentes.
3.	Custo de Treinamento	Se a solução requerer treinamento extensivo para os usuários finais ou a equipe de TI, isso pode representar custos adicionais.
Desvantagens Técnicas		
1.	Personalização Limitada	Dependendo do modelo de contratação, a personalização da solução pode ser limitada, uma vez que a fábrica de software pode seguir padrões pré-definidos.
2.	Integração com Sistemas Existentes	Pode haver desafios na integração com sistemas existentes da organização, especialmente se a fábrica de software não estiver totalmente familiarizada com a infraestrutura específica.
3.	Manutenção e Atualizações	A dependência contínua da fábrica de software para atualizações e manutenção pode criar a necessidade de esperar por recursos ou correções, o que pode afetar a agilidade operacional.
Desvantagens de Tempo		
1.	Tempo de Desenvolvimento	Projetos personalizados podem levar mais tempo para serem desenvolvidos, especialmente se houver complexidade técnica ou requisitos específicos da organização.
2.	Dependência do Cronograma da Fábrica de Software	A entrega da solução pode depender do cronograma da fábrica de software, o que pode não estar totalmente alinhado com as necessidades de implementação da organização,
3.	Possíveis Atrasos	Atrasos imprevistos no desenvolvimento podem ocorrer, seja devido a problemas técnicos, mudanças de escopo ou outros fatores,

Cenário3: Contratação de empresa especializada em fornecimento de solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web, contemplando todos os serviços necessários.

Quadro demonstrativo das vantagens para Contratação de empresa especializada - Cenário 3.

Expertise Técnica	
1.	Empresas especializadas trazem conhecimento técnico especializado na área de segurança da informação e desenvolvimento de software. Elas geralmente contam com profissionais experientes e qualificados.
Solução Customizada	
2.	A empresa especializada pode desenvolver uma solução personalizada que atenda às necessidades específicas da organização, levando em consideração requisitos exclusivos e particularidades do ambiente.
Rápida Implementação	
3.	Com sua experiência, a empresa pode acelerar o processo de implementação, reduzindo o tempo necessário para colocar a solução em produção.
Suporte Contínuo	
4.	O suporte contínuo oferecido por empresas especializadas pode garantir que a solução esteja sempre atualizada, protegida contra ameaças emergentes e pronta para atender às evoluções do ambiente tecnológico.
Integração Eficiente	
5.	Uma empresa especializada pode garantir uma integração eficiente da solução com os sistemas existentes, minimizando problemas de compatibilidade e facilitando a coexistência com outras ferramentas de segurança.
Atualizações e Melhorias Constantes	
6.	A empresa pode fornecer atualizações regulares e melhorias contínuas na solução, garantindo que ela permaneça eficaz ao longo do tempo e adaptada às mudanças no cenário de ameaças.

Gestão de Projetos	
7.	Profissionais especializados em gestão de projetos podem coordenar o desenvolvimento e implementação da solução, assegurando que o projeto seja entregue dentro do prazo e do orçamento planejados.
Conformidade com Padrões	
8.	Empresas especializadas estão cientes das regulamentações e padrões de segurança, o que facilita a conformidade com requisitos específicos da indústria e leis de privacidade.
Treinamento e Educação	
9.	Oferecimento de treinamento e educação para a equipe da organização, garantindo que os usuários finais e a equipe de TI estejam devidamente capacitados para utilizar e manter a solução.
Foco no Core Business	
10.	Permite que a organização se concentre em suas atividades principais, enquanto a empresa especializada cuida do desenvolvimento e manutenção da solução de segurança.
Acesso a Recursos Especializados	
11.	A contratação proporciona acesso a uma variedade de especialistas, como arquitetos de segurança, analistas de ameaças e desenvolvedores especializados.
Gestão de Riscos	
12.	As empresas especializadas geralmente têm experiência em avaliação de riscos de segurança, ajudando a identificar e mitigar potenciais vulnerabilidades.
Melhoria Contínua da Segurança	
13.	A empresa pode incorporar práticas de segurança avançadas e utilizar as últimas tecnologias para melhorar continuamente a postura de segurança da organização.
Contrato com SLAs Definidos	

14.	Contratos de serviço podem incluir Acordos de Nível de Serviço (SLAs) claros, estabelecendo expectativas para o desempenho da solução e os tempos de resposta.
Redução de Custos a Longo Prazo	
15.	Embora a contratação inicial possa ter custos, a eficiência operacional, atualizações contínuas e menor risco de problemas técnicos podem levar a uma redução de custos a longo prazo.

Análise dos cenários

1. **Cenário 1: Plataformas e/ ou softwares livres para atendimento da demanda indicada**
2. **Cenário 2: Contratação de fábrica de softwares**
3. **Cenário 3: Contratação de empresa especializada em fornecimento de solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web, comtemplando todos os serviços necessários.**

A possibilidade de aquisição na forma de bens ou contratação como serviço; será detalhada a seguir (item 9).

Para o cenário 1, Plataformas e/ ou softwares livres para atendimento da demanda indicada

Para contratação de Plataformas e/ ou softwares livres é importante avaliar todo ambiente, inclusive se o softwares irá atender todos as necessidades para solução proposta. A escolha de software livre poderá trazer riscos associados a fatores como a descontinuidade dessas aplicações, dificuldades de integração ausência de adequação a realidade da SETIC/DF.

Além disso, as plataformas e os softwares livres não possuem suporte técnico e atualmente a equipe da SETIC, não há profissional capacitado para sustentar soluções de software livre para esse projeto.

Assim, devido as necessidades informadas na solução do projeto, avalia-se inviável a aquisição de softwares livres para o objetivo apresentado.

Este cenário não se aplica.

Para o cenário 2, Contratação de Fábrica de Software

Embora a contratação de uma Fábrica de Software traga inúmeros benefícios como desenvolvimento de diversos softwares e ferramentas que poderiam adequar e atender a solução, é necessário observar a urgência que o caso requer. O desenvolvimento de soluções pela Fábrica de Software pode levar muito tempo para que todas as fases sejam concluídas , situação que pode deixar a base de dados do GDF vulnerável por muito tempo.

Além disso, a Fábrica de Software teria que adequar uma equipe especialista em desenvolvimento de software de Cibersegurança.

Dessa forma, pode-se avaliar que a solução não é adequada, pois existem ferramentas prontas no mercado que pode atender de forma imediata a solução do projeto.

Este cenário não se aplica.

Para o cenário 3, Contratação de empresa especializada em fornecimento de solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web, comtemplando todos os serviços necessários.

O terceiro cenário é a contratação de uma empresa que forneça a solução de um software baseado em inspeção e segurança de credenciais em rede e aplicações web. Essa solução deverá trazer diversas funcionalidades específicas que o Software livre a a Fábrica de Software não atende.

A escolha do cenário 3 permitirá a implementação da solução por uma empresa de mercado, especializada neste segmento de Cibersegurança e proteção de dados, que forneça soluções ajustadas a realidade dos eventos recentes e que possa entregar as atualizações e suporte durante todo o período contratado.

A contratação de uma Empresa especialista nessa solução acrescentará ainda que a forma de entrega do produto será de forma imediata, situação que irá trazer a mitigação de forma imediata dos riscos.

Em resumo, grande parte da infraestrutura seria atendida por licença de software capaz de inspeção e segurança de credenciais em rede e aplicações web contemplando serviços de suporte especializado, treinamento, manutenção preventiva e corretiva com atualização e upgrades de versões, pelo período de 36 meses.

.

9.1 – LEVANTAMENTO DA ALTERNATIVA (CENÁRIO POSSÍVEL).	
Cenário 3	
Entidade	**Contratação de empresa especializada em fornecimento de solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web.**
Descrição	Implantação de Solução tecnológica para inspeção e segurança de credenciais em rede e aplicações web contemplando serviços de suporte especializado, operação assistida, treinamento, manutenção preventiva e corretiva com atualização e upgrades de versões,

	pelo período de 36 meses.
Fornecedor	Layer do Brasil, Eireli, Infosec, Neotel e etc.
Analise da Solução	A avaliação técnica da solução proposta para SETIC revela uma abordagem abrangente e tecnicamente sólida para a gestão de segurança de credenciais em ambientes de rede e aplicações web. Abaixo estão os principais pontos de análise técnica: 1. Arquitetura de Segurança: • A solução apresenta uma arquitetura robusta, com camadas de segurança que abrangem a inspeção contínua de tráfego, identificação de padrões suspeitos e proteção contra ameaças comuns. Isso contribui para a prevenção eficaz de violações de segurança. 2. Detecção Avançada de Ameaças: • A capacidade de detecção de ameaças é aprimorada por meio de tecnologias avançadas, como análise comportamental, detecção de anomalias e aprendizado de máquina. Isso permite uma resposta proativa a ameaças emergentes. 3. Inteligência contra Ameaças: • A solução integra feeds de inteligência contra ameaças, mantendo-se atualizada sobre as últimas tendências de cibersegurança. Isso melhora a capacidade de identificar e neutralizar ameaças sofisticadas. 4. Suporte a Protocolos e Padrões: • A solução é projetada para suportar uma variedade de protocolos de rede e aderir a padrões de segurança reconhecidos. Isso garante interoperabilidade e compatibilidade com a infraestrutura existente. 5. Operação Assistida e Treinamento: • A oferta de operação assistida e treinamento contínuo demonstra uma preocupação em capacitar a equipe de operações. O treinamento abrange não apenas o uso da solução, mas também as práticas recomendadas de segurança. 6. Políticas de Segurança Configuráveis: • A solução permite a configuração flexível de políticas de segurança para atender às necessidades específicas da organização. Isso é crucial para adaptar as configurações de segurança de acordo com as mudanças no ambiente de ameaças. 7. Gestão Centralizada:

- A capacidade de gerenciamento centralizado facilita a administração eficiente da solução em ambientes complexos de rede. Isso simplifica as operações e reduz a carga administrativa.

8. Atualizações e Upgrades Gerenciados:

- O ciclo de vida da solução é gerenciado de forma proativa, com atualizações e upgrades planejados. Isso garante que a solução esteja sempre atualizada, com correções de segurança e novos recursos disponíveis conforme necessário.

9. Monitoramento em Tempo Real:

- A solução oferece capacidades de monitoramento em tempo real, permitindo a identificação imediata de atividades suspeitas ou anomalias. Isso contribui para a resposta rápida a incidentes.

10. Integração com Infraestrutura Existente:

- A solução é projetada para integrar-se de maneira eficiente à infraestrutura existente, minimizando interrupções operacionais durante a implementação. Isso suaviza a transição para a nova solução.

11. Protocolos de Criptografia:

- O suporte a protocolos de criptografia robustos é essencial para garantir a confidencialidade dos dados. A solução adota práticas avançadas de criptografia para proteger as comunicações.

12. Manutenção Preventiva e Corretiva Eficaz:

- A combinação de manutenção preventiva e corretiva assegura a estabilidade operacional. A manutenção proativa minimiza a ocorrência de problemas, enquanto a correção rápida aborda eventuais falhas.

13. Escalabilidade:

- A solução é escalável para acompanhar o crescimento da organização. Isso é fundamental para garantir que a infraestrutura de segurança possa lidar com um aumento no volume de tráfego e dispositivos.

14. Relatório e Auditoria:

- A solução oferece recursos abrangentes de geração de relatórios e auditoria para fornecer visibilidade sobre atividades de segurança, eventos críticos e conformidade com políticas internas.

15. Compatibilidade com Políticas de Segurança Internas e Regulamentações:

	• A solução é configurável para aderir às políticas internas de segurança e regulamentações específicas do setor. Isso é essencial para garantir conformidade com requisitos normativos. Em síntese, a análise técnica evidencia que a solução proposta para SETIC é altamente robusta, incorporando práticas avançadas de segurança, capacidades de detecção sofisticadas e uma abordagem proativa para operações, manutenção e treinamento. Essa solução representa uma escolha técnica sólida para fortalecer a postura de segurança de credenciais em rede e aplicações web da organização.

9.2 – ANÁLISE DE MERCADO – CENÁRIO 3.

A análise dos cenários indica que contratar uma empresa especializada para fornecer uma solução de software para inspeção e segurança de credenciais em redes e aplicações web é a opção mais adequada às necessidades do projeto. Para fundamentar o investimento, investigamos contratações públicas de soluções similares, mas o avanço contínuo dos crimes cibernéticos implica na adição constante de novos recursos e soluções, complicando a obtenção de um valor projetado preciso devido à falta de aderência aos requisitos técnicos necessários.

Considerando que o projeto em questão demanda apenas uma dentre várias soluções de segurança já contratadas, e dado o modelo distinto do projeto citado anteriormente, não podemos nos basear em pregões, pois os valores serão significativamente diferentes. Este fato reforça a complexidade de projetar o investimento baseando-se em processos incompatíveis, o que poderia distorcer a análise financeira do projeto, já que outras contratações, mesmo no campo da segurança da informação, podem não atender completamente às necessidades específicas desta.

Portanto, a pesquisa priorizou definir o modelo de licenciamento mais adequado, optando por licenças de uso após análise de editais similares. A busca em sites especializados, como Banco de Preços e Comprasnet, não resultou na identificação de soluções plenamente compatíveis. Entretanto, identificamos propostas com similaridade funcional, como o Pregão Eletrônico nº 00024/2020 da Agência Nacional de Águas (ANA) – UASG: 443001 item 5, conforme documento SEI n.º 134966600, que, ao avaliar a relação custo-benefício, mostrou-se inviável (utilizar o referido Pregão como Similaridade Funcional). Seguindo essa constatação, conduzimos uma pesquisa de preços com fornecedor, conforme documentado no SEI nº 134967801

Custo Total de Propriedade – Cotação de mercado para o cenário 3.

Atendimento ao inciso VI, art. 60 - DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023

MÉDIA ANÁLISE DE MERCADO – CENÁRIO 3

				Aquisição	
Item	**Descrição**	Métrica	Quantidade	**Valor Unitário**	**Valor total para 36 meses**

1	Pacote de licença de uso para solução baseada em software para inspeção e segurança de credenciais em rede e aplicações WEB pelo período de 36 (trinta e seis) meses.	Licença de uso	4	R$ 2.183.000,00	R$ 8.732.000,00
2	Pacote de serviço de Implantação e Configuração	Serviço Unitário	4	R$ 87.200,00	R$ 348.800,00
3	Pacote de serviço técnico especializado de operação assistida.	Serviço Unitário	4	R$ 120.000,00	R$ 480.000,00
4	Treinamento	Serviço (Turma)	1	R$ 92.500,00	R$ 370.000,00
TOTAL					R$ 9.930.800,00

Os valores previstos para a contratação são estimativas preliminares; no entanto, embora tenhamos obtido a cifra mencionada para um período de 36 meses, é essencial conduzir uma pesquisa de mercado mais abrangente após a elaboração do termo de referência. Isso se torna indispensável para a obtenção de uma estimativa de preços mais precisa e alinhada às condições do mercado.

Pesquisa realizada conforme documento SEI n.º 134967801.

10.2 – COMPARATIVO DE CUSTO TOTAL DE PROPRIEDADE (TCO).

Artigo 11, Inciso III, Alínea a - IN SGD/ME n.º 94 de 23 de dezembro de 2022

Não é viável realizar uma comparação de custos totais, uma vez que existe apenas um cenário possível.

Cenário 3 apresenta uma solução viável com o valor encontrado de R$

11 – JUSTIFICATIVA DO CENÁRIO ESCOLHIDO.

Art. 18 da Lei. 14.133, § 1º Inciso V

A decisão de adquirir uma solução baseada em software para inspeção e segurança de credenciais em rede e aplicações web, juntamente com um pacote completo de serviços por um período estendido de 36 meses (Cenário 3), é respaldada por uma análise detalhada de diversas vantagens estratégicas que esta escolha proporcionará à nossa organização.

Abaixo estão os aspectos detalhados que sustentam essa decisão:

- Vivemos em um ambiente digital dinâmico, com ameaças cibernéticas em constante evolução. A aquisição de uma solução de segurança por um período estendido é essencial para garantir uma defesa robusta e atualizada contra as ameaças emergentes.
- A inclusão de serviços de suporte especializado por 36 meses assegura à nossa equipe acesso imediato a especialistas altamente qualificados. Isso é crucial para lidar com incidentes, resolver problemas complexos e garantir a eficácia contínua da solução.
- O treinamento continuado é uma pedra angular para maximizar o retorno sobre o investimento. Ao longo do contrato, a equipe receberá treinamentos regulares, garantindo uma compreensão aprofundada da solução e a capacidade de explorar plenamente seus recursos.
- A manutenção preventiva proativa visa identificar e mitigar potenciais vulnerabilidades antes que se tornem problemas críticos. A manutenção corretiva rápida é essencial para minimizar os impactos de incidentes de segurança.
- Ao optar por um contrato de 36 meses, garantimos estabilidade financeira, com custos previsíveis e geralmente reduzidos em comparação com contratos de curto prazo. Isso representa um investimento sólido em nossa postura de segurança.
- As atualizações e upgrades de versões ao longo do contrato são planejados e implementados estrategicamente. Isso assegura que a solução esteja sempre alinhada com as mais recentes tecnologias e requisitos de segurança, evitando interrupções desnecessárias.
- Vivemos em um cenário tecnológico que se transforma rapidamente. Uma solução apoiada por um contrato de longo prazo permite adaptações graduais e controladas, garantindo que permaneçamos à frente das exigências do ambiente digital.
- O suporte especializado não apenas resolve problemas técnicos, mas também desempenha um papel vital na gestão de crises. Respostas rápidas e eficazes em situações críticas minimizam danos e garantem a continuidade operacional.
- Externalizar suporte e manutenção permite que nossa equipe interna se concentre em iniciativas e projetos estratégicos, alinhando-se diretamente com os objetivos da organização.
- O contrato de 36 meses inclui um compromisso de incorporar as últimas tendências e inovações na solução, garantindo que nossa organização esteja sempre à frente no que diz respeito à segurança digital.
- Avaliações regulares ao longo do contrato permitem um monitoramento contínuo do desempenho da solução, identificando áreas de melhoria e garantindo que ela atenda efetivamente às nossas necessidades operacionais.
- Um contrato de 36 meses constrói um relacionamento de parceria duradouro com o fornecedor. Isso cria uma colaboração mais estreita, alinhada aos objetivos organizacionais e permitindo uma adaptação contínua às mudanças nas circunstâncias.
- A conformidade com regulamentações é vital. O suporte especializado assegura que a solução permaneça em conformidade com requisitos legais e padrões de segurança durante toda a duração do contrato.
- A decisão de um contrato de 36 meses reflete nosso compromisso com a segurança como uma prioridade estratégica, demonstrando a seriedade com que abordamos a proteção de dados e ativos digitais.

Em conclusão, a aquisição de uma solução de inspeção e segurança de credenciais com serviços abrangentes por 36 meses é uma escolha fundamentada em benefícios significativos que abrangem desde a segurança robusta até a eficiência operacional, adaptabilidade às mudanças e construção

de um relacionamento duradouro com o fornecedor. Esta decisão representa um investimento consciente em nossa postura de segurança e no sucesso a longo prazo da organização.

12 - BENEFÍCIOS A SEREM ALCANÇADOS - Art. 18 da Lei. 14.133, § 1º, IX Atendimento ao inciso X, Art. 60 -DECRETO Nº 44.330, DE 16 DE MARÇO DE 2023 Artigo 11, Inciso V - IN SGD/ME n.º 94 de 23 de dezembro de 2022	
1.	Reforça a segurança da rede e das aplicações web, garantindo que apenas usuários autorizados tenham acesso, protegendo contra acessos não autorizados e potenciais violações de segurança
2.	Ajuda a prevenir ataques de credenciais, incluindo tentativas de login por força bruta, ataques de phishing e outras ameaças que visam comprometer as informações de login dos usuários.
3.	Facilita auditorias detalhadas e relatórios de conformidade, permitindo que as organizações atendam a requisitos regulatórios e demonstrem conformidade com padrões de segurança.
4.	Identifica comportamentos anômalos e atividades suspeitas nas credenciais, possibilitando uma detecção precoce de potenciais ameaças e ação imediata para mitigação.
5.	Oferece monitoramento contínuo e em tempo real das atividades de credenciamento, proporcionando uma visão abrangente das interações dos usuários com a rede e as aplicações.
6.	Integração de autenticação multifatorial, aumentando a segurança ao exigir múltiplos métodos de verificação de identidade além de apenas senhas.
7.	Simplifica a administração e a gestão de credenciais por meio de uma plataforma centralizada, reduzindo a carga operacional e garantindo consistência nas políticas de segurança.
8.	Facilita a resposta rápida a incidentes, permitindo bloqueio imediato em caso de atividades suspeitas ou comprometimento de credenciais.
9.	Contribui para a proteção contra ameaças internas, monitorando as atividades dos usuários e identificando comportamentos anômalos que possam indicar uma possível ameaça interna.

10.	Integra-se facilmente com outras soluções de segurança, como firewalls, antivírus e sistemas de prevenção contra intrusões, proporcionando uma abordagem holística para a segurança da rede.
11.	Implementa práticas seguras de autenticação, mantendo a segurança sem comprometer a experiência do usuário, o que é crucial para a adoção efetiva da solução.
12.	Oferece atualizações regulares para proteção contra as últimas ameaças e vulnerabilidades, mantendo a solução eficaz em um ambiente em constante evolução.

13 – NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE INTERNO PARA EXECUÇÃO CONTRATUAL

Artigo 11, Inciso II, Alínea e - IN SGD/ME n.º 94 de 23 de dezembro de 2022

1. Providências a serem Adotadas:

- A administração não necessitará de adequações em sua estrutura para que a contratação possa ser efetivada.

2. Possíveis Impactos Ambientais:

- Na presente contratação não se vislumbra impacto ambiental relevante.

14 – DECLARAÇÃO DE VIABILIDADE.

Artigo 11, Inciso V - IN SGD/ME n.º 94 de 23 de dezembro de 2022

1. A solução objeto do presente Estudo Técnico Preliminar é tecnicamente viável, além de estar alinhado ao Planejamento Estratégico Institucional da SEPLAD (PEI/SEPLAD 2023-2026) e ao Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC - 2023-2026).

2. A equipe técnica desta contratação foi formada por servidores da SETIC.

3. Esta equipe de planejamento declara viável esta contratação.

4. A viabilidade da contratação é constatada diante da análise do presente Estudo Técnico Preliminar, o qual demonstrou que não existem óbices estruturais, logísticos e normativos legais internos e externos que inviabilizem a contratação.

5. Salienta-se, por fim, que o presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD/ME n.° 94, de 23/12/2022, recepcionada no âmbito do Governo do Distrito Federal - GDF pelo Decreto Distrital nº 45.011, de 27/09/2023, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da contratação. Além disso, atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área requisitante priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que recomenda-se a contratação proposta.

15 – ASSINATURAS

Artigo 11, § 2º - IN SGD/ME n.º 94 de 23 de dezembro de 2022

Integrante Técnico

Nome: Tomé Luiz da Silva Couto	Matrícula: 283.684-X

O presente estudo foi elaborado em harmonia com a Instrução Normativa SGD/ME n.º 94, de 23/12/2022, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da aquisição, pelo que **APROVO** o presente Estudo Técnico Preliminar

_____

TOMÉ LUIZ DA SILVA COUTO

Integrante Técnico

Integrante Requisitante

Nome: Samuel Pereira de Souza Gomes	Matrícula: 282.926-6

O presente planejamento foi elaborado em harmonia com a Instrução Normativa SGD/ME n.º 94, de 23/12/2022, bem como atende adequadamente às demandas de negócio formuladas. Os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, sendo

priorizado o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que **APROVO** o presente Estudo Técnico Preliminar.

_____

SAMUEL PEREIRA DE SOUZA GOMES

Integrante Requisitante

Autoridade Máxima de TIC	
Nome: Wisney Rafael Alves de Oliveira	Matrícula: 279.261-3
O presente planejamento está de acordo com as necessidades técnicas, operacionais e estratégicas do órgão. Atende adequadamente às demandas de negócio formuladas, os benefícios pretendidos são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis e a área responsável priorizará o fornecimento de todos os elementos aqui relacionados necessários à consecução dos benefícios pretendidos, pelo que **APROVO** o presente Estudo Técnico Preliminar.	

_____

WISNEY RAFAEL ALVES DE OLIVEIRA

Secretário Executivo de Tecnologia da Informação e Comunicação.

Documento assinado eletronicamente por **SAMUEL PEREIRA DE SOUZA GOMES - Matr.0282926-6**, **Chefe da Unidade de Segurança, Centro de Dados e Mensageria**, em 11/07/2024, às 18:03, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **TOMÉ LUIZ DA SILVA COUTO - Matr.0283684-X**, **Diretor(a) de Mensageria**, em 11/07/2024, às 18:19, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

Documento assinado eletronicamente por **WISNEY RAFAEL ALVES OLIVEIRA - Matr.0279261-3**, **Secretário(a) Executivo(a) de Tecnologia da Informação e Comunicação**, em 12/07/2024, às 10:55, conforme art. 6º do Decreto n° 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.

A autenticidade do documento pode ser conferida no site: http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 verificador= **143710812** código CRC= **E5AFF596**.