Estudo Técnico Preliminar 12/2023

1. Informações Básicas

[Este documento é sigiloso | Justificativa: Órgão de Segurança da União.]

Número do processo: 00091.000066/2023-22

2. Descrição da necessidade

Problema

A Abin foi criada para dar resposta efetiva à necessidade, essencial ao Estado Democrático de Direito, de municiar o Governo com informações estratégicas, produzidas em tempo hábil e em absoluta sintonia com a Constituição e as leis do País, assegurando-lhe o conhecimento antecipado de fatos e fatores relacionados com o desenvolvimento e a segurança do Estado, em todas as áreas da vida nacional. Assim, ela deverá assessorar o Chefe de Estado no desempenho de suas funções, sobretudo em caráter preventivo, avaliando ameaças internas e externas à ordem constitucional e aperfeiçoando seu pessoal para o exercício de suas atribuições.

Para desempenhar suas atribuições institucionais é necessário que o apoio tecnológico às atividades da Abin disponha de uma infraestrutura tecnológica que tenha capacidade de suportar os diversos sistemas e atividades, finalísticas e administrativas, necessárias ao bom desempenho de suas competências legais, bem como de uma estrutura de comunicação eficiente e segura, no que diz respeito à voz e dados, de modo a permitir a manutenção do sigilo a que está, obrigatoriamente, submetida à atividade de Inteligência.

Com o setor público operando em um ambiente cada vez mais orientado por dados, a probabilidade de ações criminosas se tornarem mais frequentes são grandes e, à medida em que se tornam mais digitais, suas superfícies de ataque aumentam significativamente e, consequentemente, tornam-se muito mais vulneráveis a todos os tipos de ameaças cibernéticas. Órgãos governamentais têm sido alvos frequentes de ataques maliciosos nas redes e servidores de arquivos, foram mais de vinte mil notificações registradas por órgãos públicos em 2020, segundo monitoramento do Gabinete de Segurança Institucional (GSI) da Presidência da República. Dentre os órgãos afetados estão o Tribunal Regional Federal da 1º Região, Tribunal Superior Eleitoral e um ataque mais grave contra o Superior Tribunal de Justiça, quando os criminosos criptografaram arquivos e pediram pagamento em criptomoedas para devolvê-los.

O objetivo principal de ciberataques – tanto de dentro quanto de fora da organização – é explorar os acessos privilegiados e obter indevidamente dados sensíveis. Esses dados normalmente estão armazenados em aplicações e dispositivos de TI, e são os alvos preferidos de agentes maliciosos para obter acesso não autorizado a dados. Credenciais de alto privilégio, contas de sistema padrão ou credenciais embutidas em scripts e aplicações são os principais vetores de ataque utilizados para ganhar acesso ao ambiente de T.I. Através de um ataque phishing, por exemplo, um hacker consegue penetrar em um dispositivo, e assim se alastrar pela rede através de credenciais privilegiadas, infectando o ambiente e obtendo acesso indevido a informações privilegiadas. Desta maneira, todos os acessos realizados no ambiente devem ser gerenciados, e um usuário não autorizado nunca deve ter acesso a dados ou sistemas. Muito pelo contrário, em um cenário de aumento de vazamento de dados, os usuários administradores precisam de controle de acesso ainda mais rígidos.

Nesse contexto, é necessário manter o ambiente computacional da ABIN seguro, não apenas de ameaças externas, mas também internamente, no que tange a acessos mal-intencionados ou não, bem como as informações críticas, muitas vezes classificadas com algum grau de sigilo. A proteção dos ativos de informação requer o monitoramento e atuação em diversas áreas de Tecnologia da Informação e Comunicação (TIC). Ameaças externas são detectadas e combatidas com ferramentas que analisam tráfego na rede e pacotes de dados trocados entre aplicações. A segurança no perímetro interno da rede, por outro lado, pode ser ampliada com o emprego de soluções em software que analisam o comportamento de aplicações e ações executadas por usuários. Neste caso, as ações do próprio público interno da organização passam a ser de interesse para o monitoramento.

Os servidores com "superusuários" precisam de acesso privilegiado a tudo dentro do sistema a fim de solucionar problemas, resolver questões e manter um nível de acesso imediato aos usuários comuns que, cada vez mais, precisam de acesso fácil, rápido, a qualquer hora e em qualquer lugar, para que possam realizar seus trabalhos. Ataques, como o supracitado sofrido pelo STJ, geralmente acontecem quando pessoa mal intencionada obtém senha de acesso dos usuários com acessos privilegiados. Os invasores parecem usuários internos, mas na verdade não são. Com o nível de acesso que os usuários privilegiados possuem,

mesmo ações acidentais ou não intencionais podem criar riscos significativos para a Agência e um ataque utilizando o acesso privilegiado de um "superusuário" poderia acarretar consideráveis danos ao Estado Brasileiro.

Nesse sentido, o objeto da contratação está, desse modo relacionado com o processo Sei nº 00091.008067/2020-72 - Projeto Ampliação da Capacidade de Comunicação Segura. E com a mudança repentina da modalidade de serviço para o trabalho remoto, há algumas vulnerabilidades que precisam ser tratadas para que o ambiente possa ser expandido e utilizado por mais servidores. Atualmente, a Agência possui licença perpétua do software Varonis DatAdvantage vencidas desde julho de 2019. Além do mais, não há auditoria e controle referente aos acessos ou tentativas de acessos a arquivos nos dispositivos entregues aos usuários. Isso significa que ações executadas nesses dispositivos não serão conhecidas pelo CEPESC, tais como:

- Tentativas de instalação de aplicações não autorizadas, mediante ataques para obtenção da senha de administrador do equipamento;
- Transferência de documentos internos para esses dispositivos e, posteriormente, realização de cópia em mídias externas como USB; e
- Os usuários que têm acesso ao ambiente interno de forma remota se conectam diretamente aos seus desktops da rede interna. Além disso, o usuário tem acesso completo ao desktop, sem restrição de aplicações e bases de dados, por exemplo. Esse acesso poderia ser restrito, para que apenas algumas aplicações ou um conjunto de dados pudessem ser acessados remotamente. Atualmente, não há como restringir tal acesso.
- Não há registro da sessão aberta pelo usuário. A partir do momento em que o usuário fecha a VPN, apenas algumas ações realizadas por ele são mantidas em logs, ou seja, a maior parte do trabalho não fica registrada, o que dificulta o rastreamento de condutas suspeitas e/ou maliciosas;

Por último, não há um tipo de controle mais rigoroso com relação aos "superusuários".

Proposta de solução

Considerando as necessidades elencadas, bem como as vulnerabilidades detectadas, é necessário que ajustes sejam implementados na arquitetura existente a fim de adequá-la ao nível de segurança com que a ABIN trata seus ativos de informação. Dessa forma, a solução deve:

- Ampliar o ambiente de comunicação segura para atender os servidores da ABIN que ainda não fazem uso de soluções de acesso remoto;
- Possibilitar que os dispositivos entregues aos usuários sejam auditados e controlados pelo CEPESC;
- Permitir o registro e acompanhamento das ações executadas pelos servidores, para que desvios de conduta sejam apurados;
- Restringir o acesso remoto do usuário a aplicações e conjuntos de dados específicos, além de seu próprio desktop, se for o caso;
- Auditar os acessos de servidores com senhas de acessos privilegiados.

3. Área requisitante

Área Requisitante	Responsável
SEGOR	Daniel Baramili Fleury de Amorim

4. Necessidades de Negócio

As atividades de auditar, controlar, gerenciar e monitorar as ações dos usuários, dos serviços de administração de diretório de usuários, servidor de arquivos e outros, bem como prevenir ações e comportamentos suspeitos em tempo real, proteger os dados sensíveis e gerir todas as permissões dos usuários de forma segura, exigem soluções especializadas e eficientes que possibilitem automatizar essas tarefas, sendo de fundamental importância para o negócio a renovação e expansão da solução de auditoria Varonis;

A solução de gerenciamento de identidade privilegiada deve prover recursos de cofre para armazenamento e troca aleatória das senhas de contas administrativas, isolamento, monitoramento, gravação e auditoria de sessões privilegiadas e análise comportamental, inclusive considerando o ambiente de nuvem privada;

A solução deve suportar proteção de servidores e estações UNIX/Windows/Mac realizando o gerenciamento local de privilégios através de agentes;

A solução deve possuir um sistema confiável para gerenciar as autenticações dos acessos privilegiados através de um método robusto e seguro próprio ou integrando com soluções de autenticação externa (LDAP, Microsoft AD) para facilitar a rastreabilidade dos acessos à solução;

A solução deve ser capaz de controlar, filtrar e criar regras de permissões com base nos riscos para as operações que um administrador pode executar;

A solução deve ser capaz de gerenciar chaves SSH UNIX/Linux: As chaves SSH não gerenciadas oferecem acesso a servidores de produção críticos Unix e Linux que podem prejudicar o negócio. A falta de rotação adequada das chaves também pode aumentar a superfície de ataque cibernético;

A solução deve assegurar IDs compartilhados de usuários corporativos: Os IDs compartilhados costumam ser usados para acessar sistemas com dados financeiros e de RH confidenciais, sem gerenciamento de sessões ou autenticações.

5. Necessidades Tecnológicas

A solução de auditoria deverá ser de um único fabricante e seus módulos e/ou softwares deverão ser totalmente integrados e disponibilizados em uma única interface gráfica para preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes, a facilidade de uso e operação e a integridade dos dados utilizados nas auditorias e investigações:

1. A solução deve suportar a utilização de servidores virtualizados para todos os seus componentes;
2. A solução deverá permitir a modelagem de permissionamento de maneira gráfica antes da aplicação em produção. Esta modelagem deve demonstrar os impactos das mudanças pretendidas nos grupos e usuários em relação a suas permissões nos diretórios monitorados, ou seja, deve ser possível analisar quais acessos os usuários ganharão ou perderão antes que essas alterações sejam efetuadas em produção;
3. A solução deverá oferecer a opção de aplicação completa ou parcial das alterações pretendidas nos grupos, usuários e permissões assim como oferecer a opção de efetivação imediata ou agendada no Active Directory e servidores monitorados;
4. Os logs apresentados pela solução ofertada deverão conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário que fez a ação;
5. Os relatórios devem ser fornecidos para serem exportados em diversos formatos de arquivos, além da possibilidade do agendamento dos mesmos;
6. A solução deverá realizar a análise comportamental dos usuários, grupos e permissões aos dados não estruturados dos servidores monitorados;
7. A solução deverá identificar, de forma automática, usuários com acesso indevido a pastas, sugerindo a revogação do acesso;
8. Suportar a auditoria dos seguintes eventos do Directory Service:

- a) Criação de objetos;
- b) Deleção de objetos;
- c) Membros adicionados a grupos de segurança;
- d) Membros removidos de grupos de segurança;
- e) Propriedades do objeto do AD alteradas;
- f) Autenticação de conta;
- g) Reset de senha;
- h) Bloqueio de conta;
- i) Desbloqueio de conta;
- j) Habilitação de conta;
- k) Desabilitação de conta;
- l) Permissão adicionada a objeto do AD;
- m) Permissão removida de objeto do AD;

- n) Proprietário alterado;
- o) Modificação de configuração de GPO;
- p) Criação de link de GPO;
- q) Deleção de link de GPO.

9. A solução deverá realizar a coleta das informações sem a oneração excessiva do servidor de correio Microsoft Exchange, ou seja, sem ativação do journaling ou diagnostics nativos do servidor de correio;

10. 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 anormalidades nesses comportamentos;

11. A solução deverá coletar informações de ferramentas de perímetro para monitorar atividades na borda da organização de forma a adicionar contexto a segurança dos dados não estruturados e usuários internos.

Para controle e gestão de contas privilegiadas a solução deve:

1. Possuir armazenamento seguro e controle de credenciais não pessoais e privilegiadas em Servidores Linux/Unix, Windows, Sistemas, Aplicações Web, Bancos de Dados, Estações de Trabalho e Dispositivos de Rede, totalizando 100 usuários ou 6.550 dispositivos. Deve permitir que até 80 usuários estejam conectados simultaneamente;
2. Provisionamento de usuários locais em servidores Linux/Unix, Windows ou dispositivos de rede;
3. Notificar, via e-mail ou SMS, novas solicitações de aprovação de acesso aos respectivos responsáveis pelas credenciais;
4. Suportar a implementação em parque computacional Windows Server 2016, Windows Server 2019, Windows Server 2022 e superiores;
5. Suportar a implementação em parque computacional Linux Ubuntu;
6. Incorporar medidas de segurança, incluindo criptografia a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações Web dos usuários finais;
7. Ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (cofre), para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas gerenciadas pela solução;
8. Não permitir a abertura do cofre com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes em hipótese alguma;
9. A solução deve integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas;
10. Permitir o Backup e Recovery de seu Banco de Dados, bem como das Configurações de Software estabelecidas;
11. Utilizar um banco de dados que permita alta disponibilidade e mecanismos para a recuperação de desastres e que também sejam compatíveis com soluções de backup e arquivamento disponíveis no mercado;
12. Proxy Transparente com gravação de logs e vídeos ao sistema alvo sem revelar aos usuários as credenciais utilizadas através do cliente local utilizado pelo usuário como Putty, ou RDP Client sem necessidade de abrir interface web ou baixar nenhum cliente adicional na máquina do usuário.

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

As soluções devem estar aderentes e em conformidade com as orientações do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações - CEPESC quanto aos procedimentos e documentações exigidos.

7. Estimativa da demanda - quantidade de bens e serviços

GRUPO 1: Para a **Solução de Auditoria Interna de Rede**, a ABIN possui licenças perpétuas do software Varonis DatAdvantage, sem atualização e suporte desde julho de 2019, a seguir descritas:

1. Varonis DatAdvantage for Windows File Server para 1.300 usuários;
2. Varonis DatAdvantage for Directory Server para 400 usuários;
3. Varonis DatAdvantage for Exchange Server para 400 usuários;
4. Varonis DatAlert Suite para 1.300 usuários.

5. Assim, será permitido ao proponente a regularização do parque vencido com fornecimento de garantia e atualização, juntamente com o licenciamento dos usuários adicionais (expansão), nivelando o tempo da garantia e atualização para todas as licenças, totalizando a quantidade de usuários descritos na tabela abaixo para o período exigido;
6. A quantidade de licenças é justificada devido ao número de servidores da Agência, que recentemente teve uma expansão em seu quadro de pessoal, totalizando aproximadamente 1.400 servidores;
7. A solução deverá permitir auditar, controlar, gerenciar e monitorar as ações dos usuários, dos serviços de administração de diretório de usuários, servidor de arquivos, e-mail e outros, bem como prevenir ações e comportamentos suspeitos em tempo real, e proteger os dados.

GRUPO 2: Para o **Portal de Gerenciamento de Identidades Privilegiadas** a solução deve:

1. Possuir armazenamento seguro e controle de credenciais não pessoais e privilegiadas em Servidores Linux /Unix, Windows, Sistemas, Aplicações Web, Bancos de Dados, Estações de Trabalho e Dispositivos de Rede, totalizando 100 usuários ou 6.550 dispositivos;
2. Suportar 300 Servidores Linux/Unix e Windows;
3. Suportar 250 ativos de rede;
4. Suportar 3.000 Estações de Trabalho;
5. Deve permitir que até 80 usuários estejam conectados simultaneamente;
6. Este quantitativo foi estimado levando em conta a infraestrutura local, incluindo, analistas de infraestrutura, desenvolvedores, analistas de rede e servidores do órgão que possuem acesso privilegiado. Além disso, as quantidades de dispositivos são com base na topologia atual e mapeamento realizado pela equipe técnica.

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QTDE
GRUPO 1 **Solução de Auditoria Interna de Rede**	1	Renovação Varonis DatAdvantage for Windows File server para 12 meses	Un.	1.300
	2	Renovação Varonis DatAdvantage for Active Directory para 12 meses	Un.	400
	3	Renovação Varonis DatAdvantage for Microsoft Exchange para 12 meses	Un.	400
	4	Renovação Varonis DatAlert para 12 meses	Un.	1.300
	5	Expansão Varonis DatAdvantage for Windows File server para 12 meses	Un.	100
	6	Expansão Varonis DatAdvantage for Active Directory para 12 meses	Un.	1.000
	7	Expansão Varonis DatAdvantage for Microsoft Exchange para 12 meses	Un.	1.000
	8	Expansão Varonis DatAlert para 12 meses	Un.	100
	9	*Operação assistida	horas	250
GRUPO 2 **Portal de Gerenciamento de Identidades Privilegiadas**	1	Solução de Portal de gerenciamento de Identidades Privilegiadas para 12 meses	Un.	100
	2	*Operação assistida	horas	250

8. Levantamento de soluções

IDENTIFICAÇÃO DAS SOLUÇÕES

3.1.1. **GRUPO 1 - Solução de Auditoria Interna de Rede**: A Agência possui licenças perpétuas do software Varonis DatAdvantage vencidas desde julho de 2019, permitido ao proponente a regularização do parque vencido com fornecimento de garantia e atualização, juntamente com o licenciamento dos usuários adicionais (expansão), nivelando o tempo da garantia e atualização para todas as licenças. Este fator indica que a renovação/expansão entra no critério de melhor custo-benefício, pois já existe a solução implantada no ambiente. Outras soluções para esse grupo implicariam na inutilização das licenças de propriedade da Agência, além de gerarem demasiado ônus devido à necessidade de readequação dos sistemas.

3.1.2. **GRUPO 2 - Portal de Gerenciamento de Identidades Privilegiadas**: Com a ampliação do ambiente de comunicação segura faz-se necessário a melhoria de requisitos de segurança, uma vez que o controle sobre um número maior de dispositivos/usuários demanda maior dedicação das equipes do CEPESC. Controle este que se torna impraticável se considerados os atuais recursos disponíveis para essa tarefa. Sendo assim, é necessário a aquisição e integração de novas ferramentas e soluções que permitam a correção de vulnerabilidades já detectadas nesse ambiente, bem como possibilitem a otimização do controle e do gerenciamento dos recursos postos à disposição dos usuários.

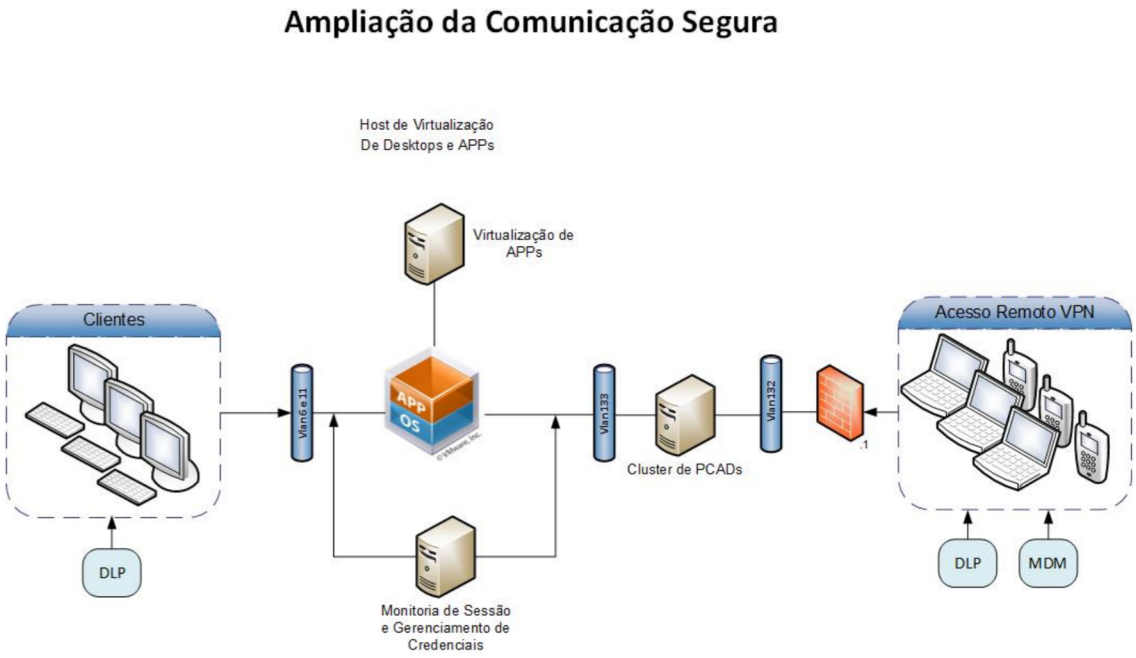

Figura 1 - Ambiente proposto para ampliação da comunicação segura

3.1.2.1. Soluções identificadas para o Grupo 2:

a) Contratação de ferramenta de Privileged Access Management (PAM) para adicionar a funcionalidade de gerenciamento de credenciais privilegiadas, além do gerenciamento de sessões privilegiadas e de acesso privilegiado a aplicativos e serviços. As ferramentas de PAM ajudam as organizações a fornecer acesso privilegiado seguro a ativos críticos e a atender aos requisitos de conformidade, gerenciando e monitorando contas e acesso privilegiados. Com a ferramenta de PAM pretende-se atender aos seguintes requisitos:

- Descoberta de contas privilegiadas em sistemas, dispositivos e aplicativos para gerenciamento subsequente;
- Gerenciamento e proteção automática de senhas e outras credenciais para contas administrativas, de serviço e de aplicativos;
- Controle de acesso de contas privilegiadas, incluindo contas compartilhadas;
- Isolamento, monitoramento, registro e auditoria de sessões, comandos e ações de acesso privilegiado;
- Fornecimento de logon único (SSO - Single Sign On) para sessões, comandos e ações privilegiadas com segurança para não revelar credenciais da conta (senhas, chaves criptográficas, etc.);
- Delegar, controlar e filtrar operações privilegiadas que um administrador pode executar;
- Garantia de níveis necessários de confiança e responsabilidade pelo acesso privilegiado, que forneça recursos robustos de autenticação ou integre produtos ou serviços de autenticação externa.

b) Eliminação de senhas codificadas, disponibilizando-as sob demanda para aplicativos. Neste caso, uma das duas categorias distintas de ferramentas, que evoluíram para segurança e gerenciamento de riscos, pode ser utilizada:

- **Gerenciamento de elevação e delegação de privilégios (PEDM)**: Privilégios específicos são concedidos no sistema gerenciado por agentes baseados em host para usuários conectados. Isso inclui controle de comando baseado em host

(filtragem) e elevação de privilégio, este último na forma de permitir que comandos específicos sejam executados com um nível mais alto de privilégios;

- **Gerenciamento privilegiado de contas e sessões (PASM)**: contas privilegiadas são protegidas protegendo suas credenciais. O acesso a essas contas é então intermediado para usuários, serviços e aplicativos humanos. As funções de gerenciamento de sessão privilegiada (PSM) estabelecem sessões com possível injeção de credenciais e gravação de sessão completa. Senhas e outras credenciais para contas privilegiadas são gerenciadas ativamente, como alterações em intervalos definidos ou na ocorrência de eventos específicos. As soluções PASM também podem fornecer gerenciamento de senha de aplicativo a aplicativo (AAPM).

Considerando o cenário de mercado das contratações públicas:

<table>
<tr><td>POSSIBILIDADE CONSIDERADA

(IN SGD 01/2019, art. 11,II)</td><td colspan="3">CONSTATADO NO ESTUDO</td></tr>
<tr><td rowspan="13">Necessidades Similares na Administração Pública e soluções adotadas:</td><td>ÓRGÃO</td><td>NECESSIDADE DE TIC</td><td>SOLUÇÃO DE TIC</td></tr>
<tr><td>Agência Nacional de Aviação Civil - ANAC</td><td>Solução de TIC para gestão, monitoração, auditoria, automação e prevenção de perdas de dados nos serviços de diretório, correio eletrônico e servidores de arquivos.</td><td>Aquisição de licenças perpétuas de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos (Microsoft File Server).
PREGÃO ELETRÔNICO Nº 28/2019</td></tr>
<tr><td>Agência Nacional de Águas e Saneamento Básico - ANA</td><td>Solução de TIC para classificação, monitoramento e auditoria de dados e comportamento de usuários.</td><td>Contratação de empresa especializada em TIC para fornecimento de solução de classificação, monitoramento e auditoria de dados e comportamento de usuários, incluindo instalação, capacitação técnica, suporte técnico e garantia.
PREGÃO ELETRÔNICO Nº 24/2020</td></tr>
<tr><td>Agência Nacional de Transportes Terrestres - ANTT</td><td>Solução de TIC de auditoria, monitoramento e gerenciamento de acessos do ambiente Microsoft .</td><td>Contratação de solução de auditoria, monitoramento e gerenciamento de acessos do ambiente Microsoft , para atender as necessidades da ANTT.
PREGÃO ELETRÔNICO Nº 26/2022</td></tr>
<tr><td rowspan="12">Alternativas de mercado:</td><td rowspan="4">Grupo 1

Solução de Auditoria Interna de Rede</td><td>ID. DA SOLUÇÃO</td><td>DESCRIÇÃO DA SOLUÇÃO</td></tr>
<tr><td>Solução 1</td><td>Varonis - Solução de auditoria, gestão, automação, monitoramento e gerenciamento de serviços.</td></tr>
<tr><td>Solução 2</td><td>Netwrix - Solução de auditoria, gestão, automação, monitoramento e gerenciamento de serviços.</td></tr>
<tr><td>Solução 3</td><td>ManageEngine - Solução de auditoria, gestão, automação, monitoramento e gerenciamento de serviços.</td></tr>
<tr><td rowspan="4">Grupo 2

Portal de Gerenciamento de Identidades Privilegiadas</td><td>ID. DA SOLUÇÃO</td><td>DESCRIÇÃO DA SOLUÇÃO</td></tr>
<tr><td>Solução 1</td><td>SenhaSegura - Solução de gestão e controle de acesso para identidades privilegiadas.</td></tr>
<tr><td>Solução 2</td><td>Cyberark - Solução de gestão e controle de acesso para identidades privilegiadas.</td></tr>
<tr><td>Solução 3</td><td>BeyondTrust - Solução de gestão e controle de acesso para identidades privilegiadas.</td></tr>
<tr><td>Existência de software público brasileiro:</td><td colspan="3">Após análise junto ao Portal de Software Público Brasileiro, não se encontrou solução que possa atender os requisitos do objeto desse Estudo.</td></tr>
<tr><td>Políticas, os</td><td colspan="3"></td></tr>
</table>

modelos e os padrões de governo:	Não se aplica.
Necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual:	a) infraestrutura tecnológica; b) logística de implantação; c) Infraestrutura lógica.
Possibilidade de aquisição na forma de bens ou contratação como serviço:	Não se aplica, pois se trata de aquisição de bens. Dadas as características de segurança orgânica, a ABIN limita a maioria dos serviços e soluções para que sejam fornecidas no modelo "on remise", ou seja, em seu próprio ambiente. Essa limitação restringe o universo de soluções que atendem às necessidades da ABIN, já que, na maioria das vezes, não se permite adoção de soluções "as a service" (como serviço).
Diferentes modelos de prestação do serviço:	Não se aplica.
Diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes:	Soluções de software livre trata-se de uma composição de pelo menos seis (6) desenvolvedores distintos, cada um atuando em uma área específica. São necessários diversos treinamentos para operação dos sistemas que, apesar de similares, trabalham com sintaxes distintas em seus softwares, sendo necessários diferentes treinamentos para cada fabricante. Também foi identificado que algumas soluções estudadas não possuem capacitação disponível no mercado bem como garantia de atualizações, correções de falhas e suporte técnico dependendo unicamente de informações compartilhadas em fóruns da comunidade dos softwares livres. Manter e gerenciar uma solução totalmente redundante com softwares diferentes acarreta custo operacional elevado, bem como alto custo de manutenção de contrato. Dificulta, ainda, o estabelecimento de processos de gestão da segurança da informação, inviabilizando a especialização da equipe para operação dos sistemas e suas funcionalidades, visto que serão necessários diversos treinamentos para softwares distintos que nem sempre irão garantir sua interoperabilidade.
Ampliação ou substituição da solução implantada:	A renovação e expansão se dará referente aos itens de 1 a 9 que se encontram no Grupo 1 da tabela do tópico 2 - Estimativa da Demanda - Quantidade de Bens e Serviços.
Diferentes métricas de prestação do serviço e de pagamento:	Os itens serão metrificados com base em quantidade de usários/dispositivos e horas para a operação assistida.

9. Análise comparativa de soluções

ANÁLISE COMPARATIVA DE SOLUÇÕES

GRUPO	REQUISITO	SOLUÇÃO Nº	SIM	NÃO	NÃO SE APLICA
	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
		Solução 2	X		
		Solução 3	X		

GRUPO 1 Solução de Auditoria Interna de Rede	A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
		Solução 2			X
		Solução 3			X
	A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
		Solução 2		X	
		Solução 3		X	
	A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
		Solução 2			X
		Solução 3			X
	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
		Solução 2			X
		Solução 3			X
	A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
		Solução 2			X
		Solução 3			X

GRUPO	REQUISITO	SOLUÇÃO Nº	SIM	NÃO	NÃO SE APLICA
GRUPO 2 Portal de Gerenciamento de Identidades Privilegiadas	A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
		Solução 2	X		
		Solução 3	X		
	A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
		Solução 2			X
		Solução 3			X
	A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
		Solução 2		X	
		Solução 3		X	
	A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
		Solução 2			X
		Solução 3			X
	A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
		Solução 2			X
		Solução 3			X
	A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
		Solução 2			X
		Solução 3			X

MAPA COMPARATIVO

GRUPO	ASPECTO DA SOLUÇÃO	SOLUÇÃO 1	SOLUÇÃO 2	SOLUÇÃO 3
	Necessidade de ajuste da infraestrutura atual:	Não será necessário realizar nenhuma mudança na infraestrutura do ambiente.	Não será necessário realizar nenhuma mudança na infraestrutura do ambiente.	Não será necessário realizar nenhuma mudança na infraestrutura do ambiente.
	Necessidade de contratação de serviços adicionais correlacionados ao objeto da contratação:	Não, a presente solução engloba todas as características necessárias para ser implementada.	Não, a presente solução engloba todas as características necessárias para ser implementada.	Não, a presente solução engloba todas as características necessárias para ser implementada.
	Grau de dependência tecnológica:	Baixo	Baixo	Baixo
		Alto, existem algumas	Alto, existem algumas	Alto, existem algumas

GRUPO 1 Solução de Auditoria Interna de Rede	Grau de integração de serviços e usabilidade ao usuário:	integrações com serviços, como diretório de usuários, arquivos, e-mail e outros.	integrações com serviços, como diretório de usuários, arquivos, e-mail e outros.	integrações com serviços, como diretório de usuários, arquivos, e-mail e outros.
	Necessidade de revisão de processos de trabalho para utilização mais eficiente da solução:	Não aplicável	Aplicável	Aplicável
	Maturidade no mercado de fornecimento da solução:	Consolidado	Consolidado	Não consolidado no mercado nacional
	Pontos de falha:	No próprio sistema ou na infraestrutura local	No próprio sistema ou na infraestrutura local	No próprio sistema ou na infraestrutura local
	Encargos de implantação da solução:	Moderado, por se tratar de solução que contempla integração com alguns serviços	Moderado, por se tratar de solução que contempla integração com alguns serviços	Moderado, por se tratar de solução que contempla integração com alguns serviços
	Necessidade de treinamento para o usuário:	Não, o usuário final não tem a necessidade de um treinamento, a solução é transparente.	Não, o usuário final não tem a necessidade de um treinamento, a solução é transparente.	Não, o usuário final não tem a necessidade de um treinamento, a solução é transparente.
	Necessidade de capacitação para a equipe de operações:	A capacitação deve ser para os administradores e equipe de operação.	A capacitação deve ser para os administradores e equipe de operação.	A capacitação deve ser para os administradores e equipe de operação.
	Consumo energético:	Baixo	Baixo	Baixo
	Necessidade de monitoramento da solução de hardware e de software:	Sim, monitoramento do software.	Sim, monitoramento do software.	Sim, monitoramento do software.

GRUPO	ASPECTO DA SOLUÇÃO	SOLUÇÃO 1	SOLUÇÃO 2	SOLUÇÃO 3
GRUPO 2 Portal de Gerenciamento de Identidades Privilegiadas	Necessidade de ajuste da infraestrutura atual:	Não será necessário realizar nenhuma mudança na infraestrutura do ambiente.	Não será necessário realizar nenhuma mudança na infraestrutura do ambiente.	Não será necessário realizar nenhuma mudança na infraestrutura do ambiente.
	Necessidade de contratação de serviços adicionais correlacionados ao objeto da contratação:	Não, a presente solução engloba todas as características necessárias para ser implementada.	Não, a presente solução engloba todas as características necessárias para ser implementada.	Não, a presente solução engloba todas as características necessárias para ser implementada.
	Grau de dependência tecnológica:	Baixo	Baixo	Baixo
	Grau de integração de serviços e usabilidade ao usuário:	Alto, existem algumas integrações com serviços, como diretório de usuários, arquivos, e-mail e outros.	Alto, existem algumas integrações com serviços, como diretório de usuários, arquivos, e-mail e outros.	Alto, existem algumas integrações com serviços, como diretório de usuários, arquivos, e-mail e outros.
	Necessidade de revisão de processos de trabalho para utilização mais eficiente da solução:	Aplicável, a utilização da ferramenta altera o fluxo de acesso aos serviços/servidores do ambiente.	Aplicável, a utilização da ferramenta altera o fluxo de acesso aos serviços/servidores do ambiente.	Aplicável, a utilização da ferramenta altera o fluxo de acesso aos serviços/servidores do ambiente.
	Maturidade no mercado de fornecimento da solução:	Consolidado	Consolidado	Consolidado
	Pontos de falha:	No próprio sistema ou na infraestrutura local	No próprio sistema ou na infraestrutura local	No próprio sistema ou na infraestrutura local
		Moderado, por se tratar de	Moderado, por se tratar de	Moderado, por se tratar de

	Encargos de implantação da solução:	solução que contempla integração com alguns serviços	solução que contempla integração com alguns serviços	solução que contempla integração com alguns serviços
	Necessidade de treinamento para o usuário:	Aplicável apenas para usuários com acesso privilegiado.	Aplicável apenas para usuários com acesso privilegiado.	Aplicável apenas para usuários com acesso privilegiado.
	Necessidade de capacitação para a equipe de operações:	A capacitação deve ser para os administradores e usuários privilegiados que farão uso da solução.	A capacitação deve ser para os administradores e usuários privilegiados que farão uso da solução.	A capacitação deve ser para os administradores e usuários privilegiados que farão uso da solução.
	Consumo energético:	Baixo	Baixo	Baixo
	Necessidade de monitoramento da solução de hardware e de software:	Sim, monitoramento do software.	Sim, monitoramento do software.	Sim, monitoramento do software.

10. Registro de soluções consideradas inviáveis

Soluções de software livre não devem ser consideradas viáveis, em função do custo operacional elevado e alto custo da gestão contratual.

11. Análise comparativa de custos (TCO)

CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

Das soluções identificadas para o Grupo 1, a renovação das licenças perpétuas que a ABIN já possui e a contratação da subscrição de novas licenças (expansão) se mostrou mais vantajosa, pois a solução já se encontra implantada na ABIN, o custo da renovação é mais barato que a aquisição completa de nova subscrição e a equipe técnica já possui conhecimento para administrar a solução. A aquisição de uma nova solução implica, necessariamente, migrar todo o ambiente para a nova solução, afetando os processos e procedimentos atualmente realizados pela equipe técnica e usuários da ferramenta.

Para o Grupo 2, a solução viável é a contratação de uma solução nova de controle de acessos privilegiadas a ser implantada na ABIN.

A opção de contratação como serviço em nuvem não foi levada em consideração uma vez que a política de segurança em vigor na ABIN proíbe esse tipo de solução.

A estimativa de preço do objeto deste processo seguiu as normas estipuladas pela IN SLTI/MPOG 73/2020, que orienta que a pesquisa de preços deverá ser realizada, em ordem de preferência, no Painel de Preços, aquisições e contratações similares de outros entes públicos, dados de pesquisa publicada em mídia especializada e por último em pesquisa direta com fornecedores.

A partir dos valores encontrados, foi elaborada a planilha a seguir, onde o valor que consta na coluna "Valor Médio Unitário" é a média simples dos valores encontrados para cada item, desprezando os valores nulos que aparecem na tabela. E o preço médio total é mostrado na coluna "Valor Médio Total". Assim, o valor total estimado da contratação é de **R$ 2.715.783,40 (dois milhões, setecentos e quinze mil, setecentos e oitenta e três reais e quarenta centavos)**.

					ANTT PE-26	**CAPES - IRP**	**Proposta Comercial**	**Proposta Comercial**	**Proposta Comercial**	**Proposta Comercial**	**Valor Médio**	**Valor Médi**

Grupo	Item	Descrição	Unidade	Quantidade	/2022	PE-11 /2022	NTSEC	Arvvo	Layer Tecnologia	Petacorp	Unitário	Total
Grupo 1 Solução de Auditoria Interna de Rede	1	Renovação Varonis DatAdvantage for Windows File server para 12 meses	UND	1.300	R$175,73	-	R$270,67	R$161,27	R$162,77	R$147,27	R$183,54	R$238.604,(
	2	Renovação Varonis DatAdvantage for Active Directory para 12 meses	UND	400	R$182,23	-	R$409,05	R$160,02	R$171,45	R$148,59	R$214,27	R$85.707,2
	3	Renovação Varonis DatAdvantage for Microsoft Exchange para 12 meses	UND	400	-	-	R$409,05	R$160,02	R$185,46	R$148,56	R$225,77	R$90.309,(
	4	Renovação Varonis DatAlert para 12 meses	UND	1.300	R$200,95	-	R$280,88	R$174,32	R$177,95	R$148,05	R$196,43	R$255.359,(
	5	Expansão Varonis DatAdvantage for Windows File server para 12 meses	UND	100	-	R$415,84	R$791,80	R$372,03	R$462,59	R$368,61	R$482,17	R$48.217,4
	6	Expansão Varonis DatAdvantage for Active Directory para 12 meses	UND	1.000	-	R$506,89	R$353,12	R$380,60	R$478,84	R$369,27	R$417,74	R$417.744,(
	7	Expansão Varonis DatAdvantage for Microsoft Exchange para 12 meses	UND	1.000	R$448,36	R$470,04	R$353,12	R$380,60	R$415,24	R$372,13	R$406,58	R$406.581,(
	8	Expansão Varonis DatAlert para 12 meses	UND	100	-	R$460,95	R$791,80	R$372,03	R$460,23	R$372,36	R$491,47	R$49.147,4
	9	*Operação Assistida	HORAS	250	R$262,50	R$226,84	R$490,00	R$326,05	R$302,16	R$357,00	R$327,43	R$81.856,2
Grupo 2: Portal de Gerenciamento de Identidades Privilegiados	1	Solução de Portal de permissionamento para 12 meses	UND	1	-	-	-	R$915.371,51	R$1.025.632,14	R$922.922,00	R$954.641,88	R$954.641,8
	2	*Operação Assistida	HORAS	250	-	-	-	R$315,76	R$415,62	R$320,00	R$350,46	R$87.615,(
											TOTAL	**R$2.715.783**

Para implantação das soluções, na fase de instalação/configuração/atualização das ferramentas, será realizado repasse de conhecimento por meio de treinamento hands-on para nivelar o conhecimento da equipe técnica do CEPESC.

MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Para calcular o custo total de propriedade, foi realizado o cálculo anual até o período de 48 meses, sem considerar nenhuma variação nos preços listados em cada item e sem considerar nenhum indicador econômico ao longo dos anos.

O Cenário 1 é o cálculo anual do TCO, considerando os mesmos valores obtidos para renovação/expansão nas propostas comerciais, totalizando ao longo de 48 meses o valor de **R$ 10.863.133,60 (dez milhões, oitocentos e sessenta e três mil, cento e trinta e três reais e sessenta centavos)**.

CENÁRIO 1	MAPA COMPARATIVO - RENOVAÇÃO / EXPANSÃO				Valor Médio Unitário	Valor Médio Total	Cálculo do Custo Total de Propriedade (TCO)				TOTA
Grupo	Item	Descrição	Unidade	Qtde			Ano 1	Ano 2	Ano 3	Ano 4	Al
Grupo 1 Solução de Auditoria Interna de Rede	1	Renovação Varonis DatAdvantage for Windows File server para 12 meses	UND	1.300	R$183,54	R$238.604,60	R$238.604,60	R$238.604,60	R$238.604,60	R$238.604,60	R$95
	2	Renovação Varonis DatAdvantage for Active Directory para 12 meses	UND	400	R$214,27	R$85.707,20	R$85.707,20	R$85.707,20	R$85.707,20	R$85.707,20	R$34
	3	Renovação Varonis DatAdvantage for Microsoft Exchange para 12 meses	UND	400	R$225,77	R$90.309,00	R$90.309,00	R$90.309,00	R$90.309,00	R$90.309,00	R$36
	4	Renovação Varonis DatAlert para 12 meses	UND	1.300	R$196,43	R$255.359,00	R$255.359,00	R$255.359,00	R$255.359,00	R$255.359,00	R$1.0
	5	Expansão Varonis DatAdvantage for Windows File server para 12 meses	UND	100	R$482,17	R$48.217,40	R$48.217,40	R$48.217,40	R$48.217,40	R$48.217,40	R$19
	6	Expansão Varonis DatAdvantage for Active Directory para 12 meses	UND	1.000	R$417,74	R$417.744,00	R$417.744,00	R$417.744,00	R$417.744,00	R$417.744,00	R$1.6
	7	Expansão Varonis DatAdvantage for Microsoft Exchange para 12 meses	UND	1.000	R$406,58	R$406.581,67	R$406.581,67	R$406.581,67	R$406.581,67	R$406.581,67	R$1.6
	8	Expansão Varonis DatAlert para 12 meses	UND	100	R$491,47	R$49.147,40	R$49.147,40	R$49.147,40	R$49.147,40	R$49.147,40	R$19
	9	*Operação Assistida	HORAS	250	R$327,43	R$81.856,25	R$81.856,25	R$81.856,25	R$81.856,25	R$81.856,25	R$32
					SUBTOTAL	**R$1.673.526,52**	**R$1.673.526,52**	**R$1.673.526,52**	**R$1.673.526,52**	**R$1.673.526,52**	**R$6.6**
Grupo 2: Portal de Gerenciamento de Identidades Privilegiados	1	Solução de Portal de permissionamento para 12 meses	UND	1	R$954.641,88	R$954.641,88	R$954.641,88	R$954.641,88	R$954.641,88	R$954.641,88	R$3.8
	2	*Operação Assistida	HORAS	250	R$350,46	R$87.615,00	R$87.615,00	R$87.615,00	R$87.615,00	R$87.615,00	R$35
					SUBTOTAL	**R$1.042.256,88**	**R$1.042.256,88**	**R$1.042.256,88**	**R$1.042.256,88**	**R$1.042.256,88**	**R$4.1**
					TOTAL	**R$2.715.783,40**	**R$2.715.783,40**	**R$2.715.783,40**	**R$2.715.783,40**	**R$2.715.783,40**	**R$10.8**
						TOTAL ACUMULADO	**R$2.715.783,40**	**R$5.431.566,80**	**R$8.147.350,20**	**R$10.863.133,60**	

O Cenário 2 é o cálculo anual do TCO, considerando os mesmos valores obtidos para aquisição (expansão) nas propostas comerciais e somando a quantidade (renovação + expansão) para o mesmo item/produto. Com isso, totalizando ao longo de 48 meses o valor de **R$ 14.565.105,07 (quatorze milhões, quinhentos e sessenta e cinco mil, cento e cinco reais e sete centavos)**.

CENÁRIO 2	MAPA COMPARATIVO - RENOVAÇÃO / EXPANSÃO				Valor Médio Unitário	Valor Médio Total	Cálculo do Custo Total de Propriedade (TCO)				TOT
Grupo	Item	Descrição	Unidade	Qtde			Ano 1	Ano 2	Ano 3	Ano 4	
Grupo 1 Solução de Auditoria Interna de Rede	5	Aquisição Varonis DatAdvantage for Windows File server para 12 meses	UND	100	R$482,17	R$675.043,60	R$675.043,60	R$675.043,60	R$675.043,600	R$675.043,60	R$2.
	6	Aquisição Varonis DatAdvantage for Active Directory para 12 meses	UND	1.000	R$417,74	R$584.841,60	R$584.841,60	R$584.841,60	R$584.841,60	R$584.841,60	R$2.
	7	Aquisição Varonis DatAdvantage for Microsoft Exchange para 12 meses	UND	1.000	R$406,58	R$569.214,33	R$569.214,33	R$569.214,33	R$569.214,33	R$569.214,33	R$2.
	8	Aquisição Varonis DatAlert para 12 meses	UND	100	R$491,47	R$688.063,60	R$688.063,60	R$688.063,60	R$688.063,60	R$688.063,60	R$2.
	9	*Operação Assistida	HORAS	250	R$327,43	R$81.856,25	R$81.856,25	R$81.856,25	R$81.856,25	R$81.856,25	R$3
					SUBTOTAL	**R$2.599.019,38**	**R$2.599.019,38**	**R$2.599.019,38**	**R$2.599.019,38**	**R$2.599.019,38**	**R$10**
Grupo 2: Portal de Gerenciamento de Identidades Privilegiados	1	Solução de Portal de permissionamento para 12 meses	UND	1	R$954.641,88	R$954.641,88	R$954.641,88	R$954.641,88	R$954.641,88	R$954.641,88	R$3.
	2	*Operação Assistida	HORAS	250	R$350,46	R$87.615,00	R$87.615,00	R$87.615,00	R$87.615,00	R$87.615,00	R$3
					SUBTOTAL	**R$1.042.256,88**	**R$1.042.256,88**	**R$1.042.256,88**	**R$1.042.256,88**	**R$1.042.256,88**	**R$4.**
					TOTAL	**R$3.641.276,27**	**R$3.641.276,27**	**R$3.641.276,27**	**R$3.641.276,27**	**R$3.641.276,27**	**R$14.**
						TOTAL ACUMULADO	**R$3.641.276,27**	**R$7.282.552,53**	**R$10.923.828,80**	**R$14.565.105,07**	

A partir desses dois cenários, obtem-se a diferença percentual entre renovar as licenças perpétuas (cenário 1) ou adquirir novas subscrições (cenário 2). Assim sendo, verifica-se que o cenário 1 é economicamente mais viável que o cenário 2, quando se obtém um valor total inferior de 25,42% (Percentual A). Ou seja, a aquisição (Cenário 2) apresenta um custo superior 34,08% (Percentual B) em relação a renovação (cenário 1), conforme demonstrado no quadro abaixo.

MAPA COMPARATIVO - CENÁRIO 1 x CENÁRIO 2	
Valor Total TCO Renovação/Expansão (Cenário 1)	**R$10.863.133,60**
Valor Total TCO Aquisição (Cenário 2)	**R$14.565.105,07**
Diferença (Cenário2 - Cenário1)	**R$ 3.701.971,47**
Percentual A (Diferença / Cenário2)	**25,42%**

Percentual B (Diferença / Cenário1)	**34,08%**

Diante do exposto, a renovação das licenças já existentes no ambiente é a melhor alternativa de solução para a contratação do grupo 1. Para o grupo 2, será contratada uma nova solução a ser implantada na agência.

12. Descrição da solução de TIC a ser contratada

Contratação de subscrições de soluções tecnológicas de software por 12 (doze) meses, renováveis por igual período até o limite de 48 meses, incluindo atualização de versões, serviços de suporte técnico, instalação, configuração e treinamento hands-on .

GRUPO 1 - Solução de Auditoria Interna de Rede: Solução de auditoria, gestão, automação, monitoramento e gerenciamento de serviços.

GRUPO 2 - Portal de Gerenciamento de Identidades Privilegiadas: Solução de gestão e controle de acesso para identidades privilegiadas.

13. Estimativa de custo total da contratação

Valor (R$): 3.524.000,00

O orçamento estimado previsto inicialmente foi de R$ 3.524.000,00 (três milhões, quinhentos e vinte e quatro mil reais), divididos entre investimento e custeio. Para a presente contratação, aplica-se o valor previsto apenas para custeio, no total de R$ 1.524.000,00 (um milhão, quinhentos e vinte e quatro mil reais). A aquisição consta no PDTIC 2021-2022 (Ação Estratégica de TIC ATIC 08 - Aprimorar segurança cibernética e segurança da informação e comunicações) e também no POA SEGOR 2023 (Ação "Modernizar sistemas de controle de acesso", subgrupo "Contratações para sede e para as SEs").

14. Justificativa técnica da escolha da solução

O Estudo Técnico Preliminar evidenciou que a contratação das soluções maximizam a probabilidade do alcance dos resultados pretendidos, atentando para a mitigação de riscos inerentes ao processo de contratação e aqueles relacionados a solução desejada, em observância dos princípios da economicidade, eficácia e eficiência desejados.

Considerando-se a necessidade dos recursos tecnológicos pretendidos para a manutenção das atividades e o cumprimento da missão institucional da ABIN, a equipe responsável pelo planejamento da contratação conclui que é técnica e economicamente viável a contratação proposta.

15. Justificativa econômica da escolha da solução

O Estudo Técnico Preliminar evidenciou que a contratação das soluções maximizam a probabilidade do alcance dos resultados pretendidos, atentando para a mitigação de riscos inerentes ao processo de contratação e aqueles relacionados a solução desejada, em observância dos princípios da economicidade, eficácia e eficiência desejados.

Considerando-se a necessidade dos recursos tecnológicos pretendidos para a manutenção das atividades e o cumprimento da missão institucional da ABIN, a equipe responsável pelo planejamento da contratação conclui que é técnica e economicamente viável a contratação proposta.

16. Benefícios a serem alcançados com a contratação

Com esta aquisição, o CEPESC pretende continuar provendo capacidade avançada em segurança da informação, adequada às novas realidades computacionais para análise de segurança e desempenho exigidos pelas soluções de criptografia utilizadas pelas áreas da ABIN. Com a aquisição proposta, pretende-se ainda:

a) Manter as diretrizes de TIC alinhadas aos Objetivos Estratégicos estabelecidos no Planejamento Estratégico 2022-2026 da ABIN;
b) Promover o uso de recursos tecnológicos que garantam agilidade e eficácia na consecução das atividades da Agência;
c) Garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
d) Permitir o gerenciamento e/ou execução de operações sigilosas de segurança para identificar ameaças ou acompanhar ocorrências de comprometimento ou violação da segurança orgânica. Neste sentido, ao registrar as ações dos servidores da ABIN nas redes e provedores internos, a solução em questão permite o acesso a dados negados de alvos de operações de segurança;
e) Melhorar a capacidade de gestão da segurança da informação, implementando controles adicionais e gerando informações que apoiem ações no sentindo de incrementar a segurança dos dados e informações armazenados no ambiente de TI da ABIN;
f) Garantir a segurança do ambiente de Tecnologia da Informação e Comunicação da ABIN, tornando-o mais seguro e confiável;
g) Permitir um controle adequado aos acessos privilegiados de servidores.

A gestão dos logs de auditorias e monitoramento adequado do ambiente de TI representa ganhos significativos para a infraestrutura de TI da Agência, tais como:
h) Registro dos acessos a arquivos realizados por cada usuário do ambiente;
i) Registro da utilização do serviço de e-mail institucional, com possibilidade de rastreamento de mensagens acessadas ou enviadas por um grupo de servidores, incluindo visibilidade sobre arquivos anexados;
j) Monitoramento de comportamentos anômalos no ambiente ocasionados por acessos privilegiados ou ataques de malwares que possam estar presentes no ambiente;
k) Monitoramento e auditoria das Estações de Trabalho (endpoints);
l) Gestão de acesso, monitoria e auditoria de acessos remotos ao ambiente de TI;
m) Possibilidade de geração de relatórios, de maneira tempestiva, que possam apoiar decisões de políticas de segurança na Agência e ações de ampliação de controle aos serviços de TI.

Além da renovação e expansão da solução de auditoria, a contratação de uma solução de controle e gestão de contas privilegiadas centralizará e permitirá uma gestão dos usuários de vários sistemas críticos, trará maior controle na administração, gestão e auditoria de acessos à rede corporativa e a todas as informações acerca dos diversos sistemas existentes no parque tecnológico, bem como aos diversos sistemas disponibilizados para o Órgão.

17. Providências a serem Adotadas

Não se aplica.

18. Declaração de Viabilidade

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

18.1. Justificativa da Viabilidade

O Estudo Técnico Preliminar evidenciou que a contratação das soluções maximizam a probabilidade do alcance dos resultados pretendidos, atentando para a mitigação de riscos inerentes ao processo de contratação e aqueles relacionados a solução desejada, em observância dos princípios da economicidade, eficácia e eficiência desejados.

Considerando-se a necessidade dos recursos tecnológicos pretendidos para a manutenção das atividades e o cumprimento da missão institucional da ABIN, a equipe responsável pelo planejamento da contratação conclui que é técnica e economicamente viável a contratação proposta.

19. Responsáveis

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

ALIANDRO RODRIGO DE OLIVEIRA GOMES

DIVGOV

Assinou eletronicamente em 04/05/2023 às 10:45:52.