Estudo Técnico Preliminar

1. Informações Básicas

Número do processo: 50500026118202219

2. Descrição da necessidade

O presente documento visa a contratação de empresa especializada para a manutenção e expansão da solução de auditoria e gerenciamento de serviços da Agência Nacional de Transportes Terrestres - ANTT, adquirida e mantida por meio do Contrato nº 54/2018, sem possibilidade regular de prorrogação, bem como o atendimento da necessidade de alteração do modelo de licenciamento de alguns serviços.

A ferramenta implantada no ambiente tecnológico da ANTT é composta por solução de Auditoria e Gerenciamento de Serviços (*Microsoft Active Directory – AD*), Servidor de Arquivos (*Microsoft File Server*), Correio Eletrônico (*Microsoft Exchanche Server*) e solução de análise de comportamento e alarme em tempo real (*DatAlert*), de uso permanente, incluindo execução de serviços técnicos especializados.

A auditoria de acessos de ambientes de serviços de arquivos, correio eletrônico e usuários é imprescindível para garantir a rastreabilidade de atividades realizadas baseadas em software. A manutenção da solução de auditoria que é a responsável pela comunicação e armazenamento dos dados não estruturados ou semiestruturados é fundamental para garantir o controle de acesso dos usuários da Agência.

Dessa forma, faz-se necessária a manutenção e atualização da solução de auditoria que garanta e amplie ações que fortaleçam a segurança das infraestruturas críticas da informação, controle e gerência de permissionamento dos serviços de AD (*Active Directory*), de servidor de Arquivos (*File Server*), de sistema de correio eletrônico (*Exchange*), como forma de centralizar e armazenar em banco de dados informações que permitam a rastreabilidade de quaisquer alterações (criação, modificação e exclusão) realizadas em objetos (contas de usuário, computadores, unidades organizacionais, objetos de diretivas de grupo e grupo dos serviços de tecnologia da ANTT.

3. Área requisitante

Área Requisitante	Responsável
Gerência de Infraestrutura Tecnológica	Victor Hugo Gouveia de Lucena Lima

4. Necessidades de Negócio

A pretensa contratação encontra-se alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação da ANTT - PDTIC 2021-2024, ao Planejamento Estratégico Institucional - PEI, de acordo com o Mapa Estratégico da ANTT 2020-2030, e ao Plano Anual de Contratações - PAC 2022, conforme tabela abaixo:

Alinhamento ao Planejamento Estratégico Institucional - PEI	
Planejamento Estratégico ANTT - 2020-2030	
ID	**Objetivo Estratégico**

PR2	aprimorar a disponibilidade, a qualidade e a integração das informações internas e externas

Alinhamento ao Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC
Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2021-2024

ID	**NECESSIDADE**
N10	Aperfeiçoar os mecanismos e ambientes para assegurar alta disponibilidade e evolução tecnológica

ID	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
-	Executar os serviços de gestão e manutenção de infraestrutura: dados em nuvem, site redundante, rede de dados, banco de dados, segurança.	-	Garantir a disponibilidade das aplicações em 99%

Alinhamento ao Plano Anual de Contratações - PAC		
Item no PAC	**Descrição**	**Aprovação**
3.41	Expansão da solução de auditoria e gerenciamento de serviços.	Aprovado na Revisão do Planejamento Anual de Contratações - PAC 2022, nos termos da Deliberação nº 171/2022.

A presente contratação visa a manutenção e atualização da solução de auditoria do ambiente da ANTT, a fim de garantir a eficiência, continuidade e evolução da solução, compreendendo a realização de atividades de manutenção corretivas e preventivas que visem garantir o adequado funcionamento da ferramenta, a disponibilização e aplicação de atualizações.

5. Necessidades Tecnológicas

A Contratada deverá prover a renovação da garantia técnica das licenças adquiridas pela ANTT e fornecer licenças de uso (subscrição) para atender o ambiente na nuvem, na forma dos itens abaixo listados:

a) Renovação da Solução de auditoria, controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory);

b) Renovação da Solução de auditoria, controle e gerência de permissionamento dos serviços de servidores de Arquivos (Microsoft File Server);

c) Aquisição de Subscrição do Módulo varonis DatAdvantage para Microsoft Exchange;

d) Renovação da Solução de Tecnologia da Informação de análise de comportamento e alarme em tempo real (DatAlert); e

e) Serviço Técnico Especializado.

A renovação da garantia técnica do produto se dará pelo período de 12 (doze) meses, podendo ser prorrogada pelo mesmo período até o limite de 36 (trinta e seis) meses.

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

A Contratada deverá fornecer todos os recursos necessários, tais como softwares, licenças e recursos humanos necessários à instalação e ativação das funcionalidades/licenças da solução.

7. Estimativa da demanda - quantidade de bens e serviços

Para o correto dimensionamento da quantidade de bens e serviços a serem contratados, a equipe de planejamento da contratação considerou para os itens 1, 2 e 4, as quantidades de licenças perpétuas adquiridas no Contrato nº 54/2018, que reflete o número de contas sob monitoramento no ambiente Microsoft da ANTT que necessitam de atualização; para o item 3 a quantidade de licenças perpétuas adquiridas no mesmo contrato, mas para atender o ambiente na nuvem; e o item 5, o histórico de horas executadas no contrato vigente.

Assim sendo, a estimativa da demanda deverá observar os itens e quantitativos da tabela abaixo:

Item	Descrição	Métrica	Quantidade
1	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Microsoft Active Directory (por 12 meses)	Licença	2.407
2	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Windows File Server (por 12 meses)	Licença	2.407
3	Subscrição do módulo Varonis DatAdvantage para Microsoft Exchange (por 12 meses)	Subscrição	2.407
4	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAlert (por 12 meses)	Licença	2.407
5	Serviço Técnico Especializado (por 12 meses)	Horas	600

8. Levantamento de soluções

Foram identificadas as seguintes soluções para atender as necessidades:

Solução	Descrição
Solução A - Manutenção da Solução Atual	Cenário que visa a manutenção das licenças proprietárias da ANTT on-premise.

Solução B - Manutenção e expansão da Solução Atual	Cenário que visa a manutenção das licenças proprietárias da ANTT on-premise e expansão da solução com a aquisição de licenciamento que atenda o ambiente em nuvem.
Solução C - Substituição da Solução Atual	Cenário que visa a substituição completa da solução atual.

9. Análise comparativa de soluções

Com base nas possíveis soluções identificadas, segue a análise abaixo:

Solução A - Manutenção da Solução Atual

A licenças proprietárias perpétuas da ANTT tem a limitaçao de auditar somente o ambiente on-premise, ou seja, somente o ambiente local. E a ANTT está utilizando atualmente o ambiente em nuvem, com o AD e e-mail já migrados para a nuvem e com projeto de migrar o servidor de arquivos. Nesse sentido, faz-se necessário que a solução atenda tanto o ambiente on-premise quanto o ambiente de nuvem. Dessa forma, a solução de manter apenas as licenças já existentes se mostram inviáveis para atender as necessidades tecnológicas atuais da ANTT.

Solução B - Manutenção e expansão da Solução Atual

A ANTT possui licenças proprietárias da solução VARONIS que são utilizadas na auditoria de seu ambiente local (on-premise). Contudo, a Agência vem migrando seu ambiente para a nuvem, o que torna necessário auditar tanto o ambiente local quanto o ambiente de nuvem. As licenças proprietárias só abrangem o ambiente local. Dessa forma, faz-se necessário adquirir subscrição para abranger também a auditoria e gerenciamento dos serviços já migrados para o ambiente de nuvem.

A solução atual da ANTT, do fabricante VARONIS, é utilizada por diversos órgãos da Administração Pública, a exemplo, da ANEEL, Ministério Público do Trabalho/Procuradoria Geral do Trabalho - MPT, Ministério da Educação/Instituto Nacional de Estudos e Pesquisas Educacionais - MEC, Conselho Federal de Engenharia Arquitetura e Agronomia – CONFEA, Tribunal Superior Eleitoral – TSE.

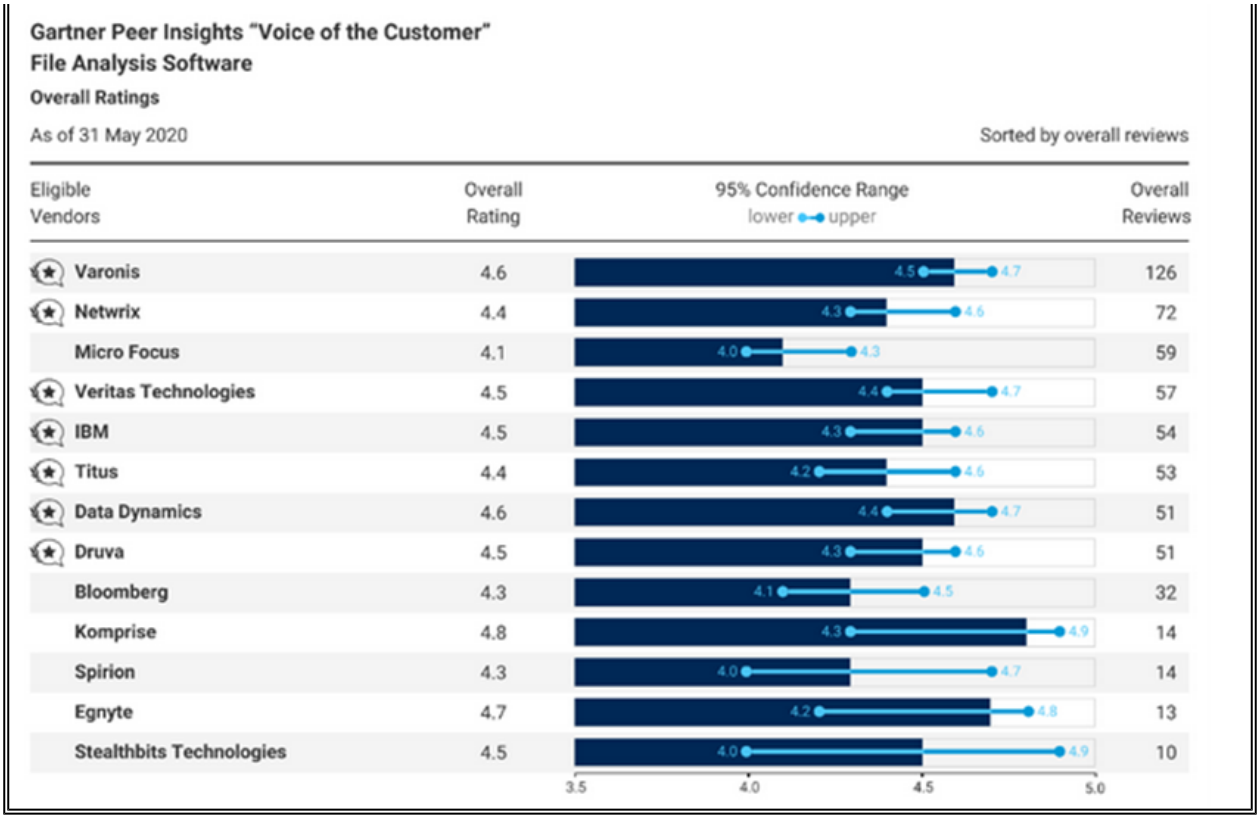
Na ANTT esta solução vem atendendo de forma satisfatória as necessidades de negócio e tecnológicas, ajudando na identificação de ações (tentativas e efetivadas) e seus responsáveis/autores no Active Directory, servidores de e-mail, servidores de arquivos, além de emitir alertas de baixo, médio e alto risco, contribuindo para o monitoramento e rastreabilidade no ambiente da ANTT. Ela se vale também da Análise do Comportamento do Usuário (UBA) e Análise do Comportamento do Usuário e da Entidade (UEBA) para estabelecer uma base sobre o comportamento considerado padrão ou normal, permitindo que qualquer ponto fora disso seja considerado suspeito; analisa e detecta atividade suspeita e previne o vazamento de dados, utilizando análise profunda de metadados, aprendizagem automática e UBA avançada; monitora acessos incomuns e atividades anormais em arquivos, e analisa alterações de políticas, escalação de associação e modificações em contas.

Assim sendo, a manutenção da solução e expansão com a aquisição de licenciamento que atenda os serviços migrados para o ambiente em nuvem, se mostra mais adequada.

Solução C - Substituição da Solução Atual

Considerando o quadro de avaliações referência do Gartner, na forma da tabela abaixo, a segunda solução melhor avaliada é a Netwrix. Em uma análise resumida observa-se que essa solução é voltada para organizações de pequeno porte, não possui granularidade nos relatórios, e tem implantação complexa. Além disso, possui interface não intuitiva e com desenho prejudicado para a visualização das informações, conforme relato de usuários.

Por fim, a aquisição de outra solução implicaria em uma nova implantação, com nova carga de aprendizagem, treinamento e integração no ambiente da ANTT, além de não aproveitar os investimentos já realizados na aquisição de licenças proprietárias.



Nesse sentido, a equipe entende que a solução de substituição da solução atual não se mostra adequada para o cenário atual das necessidades tecnológicas da ANTT.

Contratações similares realizadas por outros órgãos ou entidades da Administração Pública

Com base nos parâmetros dispostos na IN nº 73/2020, foram realizadas consultas no painel de preços/comprasnet (SEI nº 12782856) e com a Administração Pública (SEI nº 12782875), sendo identificado os seguintes resultados aderentes ao objeto:

Descrição	**UASG**	**ANÁLISE**
CT Nº 54/2018* - ANTT	393001	Contrato atual da ANTT. Utilizado no valor de referência, no que se refere ao item de serviço.
CT Nº 23/2021 - ANEEL	323028	Objeto similar. Valores utilizados na referência.
PE Nº 16/2020 - MME (Cancelado no Julgamento*)	320004	Objeto similar. Mas, o pregão foi cancelado no julgamento.

Com base nos resultados reportados no painel de preços, órgãos da Administração Pública e Pesquisa a fornecedores, considerando as especificidades do objeto obteve os seguintes resultados:

Lote	Item	Descrição	Métrica	Quantidade	REFERÊNCIAS											
					A CT Nº 54/2018* ANTT		B CT Nº 23/2021 ANEEL		C PE Nº 16/2020 MME (Cancelado no Julgamento*)		D PROPOSTA 1 (EVOLUTIA)		E PROPOSTA 2 (OMTX)		Valor Médio de Referênci	
					Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses)	Vlr. Unit.	Vlr. Total (12 meses
1	1	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Microsoft Active Directory (por 12 meses)	Licença	2.407			120,00	288.840,00	507,00	1.220.349,00	209,00	503.063,00	217,69	523.979,83	182,23	438.6
	2	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Windows File Server (por 12 meses)	Licença	2.407			120,00	288.840,00	400,00	962.800,00	201,90	485.973,30	205,28	494.108,96	175,73	422.9
	3	Subscriçao do módulo Varonis DatAdvantage para Microsoft Exchange (por 12 meses)	Subscrição	2.407				-		-	405,90	977.001,30	490,82	1.181.403,74	448,36	1.079.2
	4	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAlert (por 12 meses)	Licença	2.407					508,00	1.222.756,00	199,90	481.159,30	201,99	486.189,93	200,95	483.6
	5	Serviço Técnico Especializado (por 12 meses)	Horas	600	253,77	152.262,00	160,34	96.204,00		-	380,90	228.540,00	255,00	153.000,00	262,50	157.5

Algumas contratações identificadas na pesquisa não foram considerados na tabela acima, tendo em vista não possuírem similaridade com o objeto.

Requisito	**Solução**	**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		
A Solução está disponível no Portal do Software Público Brasileiro?	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público?	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 1			X

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 2			X
	Solução 3			X
A Solução é aderente às regulamentações da ICP-Brasil?	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?	Solução 1			X
	Solução 2			X
	Solução 3			X
Há necessidade de adequação do ambiente do órgão ou entidade?	Solução 1		X	
	Solução 2		X	
	Solução 3	X		

10. Registro de soluções consideradas inviáveis

Após o levantamento das possíveis soluções, a equipe de planejamento da contratação conclui que as soluções A e C, se mostram inviáveis.

Dessa forma, com base no § 1º do art. 11 da IN 01/2019 da SGD/ME, as soluções identificadas e consideradas inviáveis deverão ser registradas no Estudo Técnico Preliminar da Contratação (breve descrição e justificativa), dispensando-se a realização dos respectivos cálculos de custo total de propriedade.

11. Análise comparativa de custos (TCO)

A análise comparativa de custos totais de propriedade, baseou-se em contratações similares no âmbito da Administração Pública, bem como em pesquisa ao mercado fornecedor da solução.

Itens	Ano 1	Ano 2	Ano 3	Custo Total (3 anos)
1	***438.627,61***	466.085,70	495.262,66	1.399.975,97
2	***422.974,09***	449.452,26	477.587,98	1.350.014,33
3	***1.079.202,52***	1.146.760,60	1.218.547,81	3.444.510,93
4	***483.674,62***	513.952,65	546.126,08	1.543.753,34
5	***157.501,50***	167.361,09	177.837,90	502.700,49
TCO TOTAL				**8.240.955,06**

O custo total considerou o ICTI índice jun/2022, no percentual de 6,26% - Fonte: https://www.ipea.gov.br/cartadeconjuntura/index.php/2022/08/indice-de-custo-da-tecnologia-da-informacao-icti-junho-de-2022/.

12. Descrição da solução de TIC a ser contratada

O detalhamento técnico da solução encontra-se descrito no APÊNDICE “A”, deste Estudo Técnico (SEI nº 13172690).

13. Estimativa de custo total da contratação

Valor (R$): 2.581.980,33

O custo total da contratação resta estimado em **R$ 2.581.980,33** (dois milhões, quinhentos e oitenta e um mil novecentos e oitenta reais e trinta e três centavos).

14. Justificativa técnica da escolha da solução

O modelo de contratação baseado na manutenção da solução atual com a renovação de garantia técnica das licenças perpétua do módulo Varonis para atender o ambiente local (*on-premise*) e a proposta de expansão da solução com a aquisição de subscrição para atender os serviços migrados para o ambiente de nuvem, na forma especificada na tabela do Item 7, deste Estudo Técnico, justificam a escolha da solução com os requisitos técnicos específicos de cada tipo de licenciamento.

15. Justificativa econômica da escolha da solução

A solução de manutenção de renovação de garantia técnica das licenças perpétua do módulo Varonis já adquiridas pela ANTT com a expansão da solução com a aquisição de subscrição para atender os serviços migrados para o ambiente de nuvem, além de preservar os investimentos já realizados não exige integrações e nem envolve custos adicionais.

16. Justificativa para o parcelamento ou não

Os itens do objeto deverão ser licitados e adjudicados por grupo, considerando a indivisibilidade dos mesmos, pois a soluções e os serviços são de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia.

O agrupamento de itens irá garantir a qualidade técnica da solução não prejudicando a competividade do certame, já que há várias empresas no mercado de fornecimento da solução na forma agrupada.

17. Benefícios a serem alcançados com a contratação

Dentre os principais resultados a serem alcançados com a contratação, pode-se destacar:

a) Manutenção e atualização da solução de auditoria e gerenciamento de serviços;

b) Aderência às normas de segurança;

c) Aumento da produtividade e da Segurança da informação;

d) Maior controle das informações compartilhadas na Agência;

e) Aumentar a proteção dos dados contra alterações, exclusões e atividades não autorizadas, com consequente diminuição de tempo de resposta a falhas, paralisações e desastres;

f) Reduzir os riscos e vulnerabilidades existentes;

g) Garantir a disponibilidade, confidencialidade e integridade das informações.

18. Providências a serem Adotadas

A CONTRATADA deve elaborar um documento de planejamento de instalação e implantação para aprovação da ANTT, antes da execução da instalação.

19. Declaração de Viabilidade

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

19.1. Justificativa da Viabilidade

Com base nas informações levantadas ao longo do estudo técnico preliminar, os integrantes requisitante e técnico, da equipe de planejamento, declaram que a contratação da Solução B - Manutenção e expansão da Solução Atual, se mostra a mais viável, considerando os aspectos técnicos e econômicos da solução, pois visa manter e expandir a solução atual com o aproveitamento do licenciamento proprietário dos investimentos já realizados, que apesar de não ser considerado por si só uma justificativa para a manutenção, não dever ser desprezada na análise e na escolha das soluções.

Dessa forma, a Solução B - Manutenção e expansão da Solução Atual é a opção que se apresenta mais vantajosa, do ponto de vista técnico e econômico, sendo relevante e essencial para a manutenção e desenvolvimento das atividades que garanta e amplie ações que fortaleçam a segurança das infraestruturas críticas da informação, controle e gerência de permissionamento dos serviços de AD (*Active Directory*), de servidor de Arquivos (*File Server*), de sistema de correio eletrônico (*Exchange*), como forma de centralizar e armazenar em banco de dados informações que permitam a rastreabilidade de quaisquer alterações (criação, modificação e exclusão) realizadas em objetos (contas de usuário, computadores, unidades organizacionais, objetos de diretivas de grupo e grupo dos serviços de tecnologia da ANTT).

O presente estudo técnico preliminar foi elaborado em harmonia com a Instrução Normativa SGD/ME n^{o} 1/2019 e Instrução Normativa SEGES/ME nº 40/2020, da Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, bem como em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da contratação.

20. Responsáveis

O presente estudo técnico preliminar foi elaborado em harmonia com a Instrução Normativa SGD/ME no 1/2019 e Instrução

Normativa SEGES/ME nº 40/2020.

VICTOR HUGO GOUVEIA DE LUCENA LIMA

Gerente de Infraestrutura Tecnológica

O presente estudo técnico preliminar foi elaborado em harmonia com a Instrução Normativa SGD/ME no 1/2019 e Instrução Normativa SEGES/ME nº 40/2020,

JOÃO PROCÓPIO DO REGO NETO

Integrante Requisitante

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - APÊNDICE A_Requisitos Mínimos da Solução_vProcuradoria.pdf (157.5 KB)

Anexo I - APÊNDICE A_Requisitos Mínimos da Solução_vProcuradoria.pdf

APÊNDICE "A"

REQUISITOS MÍNIMOS DA SOLUÇÃO

1. DESCRIÇÃODOS DOS REQUISITOS MÍNIMOS DA SOLUÇÃO

1.1. OBJETO

1.1.1. Contratação de solução de auditoria, monitoramento e gerenciamento de serviços de acessos do ambiente Microsoft da ANTT, incluindo serviços técnicos especializados, com garantia de 12 (doze) meses, conforme tabela abaixo:

Lote	Item	Descrição	Métrica	Quantidade
1	1	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Microsoft Active Directory (por 12 meses)	Licença	2.407
	2	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Windows File Server (por 12 meses)	Licença	2.407
	3	Subscriçao do módulo Varonis DatAdvantage para Microsoft Exchange (por 12 meses)	Subscrição	2.407
	4	Renovação da garantia técnica da licença perpétua do módulo Varonis DatAlert (por 12 meses)	Licença	2.407
	5	Serviço Técnico Especializado (por 12 meses)	Horas	600

1.2. DETALHAMENTO DO OBJETO

1.2.1.ITEM 1 - Renovação da garantia técnica da solução de controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory)

1.2.1.1. A solução deve oferecer a visibilidade gráfica da estrutura hierárquica de todos os domínios, OUs e objetos monitorados no AD do órgão apresentados na mesma console em que apresenta seus logs de auditoria;

1.2.1.2. A solução deve suportar a demonstração gráfica e a auditoria de diferentes domínios;

1.2.1.3. A solução deverá ser capaz de rastrear quem fez alterações nos usuários, grupos, OUs e GPOs dos domínios monitorados do Active Directory, qual foi a alteração feita, quando foi feita, a máquina de origem da alteração e detalhes das propriedades tanto do objeto afetado quanto do objeto que gerou o evento;

1.2.1.4. A solução deverá indicar graficamente usuários ativos e inativos, usuários habilitados e desabilitados no AD;

1.2.1.5. A solução deve suportar a auditoria dos eventos do Directory Service, tais como: Criação de deleção de todos os objetos; Alteração de membros de grupos; Alteração nas propriedades do objeto do Directory Service; Access requests; Autenticação de conta; Reset de senhas; Lock/unlock de conta; Criação e deleção de conta; Habilitação e desabilitação de conta; Eventos de permissão adicionada ou removida de objeto do Directory Service; Proprietário alterado; Modificação de configuração de GPOs; Criação de link de GPO; Deleção de link de GPO; Modificação de link de GPO;

1.2.1.6. A solução ofertada deverá suportar o gerenciamento do AD permitindo aos administradores da solução as seguintes funcionalidades: Criação de novos usuários; Criação de novos grupos; Alteração de parâmetros de usuários já existentes; Alteração de membros de grupos de segurança; Deleção de usuários; Deleção de computadores; Reset de senhas; bloqueio e desbloqueio de usuários; habilitação e desabilitação de usuários;

1.2.1.7. Deve ser possível realizar as ações abaixo de uma só vez através da seleção de múltiplos usuários: Deleção; Reset de senha; Desbloqueio da conta; Habilitação e desabilitação;

1.2.1.8. A solução deve efetuar as funcionalidades de permissionamento, Log, Relatórios, Análise Comportamental e Alerta dos servidores de diretórios de usuários Microsoft Active Directory, e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;

1.2.1.9. A solução deve possuir visibilidade da hierarquia do serviço de Diretórios através de interface gráfica e em formato de relatório;

1.2.1.10. A solução deve possuir a visibilidade de todos os domínios, Unidades Organizacionais, Computadores, Grupos e outros objetos de domínio através de uma única interface gráfica e também em formato de relatório;

1.2.1.11. A solução deve suportar, numa única instalação, a auditoria de diferentes domínios;

1.2.1.12. A solução deve ter trilha de auditoria classificável e pesquisável de todas as atividades do Active Directory em uma única interface gráfica e também em formato de relatório;

1.2.1.13. A solução deverá ser capaz rastrear quem fez alterações no Active Directory, qual foi a alteração feita e quando nesta mesma interface gráfica e em formato de relatório;

1.2.1.14. A solução deverá indicar de forma automática recomendações sobre grupos de segurança não utilizados e membros de grupos que não mais se comportam como os outros membros daquele grupo de segurança em sua interface gráfica e em forma de relatório; e

1.2.1.15. A solução deverá realizar a modelagem de permissionamento através de simulações de mudança para grupos e ACLs sem afetar o ambiente de produção, e identificando quais membros que efetivamente acessam os dados serão afetados, permitindo a visibilidade anterior à realização das alterações no permissionamento de qual o impacto real no ambiente de produção.

1.2.2.<u>ITEM 2</u> - Renovação da garantia técnica da solução de controle e gerência de permissionamento dos serviços de servidores de Arquivos (Microsoft File Server)

1.2.2.1. A solução deve suportar como servidores de arquivos versões Windows Server 2012, Windows Server 2016 ou versão superior, Windows 7, Windows 10 ou versão superior e Netapp e Dell/EMC NAS;

1.2.2.2. A ANTT possui storage Netapp FAS e/ou Dell/EMC integrado (SAN e NAS), portanto a solução a ser fornecida deverá possuir compatibilidade comprovada no site do fabricante do storage, de modo a proteger o investimento previamente feito e possuir total compatibilidade com o ambiente atualmente instalado;

1.2.2.3. A solução deve conter todos os componentes passivos adicionais que se fizerem necessários para efetivar as interligações dos ativos do objeto da contratação;

1.2.2.4. A solução deve oferecer, a partir da console, as funcionalidades de visibilidade e alteração de permissionamento das pastas dos repositórios monitorados além de prever a possibilidade de criação de pastas e permissões para que a gestão do repositório seja centralizada;

1.2.2.5. A solução deve fornecer funcionalidade de ajuste aos diretórios com herança quebrada de permissões;

1.2.2.6. A solução deve oferecer as funcionalidades de permissionamento, Log, Relatórios, Análise Comportamental e Alerta descrita nos itens acima em plataformas de servidores de arquivos Windows;

1.2.2.7. A solução deve suportar como servidores de arquivos as versões Windows Server 2008, Windows Server 2012 e Windows 10 x64;

1.2.2.8. Deverá suportar as tecnologias DAS, SAN, Windows-Powered NAS e suporte à tecnologia de cluster da Microsoft;

1.2.2.9. Todos os componentes passivos adicionais que se fizerem necessários para efetivar as interligações dos ativos do objeto da contratação;

1.2.2.10. Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução fornecida deverá ser de um único fabricante em que seus módulos e ou programas sejam totalmente integrados e disponibilizados em uma única console de gerência;

1.2.2.11. O módulo (esquema) de segurança da solução (software) não deverá implicar em aquisição de componentes (hardware e software) adicionais;

1.2.2.12. Deverá ser compatível e permitir a utilização da tecnologia “hyperthreading” sem custos adicionais;

1.2.2.13. A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention);

1.2.2.14. A solução deve oferecer, a partir da console, as funcionalidades de visibilidade e alteração de permissionamento das pastas dos repositórios

monitorados além de prever a possibilidade de criação de pastas e permissões para que a gestão do repositório seja centralizada; e

1.2.2.15. A solução deve fornecer funcionalidade de ajuste aos diretórios com herança quebrada de permissões.

1.2.3.<u>ITEM 3</u> - Aquisição de Subscrição do Módulo varonis DatAdvantage para Microsoft Exchange

1.2.3.1. A solução deverá possuir as funcionalidades de visibilidade de permissionamento, log, relatórios, análise comportamental e alertas no Microsoft Exchange e deverão estar integradas na mesma plataforma e interface de monitoramento dos demais repositórios de dados;

1.2.3.2. 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;

1.2.3.3. O licenciamento deverá ser feito para as contas do Exchange on premise ou Exchange on line.

1.2.3.4. A solução deverá demonstrar graficamente diferença entre as caixas postais do Exchange OnLine e do Exchange on premise;

1.2.3.5. A solução ofertada deverá coletar os seguintes eventos de auditoria do Exchange online: Logon; Pasta aberta; Pasta criada; Pasta deletada; Pasta renomeada; Permissão adicionada a pasta; Permissão removida de pasta; Permissões de pasta alteradas; Pasta movida; Mensagem criada; Mensagem apagada; Mensagem editada; Mensagem movida; Mensagem copiada; Mensagem enviada em nome de (On behalf of); Mensagem enviada como (send as);

1.2.3.6. A solução deverá suportar a auditoria dos seguintes comandos PowerShell no Exchange: Add-MailboxPermission; Remove-MailboxPermission; Add-MailboxFolderPermission; Remove-MailboxFolderPermission; Set-MailboxFolderPermission; Add-ADPermission; Remove-ADPermission;

1.2.3.7. A solução ofertada deverá coletar os eventos dos servidores de email monitorados contemplando no mínimo os itens: Pasta aberta; Pasta criada; Pasta apagada; Pasta renomeada; Permissão adicionada a pasta;

Permissão removida de pasta; Pasta movida; Pasta esvaziada; Pasta copiada; Marcar todas com lida; Mensagem aberta; Mensagem enviada; Mensagem enviada “em nome de” (on behalf of); Mensagem enviada “como” (“As”); Mensagem recebida; Mensagem editada; Mensagem apagada; Mensagem copiada; Mensagem movida; Mensagem criada; Mensagem marcada não lida; Mensagem marcada como lida; Logon; Permissões adicionadas a mailbox; Permissões removidas de mailbox;

1.2.3.8. A solução deverá auditar, registrar eventos (log) e aplicar as análises comportamentais das caixas postais e pastas públicas compartilhadas do Microsoft Exchange Server para eventos gerados a partir de dispositivos móveis e/ou acessos externos (via internet) por meio de acesso WEB através dos seguintes protocolos de comunicação POP3, IMAP4, MAPI, OWA, EWS, ActiveSync - para smartphones e outros dispositivos similares.

1.2.3.9. Roteiro de Testes de Conformidade

1.2.3.10. A solução deve efetuar as funcionalidades de visibilidade de permissionamento, log, relatórios, análise comportamental e alertas no Microsoft Exchange e deverão estar integradas na mesma plataforma e interface de monitoração dos demais repositórios de dados;

1.2.3.11. A ferramenta 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.

1.2.4.<u>ITEM 4</u> - Renovação da garantia técnica da solução de análise de comportamento e alarme em tempo real (DatAlert)

1.2.4.1. A solução deve identificar, de forma automática, usuários com acesso a pastas e\ou arquivos indevidos sugerindo a revogação de acesso;

1.2.4.2. A solução deverá fornecer em modo gráfico recomendações sobre permissionamento excessivo, baseado na análise de atividade de acesso;

1.2.4.3. Fornecer identificação gráfica de atividades de acesso anormais;

1.2.4.4. A solução deve fornecer funcionalidade para ajuste dos excessos de permissionamento e aplicação das recomendações de revogação de acesso através de modelagem de permissionamento, quando é possível prever os impactos que as alterações causarão nas permissões dos usuários e grupos;

1.2.4.5. A solução deve realizar a descoberta automática de contas privilegiadas como usuários administrativos, contas de teste e de serviço;

1.2.4.6. Estas recomendações deverão também ser fornecidas em forma de relatório;

1.2.4.7. Baseada nos dados de auditoria, a solução deve ser capaz de aprender o comportamento padrão e dos recursos monitorados, para que desvios e anormalidades nesses comportamentos sejam identificados automaticamente e alertados em tempo real;

1.2.4.8. A solução deve 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;

1.2.4.9. O módulo deve permitir que sejam configurados alertas em tempo real para quaisquer eventos da auditoria habilitada;

1.2.4.10. Nos alertas em tempo real, deve ser possível configurar para que um usuário, uma pasta, um período ou uma ação específica seja alertada caso ocorra ação que os envolva; e

1.2.4.11. Os alertas poderão ser iniciados com base nos dados da auditoria, tais como usuário, ação, data e hora, ação realizada ou tentativa frustrada.

1.2.5.<u>ITEM 5</u> - Serviço Técnico Especializado

1.2.5.1. As horas do serviço técnico especializado serão utilizadas sob demanda, a critério da ANTT para realização da manutenção preventiva e corretiva e das atividades relacionadas à solução de segurança.

1.2.5.2. O serviço técnico especializado inclui no mínimo as seguintes atividades:

1.2.5.3. Execução de atividades operacionais, utilizando os procedimentos mais adequados e adaptados à realidade do ambiente da ANTT;

1.2.5.4. Execução de atividades de manutenção corretiva, utilizando os procedimentos que permitam maior eficiência e eficácia na solução de falhas;

1.2.5.5. Execução de atividades de manutenção preventiva, rotinas de testes, análises e medidas, utilizando procedimentos que assegurem uma mínima interferência na operação e máxima disponibilidade da solução;

1.2.5.6. Elaboração de procedimentos especiais ou detalhamento de procedimentos padrões, documentados e adaptados à realidade do ambiente da ANTT;

1.2.5.7. Elaboração de relatórios de atividades, detalhando os procedimentos realizados e eventuais ajustes, se necessário.

1.2.5.8. Procedimentos em conjunto com o fabricante da solução, para situações em que o ambiente da ANTT esteja sob ataque, destinado a prover o conhecimento para as medidas necessárias à defesa do ambiente;

1.2.5.9. Procedimentos de ajustes para manter a solução adquirida pela ANTT provendo a melhor utilização de suas funcionalidades;

1.2.5.10. Reuniões técnicas, mensais ou a critério da ANTT, para planejamento e execução de serviços com vistas à melhoria do ambiente instalado;

1.2.5.11. Reuniões gerenciais, mensais ou a critério da ANTT, para avaliação e acompanhamento dos serviços oferecidos; e

1.2.5.12. Entrega de relatórios ao final do período de serviço de apoio solicitado, contendo informações sobre atividades desenvolvidas e recomendações sobre como melhor utilizar a tecnologia.

1.2.5.13. A tabela abaixo demonstra, de forma estruturada, os itens de serviço técnico especializado, que inclui no mínimo as seguintes atividades:

ITEM	ATIVIDADES	UNIDADE	CONSUMO ESTIMADO (Horas)
1	Estruturação hierárquica dos diretórios do servidor de arquivos	Pasta	2
2	Definição de proprietários das pastas utilizando informações estatísticas providas pela solução	Pasta	2
3	Remediação de pastas com permissões a grupos globais	Pasta	20
4	Remediação de pastas com permissões inconsistentes	Pasta	75
5	Remediação de dados parados	Pasta	12
6	Remediação das senhas que nunca expiram dos usuários do domínio	Usuário	5

7	Remediação dos grupos de segurança em loop no domínio	Grupo	10
8	Remediação das pastas com permissões únicas	Pasta	8
9	Reestruturação das pastas protegidas da herança	Pasta	5
10	Remediação das SID não resolvido da ACL das pastas	Pasta	2
11	Remediação das permissões dos grupos de segurança vazios	Pasta	2
12	Remediação das permissões diretas de usuários	Pasta	2
13	Remediação dos usuários habilitados com senhas expiradas	Usuário	4
14	Configuração do compartilhamento no Portal de Permissionamento	Pasta	20
15	Investigação forense	Relatório	120
16	Análise, investigação e diagnóstico de ocorrências	Relatório	120
17	Remediação de usuários habilitados sem uso	Usuário	2
18	Remediação de pastas protegidas	Pasta	10
19	Configuração de pastas que serão gerenciadas pelo DataPrivilege	Pasta	15
20	Configuração de proprietários para as pastas gerenciadas (DP)	Pasta	15
21	Configuração de proprietários para grupos de segurança (DP)	Grupo	5
22	Configuração de barreiras éticas para fluxos de aprovação	Pasta	25
23	Revisão de permissionamento de usuários	Usuário	18
24	Configuração e execução de transporte de dados	Pasta	10
25	Data Risk Assessment – Relatório de análise de risco	Relatório	240
26	Plano de aplicação de melhores práticas	Relatório	120
27	Mapa de vulnerabilidade do ambiente	Relatório	360

28	Extração de relatórios	Relatório	45

---------- FIM DO APÊNDICE “A” ----------