Solução Integrada de Proteção e Resposta a Incidentes de Segurança.

Termo de Referência

SUMÁRIO

1. SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO 3
2. CONSIDERAÇÕES GERAIS SOBRE A SOLUÇÃO DE TI. 12
3. CARACTERÍSTICAS TÉCNICAS MÍNIMAS EXIGIDAS 13
4. DESCRIÇÃO DAS FUNCIONALIDADES 47
5. GARANTIA 110
6. RESPONSABILIDADES E DEVERES DO CONTRATANTE E DO CONTRATADO 110
7. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR 112
8. NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS. 116
9. DIRETRIZES PARA PLANO DE IMPLANTAÇÃO 122
10. TRANSIÇÃO CONTRATUAL 124
11. TERMOS CONTRATUAIS 126
12. HISTÓRICO DE ATUALIZAÇÃO DE VERSÕES. 137
13. ASSINATURAS 138
14. ANEXO I-A – TERMO ENCERRAMENTO DO CONTRATO 141
15. ANEXO I-B– MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO. 142
16. ANEXO I-C – MODELO DE TERMO DE RECEBIMENTO DEFINITIVO. 143
17. ANEXO I-D – MODELO DE APRESENTAÇÃO DA PROPOSTA DE PREÇOS. 144
18. ANEXO I-E – MODELO DE ABERTURA DE CHAMADO. 146
19. ANEXO I-F – MODELO DE DECLARAÇÃO DE PLENO CONHECIMENTO E ATENDIMENTO ÀS EXIGÊNCIAS DE HABILITAÇÃO 147
20. ANEXO I-G – MODELO DE TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO 148
21. ANEXO I-H – MODELO DE FICHA DE AVALIAÇÃO 152

1. SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

1.1. **OBJETO DA CONTRATAÇÃO**

1.1.1. Registro de Preços para Aquisição de Solução Integrada de Proteção e Resposta a Incidentes de Segurança, baseada em hardware e software, para prover proteção e capacidade de resposta a incidentes, incluindo instalação, implantação/configuração, suporte técnico e operação assistida, para atender as necessidades corporativas do Ministério da Ciência, Tecnologia e Inovação – MCTI.

1.1.1.1. Devido à natureza organizacional do MCTI e necessidade de integração tecnológica entre as várias casas a ele vinculadas (INPE, CNPq, IBICT, FINEP, CEMADEN, RNP), visando principalmente à otimização dos recursos tecnológicos e públicos, esta contratação será realizada de forma modularizada e flexível, por meio de Ata de Registro de Preços, para que cada casa tenha a liberdade para aderir, ou não, aquilo que melhor se aplicar à sua necessidade, com respaldo no artigo 3º, III, do Decreto nº 7.892/2013.

1.2. **NATUREZA DO OBJETO E PREVISÃO NO PDTI.**

1.2.1. Constitui **serviço continuado**, pois existe a necessidade de pleno funcionamento da solução visto a essencialidade dos serviços e atividades a serem executadas pelo CONTRATANTE. Caracteriza-se, também, como **comum**, pois os padrões de desempenho e de qualidade podem ser objetivamente definidos com base em **especificações usuais no mercado**, conforme Acórdão nº 2.471/2008-TCU-Plenário. Assim sugere-se a adoção da modalidade **pregão**.

> *"Consideram-se bens e serviços comuns aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos no edital, por meio de especificações usuais praticadas no mercado. Bens e serviços comuns são ofertados, em princípio, por muitos fornecedores e comparáveis entre si com facilidade."*

1.2.2. Esse instrumento guarda observância à lei de licitações para contratação de serviços na administração pública e ao Plano Diretor de Tecnologia da Informação do MCTI (**Necessidades e Ações respectivamente: N13** - Modernização e ampliação dos serviços de rede, web e informação da Administração Central do MCTI e Unidades Descentralizadas, visando atender às crescentes demandas do órgão e **N14** - Manutenção e ampliação da

capacidade de conectividade da rede local da Administração Central do MCTI e Unidades Descentralizadas, visando suprir as demandas recebidas, bem como aumentar sua eficiência, confiabilidade e segurança; **N13A5** - Ampliar e atualizar as ferramentas que suportam a segurança da informação e **N14A2** - Ampliar o número de segmentos monitorados da rede contra intrusões).

1.2.3. Cabe salientar que a referida análise e elaboração desse instrumento não afasta a apreciação da Consultoria Jurídica do MCTI.

1.3. **FUNDAMENTAÇÃO DA CONTRATAÇÃO**

1.3.1. Para combater as ameaças modernas, é preciso ir além das ferramentas tradicionais de segurança. Assim o objetivo é prover o MCTI de uma solução integrada de defesa cibernética e resposta a incidentes de segurança, construindo a infraestrutura necessária para o combate às ameaças digitais. Abrangendo a segurança das fronteiras, servidor de aplicações, segurança web e proteção contra *malware*.

1.3.2. À medida que o uso de informações e sistemas crescem não há como deixar de se abordar o item segurança que, em se tratando de empresas particulares e/ou órgãos públicos, deixa de ser um ponto apenas importante para se tornar vital. Informações sigilosas roubadas, websites destruídos, informações apagadas de um banco de dados, entre outras ações, costumam resultar em prejuízos financeiros e morais que muitas vezes não podem ser reparados.

1.3.3. O Ministério da Ciência e Tecnologia - MCTI conta hoje com uma solução de firewall frágil e desatualizada, que compromete não só a segurança como também a velocidade e disponibilidade dos dados da rede.

1.3.4. Não existe no ambiente solução que permita visibilidade do ambiente de rede, com apoio ao processo de resposta a incidentes, de forma integrada com a plataforma de proteção.

1.3.5. É necessário, portanto, a implantação de uma solução que permita a integração entre os elementos de proteção, visibilidade e resposta a incidentes, construindo uma infraestrutura coesa e eficaz de proteção e combate às ameaças digitais;

1.3.6. No que tange ao elemento de proteção, é importante observar que nos últimos anos houve uma verdadeira revolução nos meios de comunicação. Conceitos como sistemas em nuvem, técnicas de evasão, uso massivo de

criptografia e aplicações cujo tráfego independe do uso de portas específicas demandaram o uso de novas tecnologias de análise e controle de tráfego de dados. Para oferecer proteção adequada nesse contexto, é necessário partir para tecnologias de vanguarda, capazes de lidar com os desafios atuais.

1.3.7. Outro aspecto fundamental para a segurança do ambiente, e para a gestão de riscos como um todo, é a visibilidade. Com a quantidade de dados passando pela rede crescendo de forma constante, assim como a demanda por mais aplicações, sistemas e ativos, as redes corporativas tendem a se tornar algo próximo de uma "caixa preta", em que nem mesmo os administradores sabem o que se passa no ambiente. Para retomar o controle, é fundamental colocar em uso soluções que ajudem a construir uma visão mais completa do que se passa, permitindo a conquista da consciência situacional necessária para a proteção e resposta a incidentes adequadas para o ambiente.

1.4. **EXPECTATIVAS.**

1.4.1. São esperados o atendimento das seguintes expectativas com a presente contratação:

1.4.1.1. Substituição dos equipamentos obsoletos e fora do período de garantia atualmente instalados no parque computacional;

1.4.1.2. Aumento da capacidade de segurança da rede pela aquisição de novos equipamentos;

1.4.1.3. Aumento da consciência situacional e capacidade de resposta a incidentes de segurança;

1.5. **RESULTADOS.**

1.5.1.1. São esperados o atendimento das seguintes resultados com a presente contratação:

1.5.1.1.1. Assegurar a sustentabilidade e desempenho dos serviços do Ministério da Ciência, Tecnologia e Inovação;

1.5.1.1.2. Manter alta disponibilidade dos serviços;

1.5.1.1.3. Substituição dos equipamentos obsoletos, de alto custo, de baixo desempenho ou sem contrato de manutenção preventiva e/ou corretiva, por equipamentos mais modernos;

1.5.1.1.4. Garantir a segurança, integridade e disponibilidade das informações.

1.5.1.1.5. Proteção da rede e dos sistemas.

1.5.1.1.6. Ação imediata para interromper ou minimizar o incidente.

1.5.1.1.7. Investigação do Incidente.

1.5.1.1.8. Restauração dos recursos afetados.

1.5.1.1.9. Reportando o incidente aos canais apropriados.

1.5.1.1.10. Respostas rápidas e minimização dos danos em caso de incidentes.

1.5.1.1.11. Otimização do processo de conscientização de segurança e disseminação de boas práticas.

1.5.1.1.12. Implementações de Segurança proativas e decorrente de lições aprendidas em incidentes passados.

1.5.1.1.13. Facilitação da implementação e controle da política de segurança.

1.6. **MODELO DA CONTRATAÇÃO.**

1.6.1. A partir da análise dos modelos de contratação disponíveis e levando em consideração a evolução tecnológica, o MCTI adquirirá Solução Integrada de Proteção e Resposta a Incidentes de Segurança e serviços por meio de empresa que se responsabilize em fornecer os bens e serviços objetos deste instrumento, pois o MCTI ganhará na economia de escala ao realizar uma aquisição de maior vulto. Ademais, poderá barganhar por meio do pregão eletrônico a melhor proposta, ou seja, a de menor preço. Quanto ao serviço de operação assistida será adotado o modelo Unidades de Serviço Técnico, com uso sob demanda.

1.6.1.1. Cabe salientar que a compra pelo menor preço não significa a aquisição de produtos com baixa qualidade, visto que a administração deverá definir especificações técnicas necessárias para o sucesso do certame, sem restringir a competição.

1.7. **PROJETOS SIMILARES**

1.7.1. Após análise das necessidades institucionais e a busca de uma Solução de TI que supra as necessidades de TI levantadas; o responsável pela área requisitante, o integrante requisitante e o integrante técnico responsável pelas especificações da Solução de TI encontraram projetos com especificações similares em outros Órgãos da Administração Pública, como, por exemplo, na GAP Aeronáutica, TCU, CNJ.

O integrante técnico 2, responsável pelos requisitos técnicos, após análise de várias opções no mercado relacionadas a essa aquisição, optou pelas especificações, serviços e quantitativos descritos neste instrumento. Dessa forma, ele levou em consideração o melhor custo x benefício, como também o atendimento das necessidades relacionadas pelo integrante requisitante e a área requisitante. Nessa perspectiva, a escolha dessa solução é fruto de um consenso entre o integrante técnico e requisitante com anuência da área requisitante mencionados anteriormente.

1.8. **ESTIMATIVA DE DEMANDA.**

1.8.1. A licitação por grupo único é mais satisfatória do ponto de vista da eficiência técnica, por manter a qualidade do fornecimento, haja vista que o gerenciamento permanece todo o tempo a um mesmo administrador, além de garantir a compatibilidade dos ativos, fato importante quando se mantém diversos serviços e softwares trafegando na rede, a maior interação entre as diferentes fases do fornecimento, a maior facilidade no cumprimento do cronograma e na observância dos prazos, concentração da responsabilidade pela execução do fornecimento em uma só pessoa e concentração da garantia dos resultados.

1.8.2. Ademais, haverá um grande ganho para a Administração na economia de escala, que aplicada na execução de determinado fornecimento, implicaria em aumento de quantitativos e, consequentemente, numa redução de preços a serem pagos pela Administração

1.8.3. Devido às características de integração e interdependência entre os elementos da solução, à complexidade para ativação da mesma à infraestrutura de rede já existente, visando garantir a eficiência técnica e qualidade da solução como um todo, levando em consideração a unidade e integridade do objeto a ser executado e respeitando os interesses da administração em reduzir custos administrativos e de gestão, estima-se a demanda em:

Tabela 1 - Demandas e Quantitativos

	ITEM	DESCRIÇÃO	QUANTITATIVOS INDIVIDUAIS MCTI - UASG 240101 BRASÍLIA – DF	QUANTITATIVOS TOTAIS PARA REGISTRO
LOTE ÚNICO	1	**Módulo de Proteção de Rede**	1	**1**
	2	Garantia e Manutenção Mensal - Módulo de Proteção de Rede	36	**36**
	3	Serviço de Implantação - Módulo de Proteção de Rede	1	**1**
	4	Serviço de Treinamento - Módulo de Proteção de Rede	1	**1**
	5	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	36	**36**
	6	**Módulo de Análise de Rede**	1	**1**
	7	Garantia e Manutenção Mensal - Módulo de Análise de Rede	36	**36**
	8	Serviço de Implantação - Módulo de Análise de Rede.	1	**1**
	9	Serviço de Treinamento - Módulo de Proteção de Rede	1	**1**
	10	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	36	**36**
	11	**Módulo de Visibilidade e Análise de Dados**	1	**1**
	12	Garantia e Manutenção Mensal - Módulo de Visibilidade e Análise de Dados	36	**36**
	13	Serviço de Implantação - Módulo de Visibilidade e Análise de Dados	1	**1**
	14	Serviço de Treinamento - Módulo de Visibilidade e Análise de Dados	1	**1**
	15	Serviço de Suporte Técnico Mensal - Módulo de Visibilidade e Análise de Dados	36	**36**
	16	**Serviços de Operação Assistida (UST)**	2000	**2000**

1.9. **VALORES MÁXIMOS**

1.9.1. Para a apuração do valor máximo estimado, foram considerados os valores médios praticados no mercado ou recentes contratações da Administração Pública, conforme tabela abaixo:

Tabela 2 - Estimativa de Preço

	Item	DESCRIÇÃO	QNT	VALOR UNITÁRIO					VALOR MÉDIO UNITÁRIO (R$)	VALOR TOTAL ESTIMADO (R$)
				EMPRESA 1 (RS)	EMPRESA 2 (RS)	EMPRESA 3 (RS)	EMPRESA 4 (RS)	EMPRESA 5 (RS)		
LOTE ÚNICO	1	**Módulo de Proteção de Rede**	**1**	R$ 1.117.716,08	R$ 1.237.000,00	R$ 1.350.000,00	R$ 1.532.000,00	R$ 1.400.000,00	R$ 1.327.343,22	R$ 1.327.343,22
	2	Garantia e Manutenção Mensal - Módulo de Proteção de Rede	**36**	R$ 8.098,41	R$ 8.590,28	R$ 10.000,00	R$ 13.500,00	R$ 12.000,00	R$ 10.437,74	R$ 375.758,57
	3	Serviço de Implantação - Módulo de Proteção de Rede	**1**	R$ 15.000,00	R$ 17.000,00	R$ 25.000,00	R$ 20.000,00	R$ 18.000,00	R$ 19.000,00	R$ 19.000,00
	4	Serviço de Treinamento - Módulo de Proteção de Rede	**1**	R$ 27.000,00	R$ 23.000,00	R$ 30.000,00	R$ 30.000,00	R$ 35.000,00	R$ 29.000,00	R$ 29.000,00
	5	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	**36**	R$ 3.000,00	R$ 3.700,00	R$ 10.000,00	R$ 4.000,00	R$ 4.500,00	R$ 5.040,00	R$ 181.440,00
	6	**Módulo de Análise de Rede**	**1**	R$ 253.377,40	R$ 650.000,00	R$ 1.100.000,00	R$ 500.320,00	R$ 450.000,00	R$ 590.739,48	R$ 590.739,48
	7	Garantia e Manutenção Mensal - Módulo de Análise de Rede	**36**	R$ 4.115,97	R$ 4.513,89	R$ 11.167,00	R$ 4.500,00	R$ 8.000,00	R$ 6.459,37	R$ 232.537,39
	8	Serviço de Implantação - Módulo de Análise de Rede.	**1**	R$ 15.000,00	R$ 17.000,00	R$ 15.000,00	R$ 20.000,00	R$ 20.500,00	R$ 17.500,00	R$ 17.500,00
	9	Serviço de Treinamento - Módulo de Proteção de Rede	**1**	R$ 27.000,00	R$ 23.000,00	R$ 30.000,00	R$ 30.000,00	R$ 35.000,00	R$ 29.000,00	R$ 29.000,00
	10	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	**36**	R$ 3.000,00	R$ 3.700,00	R$ 3.500,00	R$ 4.732,00	R$ 4.500,00	R$ 3.886,40	R$ 139.910,40
	11	**Módulo de Visibilidade e Análise de Dados**	**1**	R$ 728.000,00	R$ 700.560,00	R$ 750.000,00	R$ 920.340,00	R$ 890.000,00	R$ 797.780,00	R$ 797.780,00

12	Garantia e Manutenção Mensal - Módulo de Visibilidade e Análise de Dados	**36**	R$ 11.300,00	R$ 13.611,11	R$ 12.500,00	R$ 7.500,00	R$ 15.700,00	R$ 12.122,22	R$ 436.399,99
13	Serviço de Implantação - Módulo de Visibilidade e Análise de Dados	**1**	R$ 71.168,83	R$ 76.500,00	R$ 80.000,00	R$ 93.000,00	R$ 100.000,00	R$ 84.133,77	R$ 84.133,77
14	Serviço de Treinamento - Módulo de Visibilidade e Análise de Dados	**1**	R$ 27.000,00	R$ 23.000,00	R$ 30.000,00	R$ 30.000,00	R$ 35.000,00	R$ 29.000,00	R$ 29.000,00
15	Serviço de Suporte Técnico Mensal - Módulo de Visibilidade e Análise de Dados	**36**	R$ 3.000,00	R$ 4.500,00	R$ 3.500,00	R$ 4.732,00	R$ 4.500,00	R$ 4.046,40	R$ 145.670,40
16	**Serviços de Operação Assistida (UST)**	**2000**	R$ 200,00	R$ 230,00	R$ 250,00	R$ 230,00	R$ 250,00	R$ 232,00	R$ 464.000,00
VALOR TOTAL ESTIMADO DA SOLUÇÃO DE TI (R$)									R$ 4.899.213,21

1.10. Assim, o valor estimado para a contratação da Solução Integrada de Proteção e Resposta a Incidentes de Segurança é de R$ 4.899.213,21 (Quatro milhões oitocentos e noventa e nove mil duzentos e treze reais e vinte e um centavos)

1.11. ESTIMATIVA DE AQUISIÇÃO IMEDIATA.

Tabela 3 - Demandas e Quantitativos (MCTI)

ITEM	DESCRIÇÃO	Preço Unitário	Custeio(CO) Capital(CA)	MCTI	
				Qtd.	Valor Total
1	**Módulo de Proteção de Rede**	R$ 1.327.343,22	CA	1	R$ 1.327.343,22
2	Garantia e Manutenção Mensal - Módulo de Proteção de Rede	R$ 10.437,74	CO	36	R$ 375.758,57
3	Serviço de Implantação - Módulo de Proteção de Rede	R$ 19.000,00	CO	1	R$ 19.000,00
4	Serviço de Treinamento - Módulo de Proteção de Rede	R$ 29.000,00	CO	1	R$ 29.000,00
5	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	R$ 5.040,00	CO	36	R$ 181.440,00
6	**Módulo de Análise de Rede**	R$ 590.739,48	CA	1	R$ 590.739,48
7	Garantia e Manutenção Mensal - Módulo de Análise de Rede	R$ 6.459,37	CO	36	R$ 232.537,39
8	Serviço de Implantação - Módulo de Análise de Rede.	R$ 17.500,00	CO	1	R$ 17.500,00
9	Serviço de Treinamento - Módulo de Proteção de Rede	R$ 29.000,00	CO	1	R$ 29.000,00
10	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	R$ 3.886,40	CO	36	R$ 139.910,40
11	**Módulo de Visibilidade e Análise de Dados**	R$ 797.780,00	CA	1	R$ 797.780,00
12	Garantia e Manutenção Mensal - Módulo de Visibilidade e Análise de Dados	R$ 12.122,22	CO	36	R$ 436.399,99
13	Serviço de Implantação - Módulo de Visibilidade e Análise de Dados	R$ 84.133,77	CO	1	R$ 84.133,77
14	Serviço de Treinamento - Módulo de Visibilidade e Análise de Dados	R$ 29.000,00	CO	1	R$ 29.000,00
15	Serviço de Suporte Técnico Mensal - Módulo de Visibilidade e Análise de Dados	R$ 4.046,40	CO	36	R$ 145.670,40
16	**Serviços de Operação Assistida (UST)**	R$ 232,00	CO	2000	R$ 464.000,00
		TOTAL			**R$ 4.899.213,21**
		CUSTEIO 3.3.90.39.57			**R$ 2.183.350,51**
		CAPITAL 4.4.90.52.35			**R$ 2.715.862,70**

1.12. UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS POR ÓRGÃO OU ENTIDADE NÃO PARTICIPANTE.

1.12.1. Desde que devidamente justificada a vantagem, a ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da administração pública federal que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador.

1.12.2. Porém, 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, conforme dita o artigo 22, parágrafo 4º do Decreto nº 7.892/2013.

2. CONSIDERAÇÕES GERAIS SOBRE A SOLUÇÃO DE TI.

2.1. A CONTRATADA, fornecedora da solução de segurança, deverá realizar os procedimentos de implantação da solução devendo observar as seguintes fases:

2.1.1. Planejamento do ambiente e validação dos parâmetros e requisitos técnicos;

2.1.1.1. Fornecer documentação completa dos procedimentos de instalação e configuração dos componentes da solução no ambiente de TI - Tecnologia de Informação - do MCTI.

2.1.1.2. Realizar os procedimentos de instalação, configuração e migração dos componentes da solução com a presença do corpo técnico do MCTI.

2.1.2. Serviços de manutenção e suporte técnico da solução, pelo prazo contratado/adquirido;

2.1.3. Serviços de Implantação e Treinamento;

2.1.4. Serviços de Operação Assistida;

2.1.4.1. Acompanhamento do ambiente em produção, após a instalação e configuração, conforme demanda por parte do CONTRATANTE;

2.1.4.2. Realização de Ajustes do Ambiente após primeiros dias de Produção para melhor utilização dos recursos da Solução;

2.1.4.3. Validação e testes do novo ambiente e realização de ajustes conforme a necessidade;

2.2. As soluções oferecidas deverão estar em linha de produção pelo fabricante e ter garantia de suporte e atualização por todo o período de vigência do contrato. Para tanto, poderão ser realizadas verificações pela área técnica do CONTRATANTE junto a sítio oficial do fabricante, onde deverá constar o ciclo de vida dos equipamentos.

3. CARACTERÍSTICAS TÉCNICAS MÍNIMAS EXIGIDAS

3.1. Deverá ser fornecida solução de segurança da informação com capacidade de proteção, visibilidade e resposta a incidentes, constituída por hardware, software e serviços, visando otimizar o processo de defesa contra ameaças digitais no ambiente de rede do MCTI.

3.2. **DESCRIÇÃO E SERVIÇOS DO MÓDULO DE PROTEÇÃO DE REDE.**

3.2.1. **MÓDULO DE PROTEÇÃO DE REDE.**

3.2.1.1. Dispositivo de sistema de segurança de informação perimetral, que inclui firewall, administração de largura de banda de serviço de internet (*QoS*) por aplicação e usuário, suporte para conexões VPN IPSec e SSL, proteção contra ameaças de vírus e malware (Antivírus e *AntiSpyware*), proteção contra ameaças avançadas e desconhecidas, controle de acesso Internet (filtro de URLs), IPS (sistema de Prevenção de Intrusão), contextos virtuais, bem como controle de transmissão de dados, bloqueio de arquivos por tipo e controle de acesso à internet.

3.2.1.2. O módulo/solução deve suportar todas as funcionalidades citadas no item anterior em um appliance, construído especificamente para a solução, com hardware e software fornecidos pelo mesmo fabricante. A solução deve possuir sistema de licenciamento modular, no sentido de permitir ativação de funcionalidades mediante apenas futura aquisição e aplicação de licença específica, sem necessidade de adição ou instalação de módulos adicionais de hardware (exceto para análise local de ameaças avançadas) e software. A solução deve ter a capacidade de suportar todos os requisitos técnicos desta especificação, e ser entregue inicialmente licenciada para, no mínimo, as seguintes funcionalidades: firewall, QoS, VPN IPSec, VPN SSL, Antivírus, AntiSpyware, IPS, de criptografia SSL, Filtro de URLs e Proteção contra ameaças avançadas/desconhecidas.

3.2.1.3. O módulo/solução deve ser fornecido em modelo de alta disponibilidade, ou seja, composto por no mínimo duas unidades físicas operando em modo “cluster” ativo-passivo ou ativo-ativo;

3.2.1.4. Requisitos de capacidade e performance:

3.2.1.4.1. O equipamento deve possuir, no mínimo:

3.2.1.4.1.1. 12 interfaces 10/100/1000 Copper Ethernet

3.2.1.4.1.2. 08 Interfaces 1GB SFP.

3.2.1.4.2. O equipamento deve possuir interface “Out-Of-Band” dedicada para gerenciamento.

3.2.1.4.3. Suportar pelo menos 05 Gbps de throughput para Firewall.

3.2.1.4.4. Suportar pelo menos 05 Gbps de throughput para controle de aplicações.

3.2.1.4.5. Suportar pelo menos 02 Gbps de throughput para controle de Antivírus e Antispyware.

3.2.1.4.6. Suportar pelo menos 02 Gbps de throughput de IPS.

3.2.1.4.7. Suportar pelo menos 02 Gbps de throughput para VPN IPSec.

3.2.1.4.8. Suportar pelo menos 02 Gbps de throughput para as funcionalidades de Firewall, Controle de Aplicações, IPS, Antivírus e Anti-Spyware habilitados simultaneamente.

3.2.1.4.9. Deve suportar pelo menos 1.000.000 de sessões concorrentes.

3.2.1.4.10. Deve suportar pelo menos 120.000 novas sessões por segundo.

3.2.1.4.11. Deve suportar pelo menos 2.000 Interfaces Túnel de VPN IPSec

3.2.1.4.12. Suportar pelo menos 5.000 Usuários concorrentes de SSL VPN.

3.2.1.4.13. Deve permitir suporte a pelo menos 10 Sistemas Virtuais.

3.2.1.5. Integração:

3.2.1.5.1. Deve possuir integração nativa com os Módulos de Análise de Rede, no sentido de permitir pivoteamento direto entre as interfaces;

3.2.1.5.1.1. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista iniciar a análise de um incidente pela interface do Módulo de Proteção, e com apenas um clique de mouse acionar a console do Módulo de Análise de Rede, mostrando dados já contextualizados com as informações de origem;

3.2.1.5.1.1.1. Um exemplo de uso dessa funcionalidade seria iniciar a análise de um incidente via console do Módulo de Proteção, identificar o endereço IP interno alvo do ataque, e realizar por meio de um clique a pesquisa no Módulo de Análise de Rede já referenciada com o IP em questão (fundamental para levantamento de impacto de eventuais incidentes de segurança).

3.2.1.5.1.2. Deve ser capaz de responder aos seguintes tipos de pergunta:

3.2.1.5.1.2.1. “Mostre tudo que esse endereço fez em minha rede interna”;

3.2.1.5.1.2.2. “Mostre agora o que essa máquina fez na minha rede após ter sido infectada”;

3.2.1.5.2. Deve possuir integração nativa com o Módulo de Visibilidade e Análise de Dados, no sentido enviar os dados de log e auditoria para armazenamento histórico e análise;

3.2.1.5.2.1. A Integração entre os módulos deve prover visibilidade em forma de gráficos, estatísticas e dashboards específicos do Módulo de Proteção no console do Módulo de Visibilidade e Análise de Dados;

3.2.1.5.2.1.1. A configuração entre os elementos deve demandar pouco esforço de configuração, no sentido de já existir o ambiente pré-configurado, bastando apenas apontar o envio de logs;

3.2.2. **GARANTIA E MANUTENÇÃO MENSAL - MÓDULO DE PROTEÇÃO DE REDE**

3.2.2.1. Serviço de garantia e manutenção do módulo/solução, cobrindo pelo prazo contratado, no mínimo, os seguintes quesitos:

3.2.2.1.1. Resolução de problemas de hardware e software do módulo;

3.2.2.1.2. Substituição de peças danificadas, ou, na impossibilidade de troca de peças, do módulo inteiro;

3.2.2.1.2.1. No evento de substituição do módulo inteiro, o novo hardware deve ser de modelo igual ou superior do que estiver sendo substituído;

3.2.2.1.3. Garantia do funcionamento das funcionalidades adquiridas da solução durante o prazo contratado;

3.2.2.1.3.1. Na existência de funcionalidades do tipo assinatura (subscription), estas devem estar necessariamente ativas durante o prazo contratado;

3.2.2.1.4. Correção de falhas de software (bugs), com fornecimento de versões atualizadas diretamente pelo fabricante da solução, durante o prazo contratado;

3.2.2.1.5. Atualização de versões de módulos de software (updates, firmware, etc.) disponibilizados pelo fabricante da solução durante o prazo contratado;

3.2.3. **SERVIÇO DE IMPLANTAÇÃO - MÓDULO DE PROTEÇÃO DE REDE.**

3.2.3.1. Serviço de implantação do módulo/solução adquirida no ambiente do CONTRATANTE, contemplando, no mínimo, as seguintes atividades:

3.2.3.2. **INSTALAÇÃO FÍSICA:**

3.2.3.2.1. Instalação dos equipamentos no local designado pelo CONTRATANTE, incluindo fixação em rack, energização e conexões de rede.

3.2.3.3. **CONFIGURAÇÃO BÁSICA:**

3.2.3.3.1. Conjunto de procedimentos de configuração com a finalidade de deixar a solução pronta para atuar em caráter operacional no ambiente de produção do CONTRATANTE, incluindo atualizações de software, endereçamento e regras iniciais.

3.2.3.3.2. Customização da configuração da solução para integração com o ambiente de rede do CONTRATANTE

3.2.3.3.3. Inclui a execução do Plano de Testes, visando verificar de forma objetiva e prática o funcionamento da solução.

3.2.3.4. **ACOMPANHAMENTO INICIAL**

3.2.3.4.1. Serviço de acompanhamento da operação inicial da solução, entre a ativação no ambiente de produção e o primeiro dia de funcionamento. Tem como objetivo prestar o apoio técnico necessário (incluindo ajustes porventura necessários) para que a migração para o ambiente de produção ocorra de forma controlada e segura.

3.2.3.5. O CONTRATANTE deve prover a infraestrutura necessária para implantação da solução em seu ambiente.

3.2.3.6. **DOCUMENTAÇÃO**

3.2.3.6.1. A Contratada deve apresentar um Plano de Implantação detalhando como a solução será instalada no ambiente do CONTRATANTE;

3.2.3.6.2. A Contratada deverá fornecer a Documentação do Projeto, detalhando como foi implantada a solução no ambiente do CONTRATANTE;

3.2.4. **SERVIÇO DE TREINAMENTO - MÓDULO DE PROTEÇÃO DE REDE.**

3.2.4.1. Serviço de treinamento da equipe técnica do CONTRATANTE visando capacitá-la na operação/administração/uso da solução, contemplando, no mínimo, os seguintes tópicos:

3.2.4.2. Apresentação do projeto/solução implementado;

3.2.4.2.1. Descrição da arquitetura física e lógica de cada elemento da solução;

3.2.4.2.2. Estratégias de implementação da solução;

3.2.4.2.3. Procedimentos de instalação da solução;

3.2.4.2.4. Operação e Administração da solução;

3.2.4.2.5. Descrição e uso das funcionalidades da solução;

3.2.4.2.6. Resolução de problemas (“troubleshooting”);

3.2.4.2.7. Procedimentos de manutenção (atualizações de software, backup/restore, instalação de módulos de hardware, etc.);

3.2.4.2.8. Elaboração de Relatórios;

3.2.4.3. A CONTRATADA deve obedecer ao prazo máximo de 15 dias úteis após assinatura do contrato para apresentação da ementa e detalhes da realização do treinamento.

3.2.4.4. A CONTRATADA deverá providenciar material didático individual que abranja todo o conteúdo do curso. Não será exigido material oficial do fabricante, entretanto este será avaliado pela equipe técnica do CONTRATANTE antes da realização do curso, e caso seja considerado insuficiente, deverá ser readaptado para as condições exigidas pelo CONTRATANTE.

3.2.4.5. O período e horário de realização do curso deverão ser definidos pela CONTRATADA, em conjunto com o CONTRATANTE, para momento posterior à implantação da solução;

3.2.4.6. A CONTRATADA deverá providenciar local e infraestrutura para o treinamento, podendo o CONTRATANTE optar por executá-lo em seu ambiente.

3.2.4.7. A CONTRATADA deve obedecer ao prazo máximo de 30 dias úteis após a implantação da solução no ambiente do CONTRATANTE para início do treinamento.

3.2.4.8. O treinamento deve ter carga horária de 16 horas.

3.2.4.9. A turma poderá ter até 08 alunos.

3.2.5. **SERVIÇO DE SUPORTE TÉCNICO MENSAL - MÓDULO DE PROTEÇÃO DE REDE.**

3.2.5.1. A CONTRATADA deve prover o serviço de Suporte Técnico para a solução adquirida pelo CONTRATANTE, pelo prazo contratual, conforme as especificações constantes neste documento;

3.2.5.2. **CHAMADOS DE SUPORTE:**

3.2.5.2.1. Os chamados de suporte técnico representam a solicitação formal de serviços de suporte à CONTRATADA e devem ser atendidos de acordo com os critérios e parâmetros estabelecidos para execução dos serviços.

3.2.5.2.2. O chamado deve conter uma descrição detalhada do problema, a indicação dos itens de configuração afetados, e o nome e telefone do contato do CONTRATANTE responsável pelo acompanhamento do serviço. O CONTRATANTE poderá ainda anexar ao chamado documentos ou imagens que auxiliem da identificação do problema, sugerir o perfil profissional adequado para a execução do serviço e, se for o caso, agendar data e hora para o atendimento.

3.2.5.3. **DISPONIBILIDADE E MODELO DE ATENDIMENTO:**

3.2.5.3.1. O atendimento será no modelo 24x7 (horário comercial, dias úteis) remoto e presencial (quando verificada a necessidade no decorrer do atendimento).

3.2.5.4. **CLASSIFICAÇÃO DE SEVERIDADE:**

3.2.5.4.1. Os chamados de suporte técnico serão classificados por severidade, dependendo do impacto que o problema a ser resolvido possa causar ao ambiente computacional do CONTRATANTE, sendo possíveis os seguintes níveis de severidade:

3.2.5.4.2. **URGENTE** – chamado para restabelecer serviço que esteja parado;

3.2.5.4.3. **ALTA** – chamado para restabelecer serviço que não esteja operando corretamente, apresente problema de desempenho ou esteja sob risco de parada;

3.2.5.4.4. **MÉDIA** – chamado para resolução de problemas que não estejam causando interrupção dos serviços da solução;

3.2.5.4.5. **BAIXA** – chamado para esclarecimento de dúvidas referentes a possíveis problemas com a solução, assim como aplicação de melhorias e correções.

3.2.5.4.6. O nível de severidade dos chamados pode ser posteriormente alterado conforme avaliação da equipe técnica da CONTRATADA, em comum acordo com o CONTRATANTE;

3.2.5.5. **NÍVEIS DE SERVIÇO E SOLUÇÃO DOS CHAMADOS:**

3.2.5.5.1. Para qualquer nível de severidade, o início do atendimento não pode ultrapassar o prazo de uma hora após abertura do chamado por parte do CONTRATANTE;

3.2.5.5.2. Nós chamados de severidade URGENTE, o início do atendimento não pode ultrapassar o prazo de trinta minutos após abertura do chamado por parte do CONTRATANTE;

3.2.5.5.3. Prazos para solução dos chamados:

3.2.5.5.3.1. Para chamados de severidade BAIXA, a CONTRATADA tem prazo máximo de 8 horas para resolução do problema;

3.2.5.5.3.2. Para chamados de severidade MÉDIA, a CONTRATADA tem prazo máximo de 4 horas para resolução do problema;

3.2.5.5.3.3. Para chamados de severidade ALTA, a CONTRATADA tem prazo máximo de 2 horas para resolução do problema;

3.2.5.5.3.4. Para chamados de severidade URGENTE, a CONTRATADA tem prazo máximo de 1 horas para resolução do problema;

3.2.5.5.4. O prazo de solução dos chamados poderá ser prorrogado, a critério exclusivo do CONTRATANTE, caso a CONTRATADA apresente, tempestivamente, razões de justificativa que comprovem a ocorrência de fatos que fogem ao controle da CONTRATADA e impedem a solução do chamado no tempo estabelecido.

3.2.5.5.5. Poderá haver suspensão de contagem de prazos para chamados que necessitarem de providência por parte do fabricante, desde que a CONTRATADA comprove que efetuou todos os esforços necessários

junto ao fabricante para a solução das pendências. Uma vez que a CONTRATADA é responsável pela abertura e acompanhamento de chamados junto ao fabricante, ela deve efetuar as gestões necessárias para priorizar, reclassificar ou escalonar o chamado, de modo a resolver o problema no menor tempo possível. A suspensão ocorrerá apenas quando for realmente necessária a atuação do fabricante e for configurada situação em que a CONTRATADA não tem mais condições de atuação, após executados todos os procedimentos e verificações documentadas em manuais e sites do fabricante, isto é, quando estiver caracterizada falha no software ou em sua documentação.

3.2.5.6. **ABERTURA E ACOMPANHAMENTO DOS CHAMADOS:**

3.2.5.6.1. Os chamados de suporte podem ser iniciados e acompanhados via:

3.2.5.6.2. **PORTAL DE SUPORTE;**

3.2.5.6.2.1. A CONTRATADA deve prover um Portal de Suporte em ambiente WEB, disponível 24x7, para abertura e acompanhamento de chamados de suporte.

3.2.5.6.3. **CONTATO TELEFÔNICO;**

3.2.5.6.3.1. A CONTRATADA deve prover número de discagem gratuita (0800) ou número local para contato de suporte;

3.2.5.6.4. **E-MAIL;**

3.2.5.6.4.1. A CONTRATADA deve prover os endereços de e-mail de contato para abertura de chamados de suporte;

3.2.5.6.5. Independente do meio utilizado para abertura do chamado, este deve ser obrigatoriamente cadastrado no Portal de Suporte para acompanhamento e controle.

3.2.5.6.6. A CONTRATADA deve fornecer, com periodicidade mensal, relatórios a respeito das atividades do Portal de Suporte, com informações sobre os chamados, SLA de atendimento, e demais dados pertinentes.

3.3. **DESCRIÇÃO E SERVIÇOS DO MÓDULO DE ANÁLISE DE REDE.**

3.3.1. **MÓDULO DE ANÁLISE DE REDE.**

3.3.1.1. Solução baseada em software;

3.3.1.1.1. A solução deve permitir execução em ambiente virtualizado (instalada como máquina virtual) compatível, no mínimo, com Citrix XenServer e VmWare ESX;

3.3.1.2. Requisitos de capacidade e performance:

3.3.1.2.1. A solução deve suportar e ser licenciada para captura de dados de rede na taxa de, no mínimo, 01gbps (um gigabit por segundo);

3.3.1.2.2. A solução deve suportar e ser licenciada para armazenamento de, pelo menos, 10tb (dez terabytes) de dados capturados (incluindo metadados gerados);

3.3.1.3. Captura e Análise de tráfego de dados de rede

3.3.1.3.1. A solução deve ser capaz de capturar e armazenar o tráfego de rede a ela direcionado, em tempo real, funcionando 24 horas por dia;

3.3.1.3.2. A solução deve prover o sistema de captura e análise distribuídos, com disposição de módulos/elementos no ambiente do CONTRATANTE para permitir, no mínimo:

3.3.1.3.2.1. Captura distribuída, no sentido de permitir a captura de dados em redes locais e remotas, conforme distribuição de sensores de captura;

3.3.1.3.2.2. A arquitetura da solução deve levar em consideração a economia de uso dos links de comunicação do CONTRATANTE, no sentido de isolar a captura e armazenamento dos dados localmente em cada rede;

3.3.1.3.2.3. A demanda por maior uso dos circuitos de comunicação para tráfego de metadados e dados deve acontecer apenas quando demandado pela análise pontual por parte dos analistas;

3.3.1.3.3. Análise distribuída, no sentido de permitir a análise local dos dados capturados em cada rede/unidade remota, mesmo no evento de perda de conectividade com os pontos centrais da rede/backbone;

3.3.1.3.4. Análise centralizada, no sentido de prover visão total do ambiente, incluindo todos os pontos de captura, a partir de um ponto único (com uso do módulo de gerenciamento centralizado);

3.3.1.4. Extração e Indexação de Metadados

3.3.1.4.1. A solução deve ser capaz de extrair metadados do tráfego de rede capturado;

3.3.1.4.2. A solução deve ser capaz de indexar os metadados, e disponibilizá-los para pesquisa e análise;

3.3.1.4.3. A solução deve manter o vínculo entre metadados indexados e os dados originais, de modo a possibilitar a recuperação dos dados originais com base na pesquisa e análise dos metadados;

3.3.1.5. Análise de Metadados

3.3.1.5.1. A solução deve possuir interface para análise dos metadados;

3.3.1.5.2. A análise dos metadados deve ser baseada, no mínimo, nos seguintes fatores de contextualização:

3.3.1.5.3. Janela de tempo de análise;

3.3.1.5.4. Filtros com base em campos de metadados;

3.3.1.5.5. A análise dos metadados deve possuir sistema de redução de escopo de pesquisa, permitindo ao analista aplicar filtros encadeados indo de uma visão macro até detalhamentos específicos;

3.3.1.6. Reconstrução de sessões;

3.3.1.6.1. A solução deve ser capaz de reconstruir sessões, no sentido de prover ao analista uma visão em camada de aplicação dos dados capturados;

3.3.1.6.2. Deve suportar reconstrução de sessões, para, no mínimo, os seguintes protocolos/aplicações:

3.3.1.6.2.1. HTTP;

3.3.1.6.2.2. SMTP;

3.3.1.6.2.3. VoIP;

3.3.1.6.2.4. Instanting Messaging

3.3.1.7. Integração:

3.3.1.7.1. Deve possuir integração nativa com os Módulos de Proteção de Rede, no sentido de permitir pivoteamento direto entre as interfaces;

3.3.1.7.1.1. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista iniciar a análise de um incidente pela interface do Módulo de Proteção, e com apenas um clique de mouse acionar a console da solução, mostrando dados já contextualizados com as informações de origem;

3.3.1.7.1.1.1. Um exemplo de uso dessa funcionalidade seria iniciar a análise de um incidente via console do Módulo de Proteção, identificar o endereço IP interno alvo do ataque, e realizar por meio de um clique a pesquisa no Módulo de Análise de Rede já referenciada com o IP em questão (fundamental para levantamento de impacto de eventuais incidentes de segurança).

3.3.1.7.1.2. Deve ser capaz de responder aos seguintes tipos de pergunta:

3.3.1.7.1.2.1. “Mostre tudo que esse endereço fez em minha rede interna”;

3.3.1.7.1.2.2. “Mostre agora o que essa máquina fez na minha rede após ter sido infectada”;

3.3.1.7.2. Deve possuir integração nativa com o Módulo de Visibilidade e Análise de Dados, no sentido enviar os dados de log e auditoria para armazenamento histórico e análise;

3.3.1.7.3. Deve possuir integração nativa com o Módulo de Visibilidade e Análise de Dados, no sentido de permitir pivoteamento direto entre as interfaces;

3.3.1.7.3.1. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista iniciar a análise de um incidente pela interface do Módulo de Visibilidade e Análise de Dados, e com apenas um clique de mouse acionar a console da solução, mostrando dados já contextualizados com as informações de origem;

3.3.1.7.3.1.1. Um exemplo de uso dessa funcionalidade seria iniciar a análise de um incidente via console do Módulo de Visibilidade e Análise de Dados, identificar um evento suspeito, e realizar por meio de um clique a pesquisa no Módulo de Análise de Rede já referenciada com e evento em questão (fundamental para levantamento de impacto de eventuais incidentes de segurança).

3.3.1.7.3.2. Deve ser capaz de responder aos seguintes tipos de pergunta:

3.3.1.7.3.2.1. “Mostre tudo que relativo a esse evento em minha rede interna”;

3.3.2. **GARANTIA E MANUTENÇÃO MENSAL - MÓDULO DE ANÁLISE DE REDE**

3.3.2.1. Serviço de garantia e manutenção do módulo/solução, cobrindo pelo prazo contratado, no mínimo, os seguintes quesitos:

3.3.2.1.1. Resolução de problemas de software do módulo;

3.3.2.1.2. Garantia do funcionamento das funcionalidades adquiridas da solução durante o prazo contratado;

3.3.2.1.2.1. Na existência de funcionalidades do tipo assinatura (subscription), estas devem estar necessariamente ativas durante o prazo contratado;

3.3.2.1.3. Correção de falhas de software (bugs), com fornecimento de versões atualizadas diretamente pelo fabricante da solução, durante o prazo contratado;

3.3.2.1.4. Atualização de versões de módulos de software (updates, firmware, etc.) disponibilizados pelo fabricante da solução durante o prazo contratado;

3.3.3. **SERVIÇO DE IMPLANTAÇÃO - MÓDULO DE ANÁLISE DE REDE.**

3.3.3.1. Serviço de implantação do módulo/solução adquirida no ambiente do CONTRATANTE, contemplando, no mínimo, as seguintes atividades:

3.3.3.2. **CONFIGURAÇÃO BÁSICA:**

3.3.3.2.1. Conjunto de procedimentos de configuração com a finalidade de deixar a solução pronta para atuar em caráter operacional no ambiente de produção do CONTRATANTE, incluindo atualizações de software, endereçamento e regras iniciais.

3.3.3.2.2. Customização da configuração da solução para integração com o ambiente de rede do CONTRATANTE

3.3.3.2.3. Inclui a execução do Plano de Testes, visando verificar de forma objetiva e prática o funcionamento da solução.

3.3.3.3. **ACOMPANHAMENTO INICIAL**

3.3.3.3.1. Serviço de acompanhamento da operação inicial da solução, entre a ativação no ambiente de produção e o primeiro dia de funcionamento. Tem como objetivo prestar o apoio técnico necessário (incluindo ajustes porventura necessários) para que a migração para o ambiente de produção ocorra de forma controlada e segura.

3.3.3.4. O CONTRATANTE deve prover a infraestrutura necessária para implantação da solução em seu ambiente.

3.3.3.5. **DOCUMENTAÇÃO**

3.3.3.5.1. A Contratada deve apresentar um Plano de Implantação detalhando como a solução será instalada no ambiente do CONTRATANTE;

3.3.3.5.2. A Contratada deverá fornecer a Documentação do Projeto, detalhando como foi implantada a solução no ambiente do CONTRATANTE;

3.3.4. **SERVIÇO DE TREINAMENTO - MÓDULO DE ANÁLISE DE REDE.**

3.3.4.1. Serviço de treinamento da equipe técnica do CONTRATANTE visando capacitá-la na operação/administração/uso da solução, contemplando, no mínimo, os seguintes tópicos:

3.3.4.2. Apresentação do projeto/solução implementado;

3.3.4.2.1. Descrição da arquitetura física e lógica de cada elemento da solução;

3.3.4.2.2. Estratégias de implementação da solução;

3.3.4.2.3. Procedimentos de instalação da solução;

3.3.4.2.4. Operação e Administração da solução;

3.3.4.2.5. Descrição e uso das funcionalidades da solução;

3.3.4.2.6. Resolução de problemas (“troubleshooting”);

3.3.4.2.7. Procedimentos de manutenção (atualizações de software, backup/restore, instalação de módulos de hardware, etc.);

3.3.4.2.8. Elaboração de Relatórios;

3.3.4.3. A CONTRATADA deve obedecer ao prazo máximo de 15 dias úteis após assinatura do contrato para apresentação da ementa e detalhes da realização do treinamento.

3.3.4.4. A CONTRATADA deverá providenciar material didático individual que abranja todo o conteúdo do curso. Não será exigido material oficial do fabricante, entretanto este será avaliado pela equipe técnica do CONTRATANTE antes da realização do curso, e caso seja considerado insuficiente, deverá ser readaptado para as condições exigidas pelo CONTRATANTE.

3.3.4.5. O período e horário de realização do curso deverão ser definidos pela CONTRATADA, em conjunto com o CONTRATANTE, para momento posterior à implantação da solução;

3.3.4.6. A CONTRATADA deverá providenciar local e infraestrutura para o treinamento, podendo o CONTRATANTE optar por executá-lo em seu ambiente.

3.3.4.7. A CONTRATADA deve obedecer ao prazo máximo de 30 dias úteis após a implantação da solução no ambiente do CONTRATANTE para início do treinamento.

3.3.4.8. O treinamento deve ter carga horária de 16 horas.

3.3.4.9. A turma poderá ter até 08 alunos.

3.3.5. **SERVIÇO DE SUPORTE TÉCNICO MENSAL - MÓDULO DE ANÁLISE DE REDE.**

3.3.5.1. A CONTRATADA deve prover o serviço de Suporte Técnico para a solução adquirida pelo CONTRATANTE, pelo prazo contratual, conforme as especificações constantes neste documento;

3.3.5.2. **CHAMADOS DE SUPORTE:**

3.3.5.2.1. Os chamados de suporte técnico representam a solicitação formal de serviços de suporte à CONTRATADA e devem ser atendidos de acordo com os critérios e parâmetros estabelecidos para execução dos serviços.

3.3.5.2.2. O chamado deve conter uma descrição detalhada do problema, a indicação dos itens de configuração afetados, e o nome e telefone do contato do CONTRATANTE responsável pelo acompanhamento do serviço. O CONTRATANTE poderá ainda anexar ao chamado documentos ou imagens que auxiliem da identificação do problema, sugerir o perfil profissional adequado para a execução do serviço e, se for o caso, agendar data e hora para o atendimento.

3.3.5.3. **DISPONIBILIDADE E MODELO DE ATENDIMENTO:**

3.3.5.3.1. O atendimento será no modelo 24x7 (horário comercial, dias úteis) remoto e presencial (quando verificada a necessidade no decorrer do atendimento).

3.3.5.4. **CLASSIFICAÇÃO DE SEVERIDADE:**

3.3.5.4.1. Os chamados de suporte técnico serão classificados por severidade, dependendo do impacto que o problema a ser resolvido possa causar ao ambiente computacional do CONTRATANTE, sendo possíveis os seguintes níveis de severidade:

3.3.5.4.2. **URGENTE** – chamado para restabelecer serviço que esteja parado;

3.3.5.4.3. **ALTA** – chamado para restabelecer serviço que não esteja operando corretamente, apresente problema de desempenho ou esteja sob risco de parada;

3.3.5.4.4. **MÉDIA** – chamado para resolução de problemas que não estejam causando interrupção dos serviços da solução;

3.3.5.4.5. **BAIXA** – chamado para esclarecimento de dúvidas referentes a possíveis problemas com a solução, assim como aplicação de melhorias e correções.

3.3.5.4.6. O nível de severidade dos chamados pode ser posteriormente alterado conforme avaliação da equipe técnica da CONTRATADA, em comum acordo com o CONTRATANTE;

3.3.5.5. **NÍVEIS DE SERVIÇO E SOLUÇÃO DOS CHAMADOS:**

3.3.5.5.1. Para qualquer nível de severidade, o início do atendimento não pode ultrapassar o prazo de uma hora após abertura do chamado por parte do CONTRATANTE;

3.3.5.5.2. Nós chamados de severidade URGENTE, o início do atendimento não pode ultrapassar o prazo de trinta minutos após abertura do chamado por parte do CONTRATANTE;

3.3.5.5.3. Prazos para solução dos chamados:

3.3.5.5.3.1. Para chamados de severidade BAIXA, a CONTRATADA tem prazo máximo de 8 horas para resolução do problema;

3.3.5.5.3.2. Para chamados de severidade MÉDIA, a CONTRATADA tem prazo máximo de 4 horas para resolução do problema;

3.3.5.5.3.3. Para chamados de severidade ALTA, a CONTRATADA tem prazo máximo de 2 horas para resolução do problema;

3.3.5.5.3.4. Para chamados de severidade URGENTE, a CONTRATADA tem prazo máximo de 1 horas para resolução do problema;

3.3.5.5.4. O prazo de solução dos chamados poderá ser prorrogado, a critério exclusivo do CONTRATANTE, caso a CONTRATADA apresente, tempestivamente, razões de justificativa que comprovem a ocorrência de fatos que fogem ao controle da CONTRATADA e impedem a solução do chamado no tempo estabelecido.

3.3.5.5.5. Poderá haver suspensão de contagem de prazos para chamados que necessitarem de providência por parte do fabricante, desde que a CONTRATADA comprove que efetuou todos os esforços necessários junto ao fabricante para a solução das pendências. Uma vez que a CONTRATADA é responsável pela abertura e acompanhamento de chamados junto ao fabricante, ela deve efetuar as gestões necessárias para priorizar, reclassificar ou escalonar o chamado, de modo a resolver o problema no menor tempo possível. A suspensão ocorrerá apenas quando for realmente necessária a atuação do fabricante e for configurada situação em que a CONTRATADA não tem mais condições de atuação, após executados todos os procedimentos e verificações documentadas em manuais e sites do fabricante, isto é, quando estiver caracterizada falha no software ou em sua documentação.

3.3.5.6. **ABERTURA E ACOMPANHAMENTO DOS CHAMADOS:**

3.3.5.6.1. Os chamados de suporte podem ser iniciados e acompanhados via:

3.3.5.6.2. **PORTAL DE SUPORTE;**

3.3.5.6.2.1. A CONTRATADA deve prover um Portal de Suporte em ambiente WEB, disponível 24x7, para abertura e acompanhamento de chamados de suporte.

3.3.5.6.3. **CONTATO TELEFÔNICO;**

3.3.5.6.3.1. A CONTRATADA deve prover número de discagem gratuita (0800) ou número local para contato de suporte;

3.3.5.6.4. **E-MAIL;**

3.3.5.6.4.1. A CONTRATADA deve prover os endereços de e-mail de contato para abertura de chamados de suporte;

3.3.5.6.5. Independente do meio utilizado para abertura do chamado, este deve ser obrigatoriamente cadastrado no Portal de Suporte para acompanhamento e controle.

3.3.5.6.6. A CONTRATADA deve fornecer, com periodicidade mensal, relatórios a respeito das atividades do Portal de Suporte, com informações sobre os chamados, SLA de atendimento, e demais dados pertinentes.

3.4. DESCRIÇÃO E SERVIÇOS DO MÓDULO DE VISIBILIDADE E ANÁLISE DE DADOS.

3.4.1. MÓDULO DE VISIBILIDADE E ANÁLISE DE DADOS.

3.4.1.1. Solução baseada em software;

3.4.1.1.1. A solução deve ser baseada em software, permitindo sua instalação e execução utilizando recursos (servidores e armazenamento) da rede do CONTRATANTE;

3.4.1.2. Requisitos de capacidade e performance:

3.4.1.2.1. A solução deve suportar e ser licenciada para processar 6000 (seis mil) EPS (eventos por segundo) ou 100 (cem) gigabytes de dados indexados por dia;

3.4.1.3. Multi-plataforma;

3.4.1.3.1. A solução deve suportar instalação e execução em múltiplas plataformas, incluindo, no mínimo:

3.4.1.3.2. Windows XP, Vista, 7, 8, Server 2003, Server 2008, Server 2012;

3.4.1.3.3. Linux Kernel 3.0+, 32 e 64 bits;

3.4.1.3.4. Linux Kernel 2.6+, 32 e 64 bits;

3.4.1.3.5. Linux Kernel 2.4+, 32 bits;

3.4.1.4. Rastreabilidade;

3.4.1.4.1. A solução deve otimizar a capacidade de rastreabilidade no ambiente de rede do CONTRATANTE, no sentido de receber eventos de qualquer origem, indexá-los e armazená-los para consulta sob demanda;

3.4.1.4.2. Deve prover interface para pesquisa nos dados indexados;

3.4.1.4.3. Deve prover um ponto único de pesquisa para análise de eventos de qualquer fonte;

3.4.1.5. Suporte a topologia em ambiente distribuído;

3.4.1.5.1. A solução deve prover o sistema de recebimento e análise de eventos em ambiente distribuído, com disposição de módulos/elementos no ambiente do CONTRATANTE para permitir, no mínimo:

3.4.1.5.2. Coleta distribuída, no sentido de permitir o recebimento de eventos em redes locais e remotas, conforme distribuição de elementos de captura;

3.4.1.5.2.1. A arquitetura da solução deve levar em consideração a economia de uso dos links de comunicação do CONTRATANTE, no sentido de isolar a coleta e armazenamento dos dados localmente em cada rede;

3.4.1.5.2.2. O envio de eventos via links de comunicação deve acontecer apenas em casos isolados, tais como envio de alertas para uma camada central de correlação;

3.4.1.5.3. Análise distribuída, no sentido de permitir a análise local dos dados capturados em cada rede/unidade remota, mesmo no evento de perda de conectividade com os pontos centrais da rede/backbone;

3.4.1.5.4. Análise centralizada, no sentido de prover visão total do ambiente, incluindo todos os pontos de coleta de dados, a partir de um ponto único;

3.4.1.6. A solução deve ser modular, no sentido de permitir sua implantação tanto de forma centralizada, quanto distribuída pelo ambiente computacional do CONTRATANTE;

3.4.1.7. A solução deve ser constituída por, no mínimo, os seguintes módulos (os módulos são referentes a funcionalidades básicas, e podem ser disponibilizados de forma unificada ou distribuída):

3.4.1.7.1. Módulo de Indexação;

3.4.1.7.2. Módulo e Pesquisas Distribuídas;

3.4.1.7.3. Módulo de Tratamento e Encaminhamento de eventos;

3.4.1.7.4. Interface/Console Web;

3.4.1.7.5. Módulo de Correlação de Eventos;

3.4.1.7.6. A comunicação entre os módulos da solução deve ser criptografada.

3.4.1.7.6.1. A solução deve suportar o uso de certificados SSL gerados pelo cliente;

3.4.1.7.7. A distribuição dos módulos da solução pelo ambiente computacional do CONTRATANTE deve ser livre, no sentido de permitir sua disposição pelo ambiente sem a necessidade de licenças adicionais, dentro do limite de processamento e indexação licenciados, conforme requisitos de capacidade e performance;

3.4.1.8. Coleta e recebimentos de eventos;

3.4.1.9. A solução deve possuir mecanismos para coletar e/ou receber eventos dos elementos do ambiente de rede do CONTRATANTE;

3.4.1.10. A solução deve ser capaz de receber diretamente os eventos, ou coletar/recebe/encaminhar via Módulos de Tratamento e Encaminhamento;

3.4.1.11. Os módulos de tratamento e encaminhamento de eventos devem possuir, no mínimo, as seguintes funcionalidades;

3.4.1.12. Criptografia dos dados a serem enviados a outros módulos da solução;

3.4.1.13. Compressão dos dados coletados;

3.4.1.14. Capacidade de enviar os dados em qualquer porta disponível;

3.4.1.15. Coletar eventos locais ou remotos;

3.4.1.16. Receber dados de outros módulos de tratamento e encaminhamento, em topologia hierarquizada;

3.4.1.17. Balanceamento de carga no encaminhamento dos eventos;

3.4.1.18. Encaminhamento de dados para outras soluções de análise de eventos;

3.4.1.19. Controle do encaminhamento de dados, com retransmissão no evento de perda de dados durante a transferência via rede;

3.4.1.20. Indexação prévia dos eventos;

3.4.1.21. Os módulos de tratamento e encaminhamento de eventos não devem exigir licenças adicionais, ou seja, seu uso e distribuição no ambiente deve ser livre, desde que o módulo principal da solução esteja licenciado, conforme seção de requisitos de capacidade e performance

3.4.1.22. Visibilidade e Consciência Situacional;

3.4.1.23. A solução deve prover visibilidade dos dados coletados, visando aumentar o nível de consciência situacional do ambiente de rede do CONTRATANTE;

3.4.1.24. Deve permitir ao analista a geração de gráficos, estatísticas e dashboards com bases nos dados indexados;

3.4.1.25. Correlação de Eventos;

3.4.1.25.1. A solução deve ser capaz de correlacionar eventos distintos, visando gerar alertas com base em eventos sem relação inicial;

3.4.1.26. Gestão do armazenamento dos dados;

3.4.1.26.1. A solução deve ser capaz de gerenciar o armazenamento dos dados coletados e indexados;

3.4.1.26.2. Deve ser possível configurar uma política de arquivamento, em que os dados mais antigos, ou que ultrapassem os limites configurados, sejam apagados automaticamente ou arquivados em área separada;

3.4.1.27. Definição de Relatórios;

3.4.1.27.1. A solução deve permitir a geração de relatórios com base nos dados indexados;

3.4.1.27.2. Deve ser possível exportar os relatórios para formato PDF;

3.4.1.28. Definição de Alertas;

3.4.1.28.1. A solução deve ser capaz de monitorar elementos do ambiente (ativos, dispositivos de rede, aplicações, sistemas, servidores, etc.) em tempo real, com base nos eventos gerados pelos elementos e permitir a geração de alertas com base em condições pré-definidas;

3.4.1.28.2. Deve ser possível disparar (com base na configuração do alerta), no mínimo, as seguintes ações:

3.4.1.28.2.1. Enviar um e-mail;

3.4.1.28.2.2. Executar um script;

3.4.1.28.2.3. Deve ser possível abrir tickets em soluções de gerenciamento de incidentes via scripts;

3.4.1.28.2.4. Mostrar alerta no console de gerenciamento de alertas da solução;

3.4.1.28.2.5. Enviar alerta via SNMP;

3.4.1.28.2.6. Deve ser possível definir o nível de severidade do alerta;

3.4.1.29. Administração Web;

3.4.1.30. A solução deve possuir interface de administração gráfica padrão WEB (via browser);

3.4.1.31. Integração:

3.4.1.31.1. Deve possuir integração nativa com os Módulos de Proteção de Rede, no sentido de receber, indexar e armazenar logs e dados de auditoria;

3.4.1.31.1.1. Deve possuir ambiente pré-configurado para dar significado aos eventos recebidos dos Módulos de Proteção de Rede, com dashboards específicos, gráficos, listas e estatísticas;

3.4.1.31.2. Deve possuir integração nativa com o Módulo de Análise de Rede, no sentido de permitir pivoteamento direto entre as interfaces;

3.4.1.31.2.1. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista iniciar a análise de um incidente pela interface do Módulo de Visibilidade e Análise de Dados, e com apenas um clique de mouse acionar a console do Módulo de Análise de Rede, mostrando dados já contextualizados com as informações de origem;

3.4.1.31.2.1.1. Um exemplo de uso dessa funcionalidade seria iniciar a análise de um incidente via console do Módulo de Visibilidade e Análise de Dados, identificar um evento suspeito, e realizar por meio de um clique a pesquisa no Módulo de Análise de Rede já referenciada com e evento em questão (fundamental para levantamento de impacto de eventuais incidentes de segurança).

3.4.1.31.2.2. Deve ser capaz de responder aos seguintes tipos de pergunta:

3.4.1.31.2.2.1. “Mostre tudo que relativo a esse evento em minha rede interna”;

3.4.2. GARANTIA E MANUTENÇÃO MENSAL - MÓDULO DE VISIBILIDADE E ANÁLISE DE DADOS

3.4.2.1. Serviço de garantia e manutenção do módulo/solução, cobrindo pelo prazo contratado, no mínimo, os seguintes quesitos:

3.4.2.1.1. Resolução de problemas de software do módulo;

3.4.2.1.2. Garantia do funcionamento das funcionalidades adquiridas da solução durante o prazo contratado;

3.4.2.1.2.1. Na existência de funcionalidades do tipo assinatura (subscription), estas devem estar necessariamente ativas durante o prazo contratado;

3.4.2.1.3. Correção de falhas de software (bugs), com fornecimento de versões atualizadas diretamente pelo fabricante da solução, durante o prazo contratado;

3.4.2.1.4. Atualização de versões de módulos de software (updates, firmware, etc.) disponibilizados pelo fabricante da solução durante o prazo contratado;

3.4.3. **SERVIÇO DE IMPLANTAÇÃO - MÓDULO DE VISIBILIDADE E ANÁLISE DE DADOS.**

3.4.3.1. Serviço de implantação do módulo/solução adquirida no ambiente do CONTRATANTE, contemplando, no mínimo, as seguintes atividades:

3.4.3.2. **CONFIGURAÇÃO BÁSICA:**

3.4.3.2.1. Conjunto de procedimentos de configuração com a finalidade de deixar a solução pronta para atuar em caráter operacional no ambiente de produção do CONTRATANTE, incluindo atualizações de software, endereçamento e regras iniciais.

3.4.3.2.2. Customização da configuração da solução para integração com o ambiente de rede do CONTRATANTE

3.4.3.2.3. Inclui a execução do Plano de Testes, visando verificar de forma objetiva e prática o funcionamento da solução.

3.4.3.3. **ACOMPANHAMENTO INICIAL**

3.4.3.3.1. Serviço de acompanhamento da operação inicial da solução, entre a ativação no ambiente de produção e o primeiro dia de funcionamento. Tem como objetivo prestar o apoio técnico necessário (incluindo ajustes porventura necessários) para que a migração para o ambiente de produção ocorra de forma controlada e segura.

3.4.3.4. O CONTRATANTE deve prover a infraestrutura necessária para implantação da solução em seu ambiente.

3.4.3.5. **DOCUMENTAÇÃO**

3.4.3.5.1. A Contratada deve apresentar um Plano de Implantação detalhando como a solução será instalada no ambiente do CONTRATANTE;

3.4.3.5.2. A Contratada deverá fornecer a Documentação do Projeto, detalhando como foi implantada a solução no ambiente do CONTRATANTE;

3.4.4. **SERVIÇO DE TREINAMENTO - MÓDULO DE VISIBILIDADE E ANÁLISE DE DADOS.**

3.4.4.1. Serviço de treinamento da equipe técnica do CONTRATANTE visando capacitá-la na operação/administração/uso da solução, contemplando, no mínimo, os seguintes tópicos:

3.4.4.2. Apresentação do projeto/solução implementado;

3.4.4.2.1. Descrição da arquitetura física e lógica de cada elemento da solução;

3.4.4.2.2. Estratégias de implementação da solução;

3.4.4.2.3. Procedimentos de instalação da solução;

3.4.4.2.4. Operação e Administração da solução;

3.4.4.2.5. Descrição e uso das funcionalidades da solução;

3.4.4.2.6. Resolução de problemas (“troubleshooting”);

3.4.4.2.7. Procedimentos de manutenção (atualizações de software, backup/restore, instalação de módulos de hardware, etc.);

3.4.4.2.8. Elaboração de Relatórios;

3.4.4.3. A CONTRATADA deve obedecer ao prazo máximo de 15 dias úteis após assinatura do contrato para apresentação da ementa e detalhes da realização do treinamento.

3.4.4.4. A CONTRATADA deverá providenciar material didático individual que abranja todo o conteúdo do curso. Não será exigido material oficial do fabricante, entretanto este será avaliado pela equipe técnica do CONTRATANTE antes da realização do curso, e caso seja considerado insuficiente, deverá ser readaptado para as condições exigidas pelo CONTRATANTE.

3.4.4.5. O período e horário de realização do curso deverão ser definidos pela CONTRATADA, em conjunto com o CONTRATANTE, para momento posterior à implantação da solução;

3.4.4.6. A CONTRATADA deverá providenciar local e infraestrutura para o treinamento, podendo o CONTRATANTE optar por executá-lo em seu ambiente.

3.4.4.7. A CONTRATADA deve obedecer ao prazo máximo de 30 dias úteis após a implantação da solução no ambiente do CONTRATANTE para início do treinamento.

3.4.4.8. O treinamento deve ter carga horária de 24 horas.

3.4.4.9. A turma poderá ter até 08 alunos.

3.4.5. **SERVIÇO DE SUPORTE TÉCNICO MENSAL - MÓDULO DE VISIBILIDADE E ANÁLISE DE DADOS.**

3.4.5.1. A CONTRATADA deve prover o serviço de Suporte Técnico para a solução adquirida pelo CONTRATANTE, pelo prazo contratual, conforme as especificações constantes neste documento;

3.4.5.2. **CHAMADOS DE SUPORTE:**

3.4.5.2.1. Os chamados de suporte técnico representam a solicitação formal de serviços de suporte à CONTRATADA e devem ser atendidos de acordo com os critérios e parâmetros estabelecidos para execução dos serviços.

3.4.5.2.2. O chamado deve conter uma descrição detalhada do problema, a indicação dos itens de configuração afetados, e o nome e telefone do contato do CONTRATANTE responsável pelo acompanhamento do serviço. O CONTRATANTE poderá ainda anexar ao chamado

documentos ou imagens que auxiliem da identificação do problema, sugerir o perfil profissional adequado para a execução do serviço e, se for o caso, agendar data e hora para o atendimento.

3.4.5.3. **DISPONIBILIDADE E MODELO DE ATENDIMENTO:**

3.4.5.3.1. O atendimento será no modelo 24x7 (horário comercial, dias úteis) remoto e presencial (quando verificada a necessidade no decorrer do atendimento).

3.4.5.4. **CLASSIFICAÇÃO DE SEVERIDADE:**

3.4.5.4.1. Os chamados de suporte técnico serão classificados por severidade, dependendo do impacto que o problema a ser resolvido possa causar ao ambiente computacional do CONTRATANTE, sendo possíveis os seguintes níveis de severidade:

3.4.5.4.2. **URGENTE** – chamado para restabelecer serviço que esteja parado;

3.4.5.4.3. **ALTA** – chamado para restabelecer serviço que não esteja operando corretamente, apresente problema de desempenho ou esteja sob risco de parada;

3.4.5.4.4. **MÉDIA** – chamado para resolução de problemas que não estejam causando interrupção dos serviços da solução;

3.4.5.4.5. **BAIXA** – chamado para esclarecimento de dúvidas referentes a possíveis problemas com a solução, assim como aplicação de melhorias e correções.

3.4.5.4.6. O nível de severidade dos chamados pode ser posteriormente alterado conforme avaliação da equipe técnica da CONTRATADA, em comum acordo com o CONTRATANTE;

3.4.5.5. **NÍVEIS DE SERVIÇO E SOLUÇÃO DOS CHAMADOS:**

3.4.5.5.1. Para qualquer nível de severidade, o início do atendimento não pode ultrapassar o prazo de uma hora após abertura do chamado por parte do CONTRATANTE;

3.4.5.5.2. Nós chamados de severidade URGENTE, o início do atendimento não pode ultrapassar o prazo de trinta minutos após abertura do chamado por parte do CONTRATANTE;

3.4.5.5.3. Prazos para solução dos chamados:

3.4.5.5.3.1. Para chamados de severidade BAIXA, a CONTRATADA tem prazo máximo de 8 horas para resolução do problema;

3.4.5.5.3.2. Para chamados de severidade MÉDIA, a CONTRATADA tem prazo máximo de 4 horas para resolução do problema;

3.4.5.5.3.3. Para chamados de severidade ALTA, a CONTRATADA tem prazo máximo de 2 horas para resolução do problema;

3.4.5.5.3.4. Para chamados de severidade URGENTE, a CONTRATADA tem prazo máximo de 1 horas para resolução do problema;

3.4.5.5.4. O prazo de solução dos chamados poderá ser prorrogado, a critério exclusivo do CONTRATANTE, caso a CONTRATADA apresente, tempestivamente, razões de justificativa que comprovem a ocorrência de fatos que fogem ao controle da CONTRATADA e impedem a solução do chamado no tempo estabelecido.

3.4.5.5.5. Poderá haver suspensão de contagem de prazos para chamados que necessitarem de providência por parte do fabricante, desde que a CONTRATADA comprove que efetuou todos os esforços necessários junto ao fabricante para a solução das pendências. Uma vez que a CONTRATADA é responsável pela abertura e acompanhamento de chamados junto ao fabricante, ela deve efetuar as gestões necessárias para priorizar, reclassificar ou escalonar o chamado, de modo a resolver o problema no menor tempo possível. A suspensão ocorrerá apenas quando for realmente necessária a atuação do fabricante e for configurada situação em que a CONTRATADA não tem mais condições de atuação, após executados todos os procedimentos e verificações documentadas em manuais e sites do fabricante, isto é, quando estiver caracterizada falha no software ou em sua documentação.

3.4.5.6. **ABERTURA E ACOMPANHAMENTO DOS CHAMADOS:**

3.4.5.6.1. Os chamados de suporte podem ser iniciados e acompanhados via:

3.4.5.6.2. **PORTAL DE SUPORTE;**

3.4.5.6.2.1. A CONTRATADA deve prover um Portal de Suporte em ambiente WEB, disponível 24x7, para abertura e acompanhamento de chamados de suporte.

3.4.5.6.3. **CONTATO TELEFÔNICO;**

3.4.5.6.3.1. A CONTRATADA deve prover número de discagem gratuita (0800) ou número local para contato de suporte;

3.4.5.6.4. **E-MAIL;**

3.4.5.6.4.1. A CONTRATADA deve prover os endereços de e-mail de contato para abertura de chamados de suporte;

3.4.5.6.5. Independente do meio utilizado para abertura do chamado, este deve ser obrigatoriamente cadastrado no Portal de Suporte para acompanhamento e controle.

3.4.5.6.6. A CONTRATADA deve fornecer, com periodicidade mensal, relatórios a respeito das atividades do Portal de Suporte, com informações sobre os chamados, SLA de atendimento, e demais dados pertinentes.

3.5. DESCRIÇÃO E SERVIÇOS DOS SERVIÇOS DE OPERAÇÃO ASSISTIDA (UST).

3.5.1. SERVIÇOS DE OPERAÇÃO ASSISTIDA (UST).

3.5.1.1. Para execução de serviços não constantes nas etapas de implantação, suporte técnico e treinamento, serão utilizadas Unidades de Serviço Técnico (UST);

3.5.1.2. A utilização dos serviços quantificados constituirá mera expectativa em favor da CONTRATADA, posto que dependa da necessidade da execução dos serviços, não estando a CONTRATANTE obrigada a realizá-los em sua totalidade e não cabendo à CONTRATADA pleitear qualquer tipo de reparação.

3.5.1.3. Os serviços compreendem no desenvolvimento e manutenção evolutiva das atividades de proteção e combate a ameaças digitais no ambiente da CONTRATANTE, incluindo ações previstas no processo de gestão de segurança da informação, estando os possíveis serviços listados na tabela de complexidade das atividades a seguir:

Tabela 4 - Tabela de Complexidade das Atividades do Objeto e Seu Valor em UST

Complexidade	Descrição	Valor UST
Baixa	Revisão da configuração dos módulos de segurança da solução, criação e/ou revisão de regras de appliance de segurança, avaliação de dispositivos, avaliação de rede (análise de problemas de rede, análise de recursos da rede), configuração básica de dispositivos de rede, instalação física de dispositivos de rede e segurança.	1,0
Intermediária	Otimização da configuração dos módulos da solução, análise de riscos de ativos de tecnologia, análise de risco de perímetro, implantação de segurança em ativo de tecnologia, serviço de operação assistida de segurança, análise de tendência de tráfego	1,5
Alta	Análise de ameaças e malwares, customizações avançadas da solução, integração com outras soluções de segurança, apoio ao processo de resposta a incidentes, análise da arquitetura de segurança, apoio ao plano diretor de segurança, transferência de conhecimento, apoio à definição de políticas de segurança da informação e comunicações, análise de tráfegos anômalos, análise de dispositivos não autorizados, análise forense, detecção de dispositivos não autorizados, análise de riscos e segurança em redes cabeadas e wireless.	2,0

3.5.1.4. As atividades são valoradas em função do seu nível de complexidade. Dada a variação da complexidade das atividades existentes, criou-se níveis para enquadramento. Proporcional ao nível de complexidade da atividade está a especialização dos profissionais que as executarão, de forma que a quantidade de unidades de suporte técnico garantam a justa remuneração da atividade.

3.5.1.5. Os serviços deverão ser prestados nas dependências da CONTRATADA ou da CONTRATANTE, a critério desta, utilizando as boas práticas de gerenciamento de projetos e repasse de conhecimento, com gestão por demanda de tarefas e uso dos perfis de serviços, em conformidade com as disposições contidas neste Termo de Referência e seus anexos. Os serviços

serão requisitados e gerenciados por Ordem de Serviços, a qual será detalhada e autorizada de acordo com as demandas específicas.

3.5.1.6. A complexidade das atividades considera a relevância dos serviços, sua precedência sobre as demais, sua dificuldade operacional, o grau de documentação existente, as características dos profissionais de mercado e sua capacidade em cumprir as atividades, conforme Tabela de Complexidade das Atividades do Objeto e Seu Valor em UST.

3.5.1.7. As Ordens de Serviço serão repassadas à CONTRATADA, que dará encaminhamento interno para sua execução. Após a execução dos serviços, serão devolvidas via sistema ao demandante, a fim de serem validadas para ateste técnico e/ou destaque de glosa em caso de não atendimento aos padrões de qualidade exigidos.

3.5.1.8. Após a execução, ao receber a devolução da Ordem de Serviço da CONTRATADA, caberá ao demandante preencher os campos relativos ao ateste técnico e encaminhar ao Fiscal do Contrato com as autorizações e observações necessárias.

3.5.1.9. As Ordens de Serviço que possam provocar impacto/indisponibilidades deverão ser executadas prioritariamente fora do horário normal de expediente, em dias úteis, ou em finais de semana após agendamento e autorização da CONTRATANTE.

3.5.1.10. A mensuração do esforço da OS (ordem de serviço) deve considerar a quantidade de USTs necessárias.

3.5.1.11. A Ordem de Serviço deverá conter os seguintes requisitos:

3.5.1.11.1. Número da Ordem de Serviço;

3.5.1.11.2. Data da Emissão;

3.5.1.11.3. Unidade Solicitante;

3.5.1.11.4. Nome do responsável solicitante que deverá acompanhar a execução e declarar, no encerramento, a qualidade dos serviços prestados;

3.5.1.11.5. Telefone e e-mail do solicitante;

3.5.1.11.6. Objeto dos Serviços: Deverá ser descrito o escopo que o serviço pretende atender, procedimentos do negócio a ser atendido ou outros documentos complementares, onde serão especificadas as necessidades gerais a serem contempladas pelo projeto;

3.5.1.11.7. Descrição do processo de negócio, dos requisitos ou outros documentos complementares, onde serão especificadas as necessidades gerais a serem contempladas pelo projeto e que possam ser úteis para que a CONTRATADA realize a especificação dos serviços;

3.5.1.11.8. Total de unidades de serviços técnicos (UST): Quantidade total de esforço estimado para conclusão dos serviços;

3.5.1.11.9. Data máxima para conclusão: Determinar o prazo em que se pretende que o serviço esteja concluído;

3.5.1.11.10. Artefatos/produtos a serem produzidos: Definição do produto final a ser entregue pela contratada, quando da conclusão dos serviços e que deverá ser utilizado para atestar a aceitação dos serviços prestados. Por produto final, entende-se todo e qualquer resultado do esforço realizado, tais como relatórios, códigos, eventos, tabelas, ou quaisquer outros que sejam descritos como objeto da Ordem de Serviços;

3.5.1.11.11. Dados da Autorização: Nome/cargo/telefone do autorizador dos serviços e data da autorização;

3.5.1.12. A autorização para o início das atividades se dará única e exclusivamente através de Ordem de Serviços (OS), emitida pela CONTRATANTE, devidamente aprovada pelo Gestor da demanda.

3.5.1.13. Todos os artefatos entregues pela CONTRATADA estarão sujeitos a auditoria e controle de qualidade executados pela CONTRATANTE ou por empresa contratada para esse fim.

3.5.1.14. A participação da CONTRATADA em reuniões para assinatura dos termos da OS, entrega de produtos, resolução de dúvidas, negociação de prazos ou quaisquer outras questões referentes ao trabalho, não resultará em remuneração adicional.

3.5.1.15. O cronograma aprovado na OS é o documento válido para definir a entrega dos artefatos acordados. Qualquer alteração deverá ser devidamente justificada e acordada entre as partes em documento próprio.

3.5.1.16. Os serviços de técnicos deverão sempre ser executados por profissionais que detenham os conhecimentos requeridos para a execução dos serviços detalhados na Ordem de Serviços.

3.5.1.17. Todos os serviços devem ser executados e documentados obedecendo aos critérios estabelecidos em metodologia a ser indicada pela CONTRATADA e referendada pela CONTRATANTE.

3.5.1.18. O atendimento à requisição de novas implementações será iniciado em, no máximo, quarenta e oito horas após recebimento formal da Ordem de Serviços e contará com esforço concentrado da CONTRATADA com vistas a apresentar o produto esperado no prazo determinado, com ressalva aos casos fortuitos ou força maior. As demandas de manutenções evolutivas deverão ser iniciadas em no máximo 3 horas.

3.5.1.19. A quantidade de esforço necessário para atendimento de um objetivo definido na Ordem de Serviços pode ser redimensionada, desde que as partes estejam em comum acordo. Neste caso, será necessária a apresentação prévia, pela CONTRATADA, de Relatório de Impacto, detalhando as causas do redimensionamento e os efeitos decorrentes, e a abertura de uma nova Ordem de Serviços em aditamento a anterior. O Relatório de Impacto pressupõe que somente as tarefas não realizadas serão objeto de redimensionamento.

3.5.1.20. Os serviços serão executados pela CONTRATADA, na forma, quantidade e qualidade pactuada, a partir da data de assinatura do CONTRATO, nos locais a critério da CONTRATANTE.

3.5.1.21. Todas as Ordens de Serviços serão controladas por sistema de informação da CONTRATADA, via web, ao qual a CONTRATANTE terá acesso para efeito de acompanhamento.

3.5.1.22. A CONTRATADA deverá fornecer relatórios mensais definidos em conjunto com a equipe técnica da CONTRATANTE e poderão sofrer atualizações na medida em que o nível de controle dos serviços prestados se torne necessário, sem custo adicional para o CONTRATANTE.

3.5.1.23. A CONTRATADA deverá indicar um Responsável Técnico e um eventual substituto para a coordenação, garantia da qualidade, e gestão do CONTRATO.

3.5.1.24. O Responsável Técnico deverá ter a sua indicação formalizada junto ao CONTRATANTE e contar com a anuência desta.

3.5.1.25. O CONTRATANTE deverá:

3.5.1.25.1. Supervisionar a execução e implantação dos produtos objetos das Ordens de Serviço; Checar e aprovar as ordens de serviço/relatórios de serviços encaminhados pela CONTRATADA;

3.5.1.25.2. Analisar a qualidade dos serviços realizados pela CONTRATADA e propor as glosas que deverão ser aplicadas a OS quando não atendidos os padrões de qualidade e resultados esperados especificados, anexando elementos comprobatórios do atendimento.

4. DESCRIÇÃO DAS FUNCIONALIDADES

4.1. **CARACTERÍSTICAS OBRIGATÓRIAS DO MÓDULO DE PROTEÇÃO DE REDE**

4.1.1. A solução deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos:

4.1.1.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

4.1.1.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação.

4.1.1.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação. Gerar roteamento virtual para pelo menos 10 roteadores virtuais e administração do tráfego entre diferentes áreas de segurança e sub-redes, suportando pelo menos 40 áreas de segurança e possibilidade de até 6 sistemas virtuais.

4.1.1.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

4.1.2. Permitir suporte para múltiplos sistemas virtuais lógicos (Contextos) no firewall Físico, de acordo com requisitos de capacidade e performance;

4.1.2.1. Os contextos virtuais devem suportar todas as funcionalidades base desta especificação.

4.1.3. Deverá contar com suporte para os serviços a seguir:

4.1.3.1. Redes Virtuais, vlans 802.1q;

4.1.3.2. Tradução de endereços da rede (NAT) por origem e destino, por endereços ip dinâmicos e pool de portas.

4.1.3.3. PPPOE, bgp, ospf e rip2, dhcp server e dhcp relay.

4.1.3.4. Protocolos de encriptação IKE, 3Des (com criptografia de 128, 192 e 256 bits), AES, SHA1 e MD5.

4.1.3.5. Deverá suportar pelos menos os seguintes protocolos de VOIP: H.323, SIP, SCCP e MGCP.

4.1.3.6. Identificação, Controle e visibilidade sendo:

4.1.3.7. Identificação, Controle (definição de regras de uso de aplicações por usuário -mediante interação com Ldap, Active Directory ou Radius – e endereço IP).

4.1.3.8. Identificação deve ser de modo independente à porta lógica e/ou aplicações que utilizam as portas 80 e 443 (Implica a descrição bidirecional de SSL e Identificação de aplicações que encapsuladas em túnel SSL).

4.1.3.9. Visibilidade de pelo menos 1400 aplicações incluindo peer-to-peer, facebook, twitter e web 2.0.

4.1.3.10. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Skype e ataques mediante a porta 443.

4.1.3.11. Em caso de protocolos desconhecidos, poderão designar-se assinaturas próprias.

4.1.3.12. Descrição e controle de tráfego SSHv2.

4.1.3.13. Detecção de aplicações dinâmicas dentro de sessões de proxy HTTP.

4.1.3.14. Controle de tráfego IPv4 e IPv6, este último inclui visibilidade e inspeção de ameaças em aplicações e controle de conteúdo. O IPV6 deve ser suportado em interfaces trabalhando em L2 e L3.

4.1.3.15. A solução deve ser ofertada em Appliance/hardware especifico para o proposito solicitado, não sendo aceito soluções baseadas em servidores abertos.

4.1.3.16. A Solução deve utilizar sistema operacional próprio "hardenizado", não sendo aceitos sistemas baseados em distribuições abertas.

4.1.3.17. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

4.1.4. Controles por Políticas de Firewall

4.1.4.1. Deve suportar controles por zona de segurança.

4.1.4.2. Suportar as seguintes características:

4.1.4.2.1. Controles de políticas por porta e protocolo.

4.1.4.2.2. Controle de políticas por Aplicações e categorias de aplicações.

4.1.4.2.3. Controle de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.

4.1.4.2.4. Controle de políticas por código de Pais (Por exemplo: BR, USA, UK, RUS).

4.1.4.2.5. Controle de inspeção e de-criptografia de SSL por política para trafego de entrada (Inbound) e Saída (Outbound).

4.1.4.2.6. Controle de inspeção e de-criptografia de SSH por política.

4.1.4.3. Suportar bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg.

4.1.4.4. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)

4.1.4.5. QoS baseado em políticas para marcação de pacotes (diffserv marking).

4.1.4.6. Suportar objetos e regras IPV6.

4.1.4.7. Suportar objetos e regras multicast.

4.1.4.8. Suportar atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.1.5. Controle de Aplicações

4.1.5.1. Deve contar com ferramentas de visibilidade que permitam administrar o tráfego de aplicações, permitindo a execução de aplicações autorizadas e bloqueio de aplicações não autorizadas.

4.1.5.2. O controle de aplicações deve identificar as mesmas independente das portas e protocolos assim como técnicas de evasão utilizadas.

4.1.5.3. Deve suportar múltiplos métodos de identificação e classificação das aplicações.

4.1.5.4. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

4.1.5.5. Deve suportar a criação de aplicações customizadas pela interface gráfica do produto.

4.1.5.6. Deve incluir a capacidade de atualização para identificar novas aplicações.

4.1.5.7. Deve atualizar a base de assinaturas de aplicações automaticamente.

4.1.5.8. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas do fabricante.

4.1.5.9. Deve alertar o usuário quando uma aplicação foi bloqueada.

4.1.5.10. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações.

4.1.5.11. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/políticas para os mesmos.

4.1.5.12. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, YIM, Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos.

4.1.5.13. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YIM chat e bloquear a transferência de arquivos.

4.1.5.14. Deve possibilitar a diferenciação de aplicações Proxies (ultrasurf, ghostsurf, freegate, etc.) possuindo granularidade de controle/políticas para os mesmos.

4.1.5.15. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuário) está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-diretório e base de dados local.

4.1.5.16. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

4.1.5.17. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

4.1.5.18. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

4.1.5.19. Deve incluir a capacidade de criação de políticas baseadas no controle por aplicação, categoria de aplicação, subcategoria, tecnologia e fator de risco.

4.1.5.20. Deve incluir a capacidade de criação de políticas baseadas no controle por usuário, grupos de usuários ou endereço ip.

4.1.5.21. Deve incluir a capacidade de criação de políticas baseadas em “traffic shaping” por aplicação, usuário, origem, destino, túnel vpn-ipsec-ssl.

4.1.5.22. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a

navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

4.1.5.23. Deve suportar autenticação Kerberos.

4.1.5.24. Deve possuir suporte a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

4.1.6. IPS

4.1.6.1. Deve possuir módulo integrado de IPS (Sistema de Prevenção de Intrusão), no mesmo appliance, fornecido pelo mesmo fabricante, operando em total compatibilidade com o módulo de firewall;

4.1.6.2. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

4.1.6.3. Deve possibilitar a criação de diferentes profiles de IPS a serem aplicados por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

4.1.6.4. Deve permitir o bloqueio de vulnerabilidades por assinatura.

4.1.6.5. Deve permitir o bloqueio de exploits conhecidos.

4.1.6.6. Deve incluir proteção contra ataques de negação de serviços.

4.1.6.7. Deve possuir os seguintes mecanismos de inspeção de IPS:

4.1.6.7.1. Análise de padrões de estado de conexões

4.1.6.7.2. Análise de decodificação de protocolo

4.1.6.7.3. Análise para detecção de anomalias de protocolo

4.1.6.7.4. Análise heurística

4.1.6.7.5. IP Defragmentation

4.1.6.7.6. Remontagem de pacotes de tcp

4.1.6.7.7. Bloqueio de pacotes malformados

4.1.6.8. Deve possuir assinaturas para bloqueio de ataques "buffer overflow".

4.1.6.9. Deve possuir assinaturas para auxilio no bloqueio de ataques DoS/DDoS.

4.1.6.10. Deve suportar o reconhecimento de ataques em trafego IPV6.

4.1.6.11. Deve possuir assinaturas e mecanismos de detecção de anomalias prontas.

4.1.6.12. Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

4.1.6.13. Deve ser possível a criação de exceções/exclusões por hosts para determinadas assinaturas.

4.1.6.14. Deve suportar referência cruzada com CVE.

4.1.6.15. Deve possuir granularidade de ajustes com opções para sobrescrever assinaturas individualmente.

4.1.6.16. Deve suportar atualização automática das assinaturas através de conexão segura.

4.1.6.17. Todos os modelos de equipamentos devem utilizar as mesmas assinaturas.

4.1.6.18. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos).

4.1.6.19. Deve suportar ações por assinaturas.

4.1.6.20. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.

4.1.7. Antivírus / Anti-Spyware

4.1.7.1. Para proteção do ambiente contra Malware, deve ser incluído modulo de Antivírus e Ant-Spyware de gateway integrado na própria ferramenta de Firewall (no mesmo appliance), fornecido pelo mesmo fabricante;

4.1.7.2. Deverá permitir o bloqueio de Malwares e Spywares.

4.1.7.3. Deverá ser possível a inspeção de Antivírus para pelo menos nos seguintes tipos de tráfegos: HTTP, SMTP, POP3, IMAP e SMB.

4.1.7.4. Deverá incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

4.1.7.5. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos.

4.1.7.6. Rastreamento de vírus em pdf.

4.1.7.7. Deverá permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

4.1.7.8. Deverá suportar bloqueio de arquivos por tipo (pelo menos 50 tipos).

4.1.7.9. A atualização de assinaturas deverá ser diária, semanal e de emergência.

4.1.7.10. Deve suportar atualização automática das assinaturas através de conexão segura.

4.1.7.11. As atualizações de ameaças, Antivírus e Anti-spyware não devem depender de reboot do equipamento para efetivação.

4.1.7.12. Suportar notificações e alertas via e-mail, SNMP traps e log de pacotes.

4.1.8. Analise de Ameaças Avançadas

4.1.8.1. Devido às características de evasão de identificação das novas gerações de malware, e o fato de um antivírus comum reativo não ser capaz de detectar as ameaças com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir módulo de análise avançada de malware, incluindo ameaças desconhecidas, fornecido pelo mesmo fabricante, e totalmente integrado com o módulo de Firewall.

4.1.8.1.1. O termo “Ameaça Desconhecida” deve ser entendido como código malicioso e/ou malware que não é reconhecido pelas soluções tradicionais de proteção (Antivírus, IPS, etc.), passando portanto despercebido pelas camadas tradicionais de proteção;

4.1.8.1.2. Uma Ameaça Desconhecida pode representar também um malware customizado, desenvolvido especificamente para atacar um determinado alvo/rede/organização;

4.1.8.1.3. A solução deve ser capaz, portanto, de identificar ameaças independentemente da existência de assinaturas de reconhecimento;

4.1.8.1.4. Não serão aceitas soluções “montadas” compostas por produtos independentes, para adicionar à solução ofertada a capacidade de identificação de ameaças avançadas.

4.1.8.1.4.1. Este requisito técnico visa proteger o CONTRATANTE dos custos administrativos e operacionais, assim como riscos decorrentes da redução de nível funcional e capacidade de proteção, em consequência do uso de soluções “montadas”, com nível insuficiente de integração, incapaz de atender aos requisitos técnicos especificados.

4.1.8.2. Para ameaças/Malwares desconhecidos, o produto deve ser capaz de enviar o arquivo suspeito para análise automática em “Cloud de análise” do mesmo fabricante e nativamente integrado à solução;

4.1.8.3. Essa analise deve suportar a monitoração do arquivo para mais de 100 comportamentos maliciosos.

4.1.8.4. A análise de ameaças avançadas não deve ser interpretada apenas como “análise heurística”, pois esta é uma técnica já utilizada por soluções tradicionais de defesa (Antivírus, por exemplo). Análise Heurística deve ser apenas uma dentre as várias técnicas utilizadas para classificar um artefato suspeito como malware.

4.1.8.5. O sistema automático de análise "In Cloud" deve prover:

4.1.8.5.1. Informações sobre as ações do malware na máquina infectada.

4.1.8.5.2. Informações sobre quais aplicações são utilizadas para causar/propagar a infecção.

4.1.8.5.3. Detectar aplicações não confiáveis utilizadas pelo Malware.

4.1.8.5.4. Gerar assinaturas de Antivírus e Anti-Spyware automaticamente, que devem ser incorporadas nos pacotes de atualização da solução. O resultado direto é que um dos produtos da análise de ameaças avançadas deve ser, após classificação do objeto como malware, a geração automática de assinaturas, de modo que a ameaça passe a ser conhecida pela solução após o próximo ciclo de atualização (com prazo de geração de novas assinaturas definido pelo nível de licenciamento da solução);

4.1.8.5.5. Definir URLs não confiáveis utilizadas pelo novo Malware.

4.1.8.5.6. Entre outros provendo uma maior segurança para a rede do cliente.

4.1.8.6. Deve possuir a capacidade de definir que tipos de arquivos podem ser enviados para análise do tipo “Cloud”.

4.1.8.7. Deve ser possível configurar a solução para enviar para análise em Cloud somente arquivos com origem em zonas de segurança não confiáveis (Internet, por exemplo);

4.1.8.8. Deve permitir criação de políticas para controlar que informações de sessão devem ser incluídas junto com o arquivo suspeito, para análise. Dentre as informações de sessão, deve ser possível escolher, no mínimo, entre:

4.1.8.8.1. Usuário Alvo;

4.1.8.8.2. Endereço IP de origem;

4.1.8.8.3. Aplicação;

4.1.8.8.4. Número da porta;

4.1.8.9. A comunicação de dados entre o appliance e o serviço “In Cloud” deve ser necessariamente criptografada e com autenticação por certificados digitais assinados pelo fabricante.

4.1.8.10. A solução deve ser entregue necessariamente licenciada, pelo prazo adquirido pelo CONTRATANTE, para possuir acesso a assinaturas

disponibilizadas pelo fabricante da solução referentes às ameaças desconhecidas identificadas, atendendo aos seguintes níveis de serviço:

4.1.8.10.1. Novas assinaturas de combate a ameaças avançadas devem ser disponibilizadas pelo fabricante em prazo inferior 48 horas;

4.1.8.10.2. O prazo especificado é referente a assinaturas que contém identificação de ameaças detectadas na rede do CONTRATANTE;

4.1.8.10.3. O prazo especificado é referente a assinaturas que contém identificação de ameaças detectadas em todas as unidades da solução existentes em produção no mundo, visando agregar a capacidade de proteção contra ameaças atuantes em outras redes;

4.1.9. Filtro de URL

4.1.9.1. Para maior controle e visibilidade dos acessos WEB dos usuários do ambiente, a solução deve possuir módulo de filtro de URL integrado na própria ferramenta de Firewall (no mesmo appliance, fornecido pelo mesmo fabricante), atendendo aos seguintes requisitos:

4.1.9.2. Deve ser possível criação de políticas por Usuários, Grupos de Usuários, IPs, Redes e Zonas de segurança.

4.1.9.3. Deve ser possível definir horários para o funcionamento da política.

4.1.9.4. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-diretório e base de dados local.

4.1.9.5. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

4.1.9.6. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

4.1.9.7. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários.

4.1.9.8. Deve incluir a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL.

4.1.9.9. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

4.1.9.10. Deve possuir suporta a identificação de usuários em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle sobre o uso das URLs que estão sendo acessadas através destes serviços.

4.1.9.11. Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs.

4.1.9.12. Deve possuir pelo menos 50 categorias de URLs.

4.1.9.13. Deve possibilitar a criação Categorias de URLs customizadas.

4.1.9.14. Deve possibilitar a exclusão de URLs do bloqueio por categoria.

4.1.9.15. Deve possibilitar a customização de página de bloqueio.

4.1.9.16. Deve possibilitar o bloqueio e continuação (Possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site por um tempo).

4.1.9.17. Os logs do produto devem incluir informações das atividades dos usuários.

4.1.9.18. A atualização da base de dados deve ser automática com a opção de ser feita manualmente via tftp.

4.1.10. Filtro de Dados

4.1.10.1. Deve ser possível a criação de filtros para arquivos e dados pré-definidos.

4.1.10.2. Os arquivos devem ser identificados por extensão e assinaturas.

4.1.10.3. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (ex. MS Office, PDF, etc.) identificados sobre aplicações (Ex. P2P, IM, SMB, etc.).

4.1.10.4. Deve ser possível a identificação de arquivos compactados e a aplicações de políticas sobre o conteúdo desses tipos de arquivos.

4.1.10.5. O firewall deve ser capaz de identificar e opcionalmente prevenir a transferência de informações sensíveis (Ex. número de cartão de credito, etc.) possibilitando a criação de novos tipos de dados via expressão regular.

4.1.10.6. Listar o número de aplicações suportadas para controle de dados.

4.1.10.7. Listar o número de tipos de arquivos suportados para controle de dados.

4.1.11. QoS

4.1.11.1. Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

4.1.11.2. Com a finalidade de controlar aplicações e trafego cujo consumo possa ser excessivo, (como youtube, ustream, etc.) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deva ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

4.1.11.3. Deve ser possível aplicar uma política de QoS para controlar o uso de banda de um determinado usuário ou grupo de usuários para uma determinada aplicação ou grupo de aplicações, como, por exemplo, controlar o uso de banda dos usuários do grupo “Desenvolvedores” para uso de Facebook e Youtube;

4.1.11.4. Suportar a criação de políticas de QoS por:

4.1.11.4.1. Endereço de origem

4.1.11.4.2. Endereço de destino

4.1.11.4.3. Por usuário ou Grupo do AD.

4.1.11.4.4. Por aplicações (como por exemplo Skype, Bittorrent, YouTube, Azureus)

4.1.11.4.5. Por aplicações estaticamente ou grupos dinamicamente (como por exemplo Instant Messaging ou grupo de aplicações P2P)

4.1.11.4.6. Por porta

4.1.11.5. O QoS deve possibilitar a definição de classes por:

4.1.11.5.1. Banda Garantida

4.1.11.5.2. Banda Máxima

4.1.11.5.3. Fila de Prioridade.

4.1.11.6. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.

4.1.11.7. Suportar marcação de pacotes Diffserv

4.1.11.8. Disponibilizar estatísticas RealTime para classes de QoS.

4.1.11.9. Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

4.1.12. GeoLocation

4.1.12.1. Suportar a criação de políticas por Geo-localização, permitindo o tráfego de determinado País/Países seja bloqueado.

4.1.12.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

4.1.12.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

4.1.13. Decriptografia SSL/SSH

4.1.13.1. Deve identificar, decriptografar e analisar o tráfego SSL em conexões de saída (Outbound)

4.1.13.2. Deve identificar, decriptografar e analisar o tráfego SSL em conexões de entrada (Inbound)

4.1.13.3. Deve identificar, decriptografar e analisar o tráfego SSH em conexões de saída (Outbound)

4.1.13.4. Deve identificar, decriptografar e analisar o tráfego SSH em conexões de entrada (Inbound)

4.1.13.5. A inspeção de SSL deve permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc.) e tráfegos não Pessoais.

4.1.13.6. Deve decriptografar o trafego em todos os tipos de implementação, como:

4.1.13.6.1. Tap mode

4.1.13.6.2. Modo Transparente/Bridge

4.1.13.6.3. Layer 2

4.1.13.6.4. Layer 3

4.1.14. Identificação de Usuários.

4.1.14.1. Deve suportar pelo menos os seguintes serviços de autenticação para identificação de usuários:

4.1.14.1.1. Active Directory

4.1.14.1.2. LDAP

4.1.14.1.3. eDirectory

4.1.14.1.4. RADIUS

4.1.14.1.5. Kerberos

4.1.14.1.6. Client Certificate

4.1.14.2. Deve suportar a criação de políticas baseado em Grupos e Usuários do Active Directory adicionalmente a IP Origem / Destino.

4.1.14.3. Deve possibilitar a identificação de usuários sem a necessidade de instalação de agente individualmente em cada equipamento da rede.

4.1.14.4. Deve suportar a identificação de usuários em ambientes Citrix e Terminal Server, assim como a utilização dos mesmos nas políticas de acesso.

4.1.14.5. Deve popular todos os logs de trafego, IPS, URL, Data, Aplicações entre outros com as informações dos usuários.

4.1.14.6. Os logs de identificação de usuários deve ser feito em tempo real, e não correlacionado após a ocorrência do tráfego em questão.

4.1.15. Funcionalidades de Rede

4.1.15.1. Suportar funcionamento em Tap Mode (Via porta espelhada, Tap ou SPAN port).

4.1.15.2. Suportar funcionamento em mode transparente (Bridge ou similar).

4.1.15.3. Suportar funcionamento em Layer 2

4.1.15.4. Suportar funcionamento em Layer 3

4.1.15.5. Suportar a implementação simultânea em todos os modos descritos acima (Tap, Transparente, Layer2 e Layer3) no mesmo equipamento.

4.1.15.6. Deve suportar Vlan Tagging (802.1Q) em todos os cenários de implementação acima (Transparente, Layer2 e Layer3).

4.1.15.7. Deve suportar controle de aplicações em IPV6 em todos os cenários de implementação acima (Tap, Transparente, Layer2 e Layer3).

4.1.15.8. Suportar sub-interfaces ethernet logicas.

4.1.16. NAT

4.1.16.1. Deverá suportar:

4.1.16.1.1. Porta/IP Nat dinâmico (Many-to-1 e Many-to-Many).

4.1.16.1.2. IP Nat dinâmico (Many-to-Many).

4.1.16.1.3. IP Nat estático (1-to-1, Many-to-Many, Ips).

4.1.16.1.4. Nat estático bidirecional 1-to-1.

4.1.16.1.5. IP Virtual (VIP)

4.1.16.1.6. Tradução de porta (PAT).

4.1.16.1.7. NAT de Origem

4.1.16.1.8. NAT de Destino

4.1.16.2. Suportar NAT de Origem e NAT de Destino simultaneamente.

4.1.16.3. Prover capacidade de NAT Traversal, suportando aplicações e Serviços VoIP.

4.1.17. VPN

4.1.17.1. Suportar VPN Site-to-Site e Cliente-To-Site.

4.1.17.2. Suportar IPSec VPN

4.1.17.3. Suportar SSL VPN

4.1.17.4. Suportar atribuição de IPs nos clientes remotos de VPN.

4.1.17.5. Suportar atribuição de DNS nos clientes remotos de VPN.

4.1.17.6. Estar licenciada para 2000 clientes de VPN simultâneos.

4.1.17.7. IPSec VPN deve suportar:

4.1.17.8. 3DES, AES

4.1.17.9. Autenticação MD5 e SHA1

4.1.17.10. Diffie Hellman Group 1, Group 2 e Group 5

4.1.17.11. Algoritmo Internet Key Exchange (IKE)

4.1.17.12. AES 128, 192 & 256 (Advanced Encryption Standard).

4.1.17.13. Deve possuir interoperabilidade de VPN com, no mínimo, os seguintes fabricantes:

4.1.17.13.1. Cisco

4.1.17.13.2. Palo Alto Networks

4.1.17.13.3. Fortinet

4.1.17.13.4. Sonic Wall

4.1.17.14. Deverá permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

4.1.17.15. Deverá contar com um software cliente de VPN-SSL para os sistemas operacionais Windows SP, Vista (32 e 64 bits) e Windows 7 (32 e 64 bits).

4.1.17.16. Deverá permitir criar políticas para tráfego VPN-SSL.

4.1.17.17. SSL VPN com suporte a proxy arp e uso de interfaces PPPOE.

4.1.17.18. Suporte para autenticação de VPNs SSL, Ldap, Secure id e base de dados própria.

4.1.18. Roteamento

4.1.18.1. Deve suportar as seguintes funcionalidades de roteamento:

4.1.18.2. Estático e Dinâmico.

4.1.18.3. RIP v2

4.1.18.4. OSPF

4.1.18.5. BGP v4

4.1.18.6. Suporte a roteamento IPv6.

4.1.18.7. Suporte a roteadores Virtuais (Virtual Routers).

4.1.18.8. Suporte a "Policy Based Fowarding" por:

4.1.18.8.1. Zona de segurança

4.1.18.8.2. Endereço de Origem e Destino

4.1.18.8.3. Porta

4.1.18.8.4. Aplicação

4.1.18.8.5. Usuários e/ou Grupos da base AD/LDAP

4.1.18.8.6. Combinação de todos acima.

4.1.19. Alta Disponibilidade

4.1.19.1. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

4.1.19.2. Em modo Transparente.

4.1.19.3. Em layer 2

4.1.19.4. Em layer 3

4.1.19.5. O H.A. deve sincronizar:

4.1.19.5.1. Todas as sessões.

4.1.19.5.2. Certificados decriptogafados

4.1.19.5.3. Todas Associações de Segurança das VPNs

4.1.19.5.4. Todas as assinaturas de Antivírus, Anti-spyware e Aplicações.

4.1.19.5.5. Todas as configurações

4.1.19.5.6. Tabelas FIB.

4.1.19.6. O HA deve possibilitar tracking de IP

4.1.19.7. Deve permitir monitoração de falha de link.

4.1.20. Suporte à Segurança nos computadores da organização

4.1.20.1. Mediante apenas futura aquisição e aplicação de licença específica (sem adição de novos módulos no appliance ou hardware adicional), deverá suportar um agente que, quando instalado nos equipamentos desktop ou

laptop da instituição, transportem as políticas e todas as características de segurança do Firewall a tal equipamento.

4.1.20.2. O Agente de software a ser instalado nos equipamentos desktop e laptops, deverá ser capaz de ser distribuído de maneira automática por ferramentas de distribuição de software, no mínimo, via SMS e Active Directory, e ser descarregado diretamente desde o seu próprio portal, o qual residirá no Firewall.

4.1.20.3. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

4.1.20.4. Deve manter uma conexão segura com o portal durante a sessão.

4.1.20.5. Determinar o perfil de host com base em: Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.

4.1.20.6. Deve ser possível a criação de perfis customizados com base em Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.

4.1.20.7. O portal deverá enviar ao agente a lista de portais trabalhando como gateways ativos, os quais serão administrados centralmente e deverá trabalhar com os certificados de autenticação correspondentes a cada usuário. O cliente poderá encontrar a melhor rota com base nos gateways disponíveis e a localização do host, determinando a rota com o tempo de resposta mais rápido.

4.1.20.8. Em conformidade com o perfil de segurança detectado, se o endpoint não for suficientemente seguro, serão determinadas políticas de segurança novas com base no seu perfil. Estas políticas estarão baseadas em: Sistema Operacional e seus níveis de instalação de patches, versão de anti-malware no host, versão de Firewall no host, criptografia do disco, chaves de registros e processos ativos.

4.1.20.9. Deve estabelecer um túnel VPN-SSL do cliente ao Gateway, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-login.

4.1.20.10. Deverá ter suporte aos sistemas operacionais Windows XP, Vista (32 e 64 bits), Windows 7 (32 e 64 bits) e MacOS.

4.1.21. Gerenciamento

4.1.22. Deve ser suportado o gerenciamento por:

4.1.22.1. CLI via SSH

4.1.22.2. WebUI via HTTPS

4.1.22.3. Console

4.1.22.4. API Aberta baseada em REST.

4.1.23. O gerenciamento local do equipamento deve permitir/Possuir:

4.1.23.1. Criação e administração de políticas

4.1.23.2. Administração de políticas de IPS, Antivírus e Anti-Spyware

4.1.23.3. Política de Filtro de Dados e Filtro de URLs.

4.1.23.4. Monitoração de logs.

4.1.23.5. Ferramentas de investigação de logs

4.1.23.6. Debugging

4.1.23.7. Captura de pacotes e geração de arquivos no formato pcap, permitindo integração com ferramentas de análise e diagnóstico.

4.1.23.8. Exportar fluxos de tráfego de dados no formato Netflow, permitindo integração com ferramentas de análise e diagnóstico.

4.1.24. O fabricante deverá possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos distribuídos a partir de um ponto único.

4.1.25. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o trafego que passar pelos gateways de segurança.

4.1.26. Deve possuir relatórios de utilização dos recursos por aplicações, URL, Ameaças, etc.

4.1.27. Prover uma visualização sumarizada de todas as aplicações, ameaças e URLs que passaram pela solução.

4.1.28. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios RealTime.

4.1.29. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.

4.1.30. Deve ser possível exportar os logs CSV.

4.1.31. Deve ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

4.1.32. Deve ser possível capturar as URLs acessadas para todas as sessões HTTP.

4.1.33. Deve possibilitar a criação de diferentes profiles de administração separando pelo menos: Leitura, Alterações, Relatórios e Monitoração.

4.1.34. Deve ser possível, de forma granular, assinar permissões para os administradores criarem outros usuários, alterarem configurações, ler configurações, etc.

4.1.35. Deve ser possível administrar o firewall localmente ou remotamente sem causar problemas de sincronismo de configurações.

4.1.36. Deve possuir interface ethernet "Out-of-Band" para gerenciamento, via:

4.1.36.1. SSH

4.1.36.2. HTTPS

4.1.37. Gerar alertas automáticos via:

4.1.37.1. E-mail

4.1.37.2. SNMP

4.1.37.3. Sysco

4.1.38. Habilidade de upgrade via SCP, TFTP e Web-UI.

4.1.39. Suportar Rollback de configuração para a última configuração salva.

4.1.40. Suportar Rollback de Sistema Operacional para a última versão local.

4.1.41. Suportar validação de regras antes da aplicação.

4.1.42. Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando tiver mais de um administrador executando alterações simultaneamente.

4.1.43. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

4.1.44. Deve possibilitar a integração com soluções de SIEM de mercado (third-party SIEM vendors)

4.1.45. O gerenciamento centralizado deve permitir controle sobre todos os Firewalls em uma única console, com administração de privilégios ou funções.

4.1.46. O gerenciamento centralizado deve possibilitar a instalação como virtual appliance sobre VMware, fornecendo a flexibilidade para instalar-se em diferentes combinações de Hardware e sistemas operacionais.

4.1.47. Administração baseada em Web e Linha de comandos.

4.1.48. Deve suportar autenticação de administradores usando base de dados local e Radius.

4.1.49. Permitir acesso à linha de comandos mediante sessões SSHv2 e telnet

4.1.50. Permitir geração de relatórios de atividades do usuário.

4.1.51. Permitir controle Global de Políticas

4.1.52. Deve suportar organização em grupos de Firewalls: Os sistemas virtuais serão administrados como dispositivos individuais, os grupos podem ser geográficos, por Funcionalidade (por exemplo, como IPS), e distribuição.

4.1.53. Deve suportar objetos e políticas compartilhadas.

4.1.54. Deve possuir relatórios predefinidos e permitir relatórios projetados pelo usuário

4.1.55. Deve permitir exportar todos os relatórios nos formatos CSV e PDF.

4.1.56. Autenticação

4.1.56.1. Para autenticação dos administradores da solução deve ser suportado:

4.1.56.1.1. LDAP

4.1.56.1.2. Radius

4.1.56.1.3. Soluções Baseadas em Token (i.e. Secure-ID)

4.1.56.1.4. Kerberos

4.1.56.2. Para autenticação de VPN SSL deve ser suportado:

4.1.56.2.1. LDAP

4.1.56.2.2. Radius

4.1.56.2.3. Soluções Baseadas em Token (i.e. Secure-ID)

4.1.56.2.4. Kerberos

4.1.57. Captura de pacotes.

4.1.57.1. Deve ser possível a captura de pacotes, como funcionalidade nativa da solução, com geração de arquivos no formato PCAP, por:

4.1.57.1.1. Endereço de Origem

4.1.57.1.2. Endereço de destino

4.1.57.1.3. Aplicações

4.1.57.1.4. Aplicações desconhecidas

4.1.57.1.5. Portas

4.1.57.1.6. IPS

4.1.57.1.7. Antivírus

4.1.57.1.8. Anti-Spyware

4.1.57.1.9. Filtro de dados.

4.1.57.1.10. Qualquer combinação acima.

4.1.58. Relatórios

4.1.58.1. Deve incluir a capacidade de proporcionar um resumo gráfico de aplicações utilizadas e ameaças encontradas diariamente.

4.1.58.2. Deve permitir o controle de transferência de dados não autorizados com ferramenta para realizar padrões definidos por usuário.

4.1.58.3. Deve contar com a funcionalidade para exportação de logs, captura de tráfego URL e ameaças.

4.1.58.4. Deve permitir a criação de relatórios personalizáveis.

4.1.58.5. Deve contar com ferramenta para criar filtros de monitoramento das sessões históricas no firewall seja por aplicação, ip origem e ip destino.

4.1.58.6. Deve ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado.

4.1.58.7. Deve gerar relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição.

4.1.58.8. O equipamento deve proporcionar, no mínimo, os seguintes conjuntos de relatórios:

4.1.58.8.1. Utilização de largura de banda de entrada e saída por aplicação (TOP 10)

4.1.58.8.2. Número de Sessões por aplicação (TOP 10)

4.1.58.8.3. Comparativo semanal de aplicações utilizadas na rede que possam induzir Latência. (TOP 10)

4.1.58.8.4. Taxa de transferência (em bytes) por aplicação (TOP 10).

4.1.58.8.5. Origem e destino do tráfego por aplicação – Usuário (TOP 10)

4.1.58.8.6. Sessões e E-mail público

4.1.58.8.7. Utilização de navegação

4.1.58.8.8. Eventos / Ataques por: Origem, Categoria, Ameaça, Protocolo. (TOP 10)

4.1.58.8.9. Nível de risco da rede

4.1.58.8.10. Principais protocolos e aplicações que circulam pelo Firewall (TOP 25).

4.1.58.8.11. Principais endereços de IP destino por protocolo (TOP 25).

4.1.58.8.12. Os principais endereços IP para cada um dos protocolos e aplicações principais (TOP 50)

4.2. **CARACTERÍSTICAS OBRIGATÓRIAS DO MÓDULO DE ANÁLISE DE REDE.**

4.2.1. A solução deve permitir execução em ambiente virtualizado (instalada como máquina virtual) compatível, no mínimo, com Citrix XenServer e VmWare ESX;

4.2.2. A solução deve permitir uso da infraestrutura de armazenamento de dados do CONTRATANTE, até o limite da licença adquirida;

4.2.3. A solução deve reconhecer nativamente, no mínimo, 1200 aplicações e protocolos;

4.2.4. Deve suportar, no mínimo, as seguintes técnicas de classificação de aplicações e protocolos:

4.2.4.1. Reconhecimento de padrão;

4.2.4.2. Reconhecimento de certificados SSL;

4.2.4.3. Número de protocolo IP;

4.2.4.4. Nome de host;

4.2.4.5. Correlação de sessões;

4.2.4.6. Portas TCP e UDP;

4.2.5. A solução deve ser capaz de realizar armazenamento de dados/metadados capturados da rede;

4.2.5.1. A solução deve ser capaz de gerenciar automaticamente o uso do espaço de armazenamento, no sentido de sobrescrever os dados antigos por dados novos quando o limite de armazenamento for alcançado;

4.2.5.2. A solução deve manter dados, metadados e arquivos de sistema em volumes separados;

4.2.5.3. A solução deve ser capaz de manter metadados mesmo quando os respectivos dados forem sobrescritos no volume de dados, até o limite do espaço de alocação do volume de metadados;

4.2.5.4. A solução deve informar graficamente e textualmente o estado da alocação dos volumes de dados e metadados, incluindo, no mínimo, as seguintes informações:

4.2.5.5. Período de tempo em que estão disponíveis tanto dados quanto metadados;

4.2.5.6. Período de tempo em que estão disponíveis apenas metadados;

4.2.5.7. Deve ser possível visualizar as janelas de tempo em que estão disponíveis dados e metadados, ou apenas metadados, de forma simples, pela interface padrão da solução;

4.2.5.8. Deve ser possível definir uma política fixa de janela de tempo de armazenamento;

4.2.5.9. Deve ser possível definir que dados mais antigos que uma determinada quantidade de dias ou horas sejam automaticamente apagados;

4.2.5.10. A solução deve suportar captura de dados a, no mínimo, 1gbps;

4.2.5.11. Deve ser capaz de realizar captura em mais de um adaptador de rede físico ao mesmo tempo;

4.2.5.12. Deve permitir início ou paralização da captura de cada adaptador físico de forma independente;

4.2.5.13. Deve apresentar estatísticas de captura para cada adaptador, incluindo:

4.2.5.13.1. Quantidade de dados capturados;

4.2.5.13.2. Taxa corrente de captura;

4.2.5.13.3. Taxa máxima de captura;

4.2.5.13.4. Quantidade dados filtrados;

4.2.5.14. Deve ser capaz de agregar adaptadores de rede físicos (até o limite de adaptadores instalados no sistema) em um único adaptador virtual, com controles próprios de início e paralização de captura, assim como apresentação de estatísticas similares a um adaptador físico;

4.2.5.15. Deve suportar nativamente a aplicação de filtros de captura, de modo a permitir a definição de que tipo de tráfego será capturado, incluindo a exclusão da captura de perfis de dados a critério do administrador;

4.2.6. Deve suportar a importação e exportação de filtros de captura;

4.2.7. A solução deve possuir nativamente a funcionalidade de encaminhamento/regeneração/ injeção de tráfego de dados na rede;

4.2.7.1. Deve permitir encaminhamento de tráfego, em tempo próximo a real, capturado em uma ou mais interfaces para outra interface, de modo a possibilitar análises adicionais no tráfego por outras soluções (IDS, Anti-Malware, etc.);

4.2.7.1.1. A funcionalidade de encaminhamento/regeneração de tráfego em rede deve permitir a injeção de tráfego de dados na interface destino com latência inferior a 01 ms, em redes com taxa de transmissão até 10gbps;

4.2.7.2. Deve permitir encaminhamento/reconstrução de tráfego previamente capturado em uma interface, de modo a possibilitar análises adicionais no tráfego por outras soluções (IDS, Anti-Malware, etc.);

4.2.7.2.1. Deve ser possível definir a janela de tempo de dados a ser reconstruída, assim como a aplicação de filtros para controle dos dados a serem injetados na rede via interface destino;

4.2.8. A solução deve permitir a exportação de dados capturados para arquivos no formato PCAP;

4.2.8.1. Deve ser possível definir o tamanho máximo do arquivo PCAP a ser gerado;

4.2.8.2. Deve ser possível definir a janela de tempo de dados a ser exportada para o arquivo PCAP;

4.2.9. A solução deve possuir sistema de firewall próprio, de modo a permitir o controle de acesso às interfaces de administração/operação/análise, assim como serviços correlatos;

4.2.10. A console de administração e análise da solução deve ser padrão WEB, compatível com browsers em plataformas Windows e Linux;

4.2.10.1. A solução deve possuir também console de configuração via linha de comandos;

4.2.10.2. Deve ser possível definir a quantidade máxima de tentativas falhas de logon antes que a conta de usuário seja desabilitada automaticamente;

4.2.10.3. Deve ser possível definir a quantidade máxima de sessões concorrentes de cada usuário no console de administração/análise;

4.2.10.4. Deve permitir aplicação e uso de certificado digital assinado por AC interna do cliente;

4.2.11. Deve possuir sistema de autenticação do tipo RBAC (role-based access control);

4.2.11.1. Deve permitir criação de grupos de usuários com privilégios distintos, com a possibilidade de definição de usuários com perfil de administrador, auditor ou usuário simples;

4.2.11.2. Deve permitir a criação de grupos com privilégios customizados, por meio da granularização de tipos de ações/configurações/privilégios;

4.2.11.3. Deve permitir a definição do escopo de acesso aos dados, por meio de filtro aplicado no perfil do grupo;

4.2.11.4. Deve ser possível criar perfis de acesso com base no tipo de informação a ser analisada, como, por exemplo, usuários com acesso restrito ao protocolo SMTP, ou somente a dados de uma faixa de IPs específica;

4.2.11.5. Os filtros para restrição de conteúdo de visualização devem ser baseados nos metadados utilizados pela solução;

4.2.12. Deve permitir a criação de usuários locais;

4.2.13. Deve permitir autenticação remota, via, no mínimo:

4.2.13.1. LDAP;

4.2.13.1.1. Deve suportar LDAP v2 e v3;

4.2.13.1.2. Deve suportar criptografia na comunicação com o servidor LDAP via TLS ou SSL;

4.2.13.1.3. Deve ser possível definir o escopo de pesquisa no diretório LDAP;

4.2.13.2. RADIUS;

4.2.14. A solução deve possuir nativamente a funcionalidade de autenticação em dois fatores;

4.2.14.1. A habilitação de autenticação em dois fatores deve ser por conta de usuário, ou seja, deve ser possível ter na mesma caixa usuários com ou sem autenticação de dois fatores;

4.2.14.2. Os tokens do segundo nível de autenticação devem ser gerados em aplicação para dispositivos móveis, compatível, no mínimo, com as seguintes plataformas:

4.2.14.2.1. Iphone iOS 3.1.3 ou superior;

4.2.14.2.2. BlackBerry OS 4.5-6.0;

4.2.14.2.3. Android 2.1 ou superior;

4.2.15. A solução deve possuir e ser entregue com mecanismo para mapeamento de endereços IP com contas de usuários do Active Directory da Microsoft;

4.2.16. A solução deve possuir plugin para browsers, de modo a permitir a seleção de endereços IP em páginas web (ou consoles web de soluções de segurança) e disparar diretamente a pesquisa na base de dados da solução;

4.2.17. Deve suportar, no mínimo, os seguintes browsers:

4.2.17.1. Internet Explorer;

4.2.17.2. Firefox;

4.2.17.3. Safari;

4.2.17.4. Chrome;

4.2.18. A solução deve permitir o controle da visualização dos dados capturados via, no mínimo:

4.2.18.1. Janela de tempo definida pelo usuário/analista;

4.2.18.2. Filtro de visualização aplicado pelo usuário/analista, com base em metadados em uso na solução;

4.2.19. A solução deve possuir nativamente sistema de alertas, com base no resultado de análise automatizada dos dados capturados;

4.2.19.1. Os alertas devem ser disparados com base em regras definidas/criadas pelo usuário;

4.2.19.2. As regras de alertas devem utilizar filtros baseados nos metadados em uso na solução, como, por exemplo;

4.2.19.2.1. Tráfego na porta de protocolo DNS, mas o conteúdo não é DNS;

4.2.19.2.2. Tráfego com destino a um site específico;

4.2.19.2.3. Tráfego com origem ou destino a um país específico;

4.2.19.2.4. E-mails de/para determinado usuário;

4.2.19.2.5. Arquivos com um determinado nome;

4.2.19.2.6. Comunicação entre dois endereços IPs;

4.2.19.2.7. Determinados comandos (GET, SET, PUT) enviados a um servidor específico;

4.2.19.3. Deve suportar o uso de operadores lógicos e coringas para criação das regras de alertas e filtros;

4.2.20. A solução de suportar nativamente a importação de regras em padrões abertos de mercado, incluindo, no mínimo:

4.2.20.1. Snort;

4.2.20.2. Dshield;

4.2.21. Deve ser possível enviar alertas via, no mínimo:

4.2.21.1. E-mail;

4.2.21.2. SNMP;

4.2.21.2.1. A solução deve possuir e prover MIBs SNMP para importação em soluções de gerenciamento SNMP;

4.2.21.3. Syslog;

4.2.22. A solução deve permitir nativamente a customização e criação de dashboards para visualização das informações coletadas;

4.2.22.1. Deve ser possível a criação de múltiplos dashboards, de acordo com as preferências de visualização de cada analista;

4.2.22.2. O sistema de múltiplos dashboards deve atender ao conceito de visões específicas, no sentido de montar dashboards para tipos de análises, como, por exemplo:

4.2.22.2.1. Visão de correio eletrônico;

4.2.22.2.2. Visão de aplicações web;

4.2.22.2.3. Visão de camada Ethernet;

4.2.22.2.4. Visão social;

4.2.23. A solução deve possuir mecanismo de filtros de navegação encadeados, com objetivo de reduzir o escopo de pesquisa;

4.2.23.1. Deve permitir aplicação de filtros por meio de cliques de mouse em uma determinada informação;

4.2.23.2. Deve permitir a criação de cadeias de filtros, reduzindo o escopo de pesquisa de acordo com as definições do analista;

4.2.23.3. Esta funcionalidade tem como objetivo (e deve suportar) a navegação intuitiva pelos dados capturados, permitindo ações, como, por exemplo, a seguinte sequência de análise:

4.2.23.3.1. "Mostre o tráfego de dados com destino ao endereço IP 10.1.1.1 na semana passada";

4.2.23.3.2. "Reduza o escopo de visualização para o período entre 10:00hs e 12:00hs da última quinta-feira"

4.2.23.3.3. "Mostre agora apenas protocolo HTTP";

4.2.23.3.4. "Filtre pelo user-agent que contenha a palavra nmap";

4.2.23.3.5. "Remova o último filtro";

4.2.23.3.6. "Reduza o escopo para o tráfego com origem no IP 10.2.2.2";

4.2.23.4. Deve ser possível salvar filtros aplicados como "favoritos", similar à navegação web por browser;

4.2.23.5. Deve permitir reaproveitar os filtros salvos como favoritos como condições de alertas;

4.2.24. A solução deve possuir a capacidade de plotar as sessões capturadas em formato gráfico, e permitir a seleção da janela de tempo a ser visualizada por meio de seleção direta no gráfico (selecionar com o mouse uma parte do gráfico e com isso reduzir a janela de tempo de visualização para aquele período específico);

4.2.24.1. O objetivo desta funcionalidade é permitir ao analista o breve diagnóstico de problemas por meio da combinação de visualização gráfica

com escopo temporal, como, por exemplo, focalizar a visualização no momento em que ocorreu um pico anormal de acessos de uma determinado tipo de aplicação;

4.2.25. A interface de análise e visualização das informações coletadas deve suportar o sistema de Web Widgets (ou equivalente), de modo a permitir sua customização por meio de adição, remoção ou drag-and-drop de widgets;

4.2.25.1. Os widgets devem permitir associação a um determinado tipo de metadado;

4.2.25.2. Os widgets devem permitir customizar a visualização dos dados, no mínimo, pelos seguintes métodos:

4.2.25.2.1. Ordenar a listagem pela quantidade de bytes, pacotes ou sessões;

4.2.25.2.2. Ordenar a listagem em ordem ascendente ou decrescente;

4.2.25.3. Customizar a apresentação dos dados via, no mínimo, os seguintes formatos:

4.2.25.3.1. Tabela;

4.2.25.3.2. Gráfico Pizza;

4.2.25.3.3. Gráfico Coluna;

4.2.25.3.4. Gráfico Barra;

4.2.26. A solução deve possuir sistema de geração de relatórios;

4.2.26.1. Deve permitir a exportação dos relatórios em, no mínimo, formatos PDF e CSV;

4.2.26.2. Deve permitir salvar os relatórios para visualização futura na própria interface da solução;

4.2.26.3. Deve possuir, no mínimo, 40 tipos de relatórios pré-configurados;

4.2.26.4. A geração dos relatórios deve ser dinâmica, com base tanto nos tipos de metadados selecionados, quanto na janela de tempo e filtro aplicados à visualização;

4.2.26.4.1. Essa funcionalidade tem como objetivo (e deve suportar) a criação de relatórios customizados, com base em perguntas como: “Me mostre todos os arquivos que o usuário fulano trafegou na rede durante a manhã de quarta-feira da semana passada”;

4.2.26.5. Deve ser possível aplicações de filtros adicionais nos resultados apresentados, de acordo com o tipo de metadado a ser visualizado;

4.2.26.5.1. Essa funcionalidade tem como objetivo (e deve suportar) a redução customizada do escopo de visualização dos relatórios, com base em perguntas como: “Filtre os resultados mostrando apenas arquivos que cujo nome contenha o termo ´comissão´”;

4.2.27. A solução deve suportar nativamente a comparação dinâmica entre relatórios, de modo a apontar alterações no perfil de tráfego selecionado em janelas de tempos distintas;

4.2.27.1. Deve ser possível determinar as janelas de tempo a serem comparadas;

4.2.27.2. Deve ser possível definir a unidade de medida entre bytes, pacotes e sessões;

4.2.27.3. As mudanças ocorridas entre as janelas de tempo comparadas devem ser apresentadas em formatos gráfico e texto;

4.2.27.4. Deve listar as mudanças por quantidade, e também em percentuais;

4.2.27.5. Deve ser possível demonstrar alterações, como, por exemplo:

4.2.27.5.1. Aumento de x% do tráfego de determinado protocolo em relação ao período anterior;

4.2.27.5.2. Aumento de x para y sessões (ou z%) com destino ao servidor de correio eletrônico pelo usuário fulano;

4.2.28. A solução deve suportar nativamente a reconstrução de arquivos capturados no tráfego de rede;

4.2.29. Deve suportar reconstrução de arquivos capturados, no mínimo, nos seguintes protocolos:

4.2.29.1. HTTP;

4.2.29.2. SMTP;

4.2.29.3. SMB;

4.2.30. Deve suportar reconstrução de, no mínimo, os seguintes tipos de artefatos:

4.2.30.1. Páginas HTML;

4.2.30.2. E-mails EML;

4.2.30.3. Documentos DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, WPD;

4.2.30.4. Mensagens instantâneas AOL, MSN, Yahoo, Jabber;

4.2.30.5. Imagens JPG, BMP, GIF, PNG;

4.2.30.6. Som e Vídeo ASF, AVI, MOV, MPG, WMV, RIFF, FLV, VJPEG, WAW, RA;

4.2.30.7. Arquivos REG, DLL, CONF, CPP, ELF, EXE;

4.2.30.8. Compactados ZIP, GZIP, RAR;

4.2.30.9. Updates RPM;

4.2.31. Deve apresentar graficamente a distribuição dos artefatos reconstruídos na linha de tempo;

4.2.32. Deve permitir filtrar os artefatos reconstruídos por, no mínimo, as seguintes informações:

4.2.32.1. Tipo de arquivo;

4.2.32.1.1. O objetivo dessa funcionalidade é responder a perguntas como: “Mostre apenas os artefatos reconstruídos do tipo HTML”;

4.2.32.2. Extensão do arquivo;

4.2.32.3. Tamanho do arquivo;

4.2.32.4. Conflito entre extensão e tipo de arquivo detectado;

4.2.32.5. Endereço IP de origem ou destino da comunicação;

4.2.32.6. Palavras-chave no conteúdo do artefato;

4.2.32.6.1. Essa funcionalidade tem como objetivo responder a perguntas como: “Filtre os resultados mostrando apenas arquivos que contenham a palavra ´secreto´”;

4.2.32.7. Campos de e-mail:

4.2.32.8. Endereços de origem e destino;

4.2.32.9. Assunto da mensagem;

4.2.32.10. Prioridade da mensagem;

4.2.32.11. Endereços em cópia carbono ou oculta;

4.2.32.12. Valores de hash MD5 e/ou SHA1;

4.2.33. Deve suportar operadores lógicos “e” e/ou “ou” na aplicação dos filtros;

4.2.34. Deve suportar filtros encadeados;

4.2.34.1. Essa funcionalidade tem como objetivo reduzir o escopo de pesquisa, respondendo a perguntas como: “Mostre arquivos do tipo documento, com mais de 50Kb e que contenham a palavra ´secreto´”;

4.2.35. Para cada artefato reconstruído, a solução deve apresentar, no mínimo, os seguintes metadados:

4.2.35.1. Tipo de arquivo apresentado;

4.2.35.2. Tipo de arquivo detectado;

4.2.35.3. Portas TCP/UDP de origem e destino;

4.2.35.4. Extensão do arquivo;

4.2.35.5. Hashes MD5 e SHA1;

4.2.35.6. Fuzzy Hash;

4.2.35.7. URL original;

4.2.35.8. Host de origem;

4.2.35.9. Endereços IP de origem e destino;

4.2.35.10. Tamanho do artefato;

4.2.36. No caso de reconstrução de e-mails, deve apresentar também os metadados:

4.2.36.1. Endereços de origem e destino;

4.2.36.2. Assunto da mensagem;

4.2.36.3. Arquivos em anexo;

4.2.37. Deve possuir painel de visualização de arquivos de media, permitindo rápida identificação visual do conteúdo de determinadas sessões capturadas na rede;

4.2.38. Deve ser capaz de apresentar thumbnails dos arquivos reconstruídos;

4.2.39. Deve ser capaz de realizar um “zoom” no arquivo original quando o analisa clica sobre o thumbnail;

4.2.40. Deve incluir, na visão ampliada, no mínimo, as seguinte informações referentes ao artefato:

4.2.40.1. Endereços IP de origem e destino;

4.2.40.2. URL;

4.2.40.3. Tamanho do arquivo;

4.2.40.4. MIME Type;

4.2.41. A solução deve suportar nativamente a funcionalidade de Fuzzy Hash, de modo a permitir a busca por arquivos semelhantes com base no Fuzzy Hash calculado para cada artefato reconstruído;

4.2.41.1. Essa funcionalidade tem como objetivo (e deve suportar) perguntas do tipo: “Mostre todos os arquivos semelhantes a este documento”;

4.2.42. Para cada artefato reconstruído, a solução deve prover, no mínimo, as seguintes ações:

4.2.42.1. Prever o conteúdo do arquivo na interface da solução, em formato próximo ao original;

4.2.42.2. Permitir o download do artefato para a estação de trabalho do analista;

4.2.42.3. Analisar detalhadamente sessão em que o artefato foi capturado em formato PCAP, pacote a pacote, em estilo Wireshark;

4.2.42.4. Permitir o download do arquivo PCAP para a máquina do analista, para ser analisado por outras soluções;

4.2.42.5. Submeter o artefato para análise de reputação, para, no mínimo, as seguintes fontes de informações:

4.2.42.5.1. SANS ISC (para hash do arquivo, endereço de origem e hostname);

4.2.42.5.2. Google Safe Browse;

4.2.42.5.3. Whois nos endereços de origem e destino;

4.2.42.5.4. SORBS DNSL;

4.2.42.5.5. ClamAV (hash do arquivo);

4.2.43. A solução deve suportar nativamente a execução de ações em consequência do "match" de filtros pré-configurados;

4.2.43.1. Deve permitir, no mínimo, os seguintes tipos de ações:

4.2.43.1.1. Alertas via:

4.2.43.1.2. E-mail;

4.2.43.1.3. SNMP;

4.2.43.1.4. Syslog;

4.2.43.2. Exportação do arquivo PCAP referente à sessão capturada para um servidor remoto;

4.2.43.3. Exportação do fluxo (Netflow) para um servidor IPFIX remoto;

4.2.43.4. Envio do artefato para análise um serviço de reputação; Deve suportar, no mínimo, os seguintes serviços:

4.2.43.4.1. VirusTotal (www.virustotal.com, via API do serviço);

4.2.43.4.1.1. Análise de quantidade de arquivos superior a 1000 artefatos mensais depende de aquisição prévia de licença de uso);

4.2.43.4.2. Jsunpack-n;

4.2.43.4.3. Cuckoo (análise de sandbox);

4.2.43.4.4. Envio para servidor FTP remoto;

4.2.43.4.5. FireEye (para análise de ameaças avançadas. O CONTRATANTE precisa ter a solução FireEye em sua rede corporativa para usar essa funcionalidade);

4.2.43.4.6. LastLine (depende de aquisição prévia de licença de uso do serviço);

4.2.43.4.7. Portable Executable Scanner (apara análise de arquivos maliciosos, em uma escala de 1 a 10);

4.2.44. A solução deve possuir nativamente ferramenta e interface própria de geolocalização de endereços IP;

4.2.44.1. Deve ser capaz de plotar os endereços IP encontrados no tráfego de rede capturado em mapa na própria interface da solução;

4.2.44.2. Deve ser capaz de representar a quantidade de dados transferidos de/para um determinado IP graficamente, pelo símbolo usado para plotar a posição geográfica;

4.2.44.3. Deve possuir mecanismo de navegação pelo mapa, incluindo zoom geral, e ampliação de áreas específicas;

4.2.44.4. Deve permitir salvar visões específicas do mapa para agilizar visualizações posteriores;

4.2.44.4.1. Deve permitir, por exemplo, salvar uma visão com o zoom e foco no mapa do Brasil;

4.2.44.4.2. Deve ser possível ao analista escolher qual visão previamente salva utilizar para visualizar o mapa;

4.2.44.5. Deve ser capaz de listar os endereços IP referentes à visão gráfica do mapa.

4.2.44.5.1. A lista de endereços IP deve ser dinâmica, ou seja, deve ser atualizada de acordo com a visão gráfica. Caso o analista efetue um zoom em determinada área do mapa, a lista deve ser atualizada automaticamente para mostrar apenas endereços IP referentes à área do mapa em destaque;

4.2.44.6. Deve permitir ao administrador da solução definir nomes e posições geográficas (latitude e longitude) de redes internas da organização (redes e subredes contidas no espaço de endereços reservados: 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16);

4.2.44.6.1. As redes e subredes internas configuradas com nome e posição geográfica devem passar a ser listadas na interface de geolocalização, conforme exemplo a seguir:

4.2.44.6.1.1. Nome: Regional São Paulo;

4.2.44.6.1.2. Faixa de Endereços: 10.11.0.0/16;

4.2.44.6.1.3. Localização: -23.548943, -46.638818;

4.2.44.7. Deve permitir a localização no mapa das unidades regionais da organização, assim como a identificação de todos os endereços IP capturados referentes a cada unidade;

4.2.44.7.1. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista mapear de forma dinâmica e simplificada endereços IP internos com sua respectiva localização geográfica, de modo a responder perguntas recorrentes em análises, tais como:

4.2.44.7.2. “Mostre as unidades regionais e respectivos endereços IP em uso dessa determinada região do mapa”;

4.2.44.7.3. “De qual unidade regional é esse endereço IP?”;

4.2.44.8. Deve permitir a aplicação de filtros nos resultados de cada visualização geográfica, com, no mínimo, os seguintes filtros:

4.2.44.8.1. Quantidade de bytes;

4.2.44.8.2. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista listar somente endereços que trafegaram na rede determinadas quantidades de dados;

4.2.44.8.3. Contagem de endereços IP;

4.2.44.8.4. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista listar somente localidades com determinada quantidade de endereços IP gerando tráfego;

4.2.44.8.5. Localização;

4.2.44.8.6. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista listar somente endereços de uma determinada localidade (tanto as pré-existentes no mapa, quanto as criadas na solução para mapear unidades da organização);

4.2.44.8.7. Deve permitir o encadeamento de filtros (com operadores “e” ou “ou”), permitindo aplicação de filtros mais específicos/avançados;

4.2.44.8.8. O fabricante da solução deve prover ferramenta própria online para auxiliar a localização das coordenadas e latitude e longitude de cada unidade geográfica;

4.2.45. A solução deve prover nativamente estatísticas de uso em sua interface;

4.2.45.1. Deve prover estatísticas detalhadas de:

4.2.45.1.1. Uso de rede (captura de dados);

4.2.45.1.2. Uso de disco por interface;

4.2.45.1.3. Consumo de CPU e memória;

4.2.46. A solução deve possuir nativamente sistema de auditoria;

4.2.46.1. Deve ser capaz de registrar login e logoff de usuários, contendo data, horário e endereço IP de origem da conexão;

4.2.46.2. Deve ser capaz de registrar as pesquisas realizadas pelo usuário na solução, incluindo janelas de tempo e metadados/dados acessados;

4.2.46.3. Deve permitir aplicação de filtros no conteúdo dos registros de auditoria, com busca por, no mínimo, os seguintes campos:

4.2.46.3.1. Categoria do evento;

4.2.46.3.2. Tipo de evento;

4.2.46.3.3. Prioridade do evento;

4.2.47. A solução deve possuir funcionalidades para uso em ambientes distribuídos, com diversos pontos de captura e análise;

4.2.48. Deve permitir integração com console central de gerenciamento, fornecida pelo mesmo fabricante;

4.2.49. A solução deve possuir nativamente a capacidade de analisar detalhadamente os dados capturados em formato pacote a pacote, com interface similar a ferramentas como Wireshark;

4.2.50. A interface de análise detalhada de pacotes deve permitir aplicação de filtros com sintaxe Wireshark;

4.2.51. A solução deve possuir nativamente funcionalidades para integração com outras soluções de segurança e análise de rede;

4.2.51.1. Deve possuir API REST, baseada em Web Services;

4.2.51.2. Deve permitir pivoteamento automático entre consoles de soluções de segurança para análise detalhada de dados;

4.2.51.2.1. Essa funcionalidade tem como objetivo (e deve suportar) permitir ao analista iniciar a análise de um incidente pela interface de outros produtos (como Firewall ou SIEM), e com apenas um clique de mouse acionar a console da solução, mostrando dados já contextualizados com as informações de origem;

4.2.51.2.2. Um exemplo de uso dessa funcionalidade seria iniciar a análise de um incidente via console de um Firewall/IPS/SIEM, identificar o endereço IP interno alvo do ataque, e realizar por meio de um clique a pesquisa na solução já referenciada com o IP em questão (fundamental para levantamento de impacto de eventuais incidentes de segurança).

4.2.51.2.2.1. Deve ser capaz de responder aos seguintes tipos de pergunta:

4.2.51.2.2.2. “Mostre tudo que esse endereço fez em minha rede interna”;

4.2.51.2.2.3. “Mostre agora o que essa máquina fez na minha rede após ter sido infectada”;

4.2.52. A solução deve possuir sistema de arquivos próprio, desenvolvido especificamente para uso em captura e análise de dados de rede;

4.3. **CARACTERÍSTICAS OBRIGATÓRIAS DO MÓDULO DE VISIBILIDADE E ANÁLISE DE DADOS.**

4.3.1. A distribuição dos módulos da solução pelo ambiente computacional do CONTRATANTE deve ser livre, no sentido de permitir sua distribuição pelo ambiente sem a necessidade de licenças adicionais, dentro do limite de processamento e indexação licenciados, conforme item requisitos de capacidade e performance;

4.3.1.1. Deve ser possível ao CONTRATANTE, portanto, distribuir o volume contratado (requisitos de capacidade e performance) pelo seu ambiente, de acordo com a demanda da cada unidade/regional/subrede/rede remota;

4.3.1.1.1. Deve ser possível ao CONTRATANTE, por exemplo, distribuir uma hipotética licença de 100gb em três pontos de sua rede, sendo, neste exemplo, 80gb para o ponto central, e os restantes 20gb alocados em 10gb para cada localidade regional remota de menor porte;

4.3.1.2. A distribuição dos módulos pelo ambiente do CONTRATANTE depende da disponibilização de infraestrutura de hardware e software pelo CONTRATANTE, de acordo com os requisitos e compatibilidades descritos nas especificações;

4.3.2. Não deve haver limite de licenciamento para quantidade de usuários simultâneos acessando qualquer elemento da solução, incluindo interface/console web;

4.3.3. A solução deve possuir sistema de auditoria de uso;

4.3.3.1. Cada evento de auditoria deve possuir, no mínimo, os seguintes campos:

4.3.3.2. Data e horário da ação executada pelo usuário;

4.3.3.3. Identificação do usuário que executou a ação;

4.3.3.4. Informação sobre a ação executada;

4.3.3.5. Identificador sequencial do evento;

4.3.3.6. Assinatura do evento (hash criptográfico), para garantir a integridade das informações;

4.3.4. A solução deve suportar e permitir implantação em modelos de balanceamento de carga e tolerância a falhas;

4.3.4.1. A solução deve permitir o crescimento/expansão horizontal no ambiente do CONTRATANTE mediante adição de novos módulos em cada camada;

4.3.4.1.1. O crescimento/expansão horizontal da solução depende da disponibilização de infraestrutura de hardware e software pelo CONTRATANTE, de acordo com os requisitos e compatibilidades descritos nas especificações;

4.3.4.2. Os módulos de tratamento e encaminhamento de eventos devem suportar e permitir a configuração em que os eventos são encaminhados para mais de um servidor de indexação, visando balancear a carga, prover tolerância a falhas e permitir crescimento horizontal da solução no ambiente;

4.3.4.2.1. O balanceamento de carga no encaminhamento de eventos deve ser automatizado;

4.3.4.3. Os Módulos de Indexação devem suportar e permitir configuração em modo cluster, para tolerância a falhas;

4.3.4.3.1. Os módulos em modo cluster devem sincronizar seus dados;

4.3.4.4. A solução não deve exigir licenças adicionais (além do listado nos requisitos de capacidade e performance) para configuração em alta disponibilidade;

4.3.4.4.1. A implantação dos módulos em modo cluster depende da disponibilização de infraestrutura de hardware e software pelo CONTRATANTE, de acordo com os requisitos e compatibilidades descritos nas especificações;

4.3.5. Requisitos para os Módulos de Tratamento e Encaminhamento de eventos:

4.3.5.1. Os módulos para tratamento e encaminhamento de eventos devem suportar, no mínimo, as seguintes plataformas:

4.3.5.1.1. Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012;

4.3.5.1.2. Windows XP, Vista, 7 e 8;

4.3.5.1.3. Linux Kernel 3.0+, 32 e 64 bits;

4.3.5.1.4. Linux Kernel 2.6+, 32 e 64 bits;

4.3.5.1.5. Linux Kernel 2.4+, 32 bits;

4.3.5.1.6. FreeBSD 7 e 8, 32 e 64 bits;

4.3.5.1.7. Mac OS X 10.5 e 10.6;

4.3.5.1.8. Mac OS X 10.7 e 10.8 em plataforma Intel;

4.3.5.1.9. Solaris 8, 9 10 e 11;

4.3.5.1.10. AIX 5.3, 6.1 e 7.1;

4.3.5.1.11. HP/UX 11i v2 e v3;

4.3.5.2. Os módulos de tratamento e encaminhamento de eventos devem suportar, no mínimo, os seguintes sistemas de arquivos (por plataforma):

4.3.5.2.1. Linux ext2/3/4, reiser3, XFS, NFS 3/4;

4.3.5.2.2. Solaris UFS, ZFS, VXFS, NFS 3/4;

4.3.5.2.3. FreeBSD FFS, UFS, NFS 3/4, ZFS;

4.3.5.2.4. Mac OS X HFS, NFS 3/4;

4.3.5.2.5. AIX JFS, JFS2, NFS 3/4;

4.3.5.2.6. HP-UX VXFS, NFS 3/4;

4.3.5.2.7. Windows NTFS, FAT32;

4.3.5.3. A solução deve possuir módulo para testar a compatibilidade e viabilidade de execução em sistemas de arquivos não listados na lista de compatibilidade;

4.3.5.4. Os módulos de tratamento e encaminhamento de eventos devem possuir, no mínimo, as seguintes funcionalidades;

4.3.5.4.1. Criptografia dos dados a serem enviados a outros módulos da solução;

4.3.5.4.2. Compressão dos dados coletados;

4.3.5.4.3. Capacidade de enviar os dados em qualquer porta disponível;

4.3.5.4.4. Coletar eventos locais ou remotos;

4.3.5.4.5. Receber dados de outros módulos de tratamento e encaminhamento, em topologia hierarquizada;

4.3.5.4.6. Balanceamento de carga no encaminhamento dos eventos;

4.3.5.4.7. Encaminhamento de dados para outras soluções de análise de eventos;

4.3.5.4.8. Controle do encaminhamento de dados, com retransmissão no evento de perda de dados durante a transferência via rede;

4.3.5.4.9. Indexação prévia dos eventos;

4.3.5.5. Os módulos de tratamento e encaminhamento de eventos não devem exigir licenças adicionais, ou seja, seu uso e distribuição no ambiente deve ser livre, desde que o módulo principal da solução esteja licenciado, de acordo com requisitos de capacidade e performance;

4.3.6. A solução deve indexar os dados recebidos, e prover interface para busca nos dados indexados;

4.3.7. Deve permitir o uso de coringas (wildcards);

4.3.8. Deve permitir o uso de operadores booleanos (AND, OR, NOT);

4.3.9. Deve permitir a construção de buscas complexas com uso de parênteses para agrupar termos e expressões;

4.3.10. Deve possuir assistente de busca;

4.3.10.1. O assistente de busca deve surgir automaticamente quando o usuário executa uma busca;

4.3.10.2. Deve prover apoio ao usuário, indicando possíveis erros de sintaxe, assim como trechos da documentação com dicas para execução da busca em questão;

4.3.10.3. Deve apresentar resumo dos “matches” parciais referentes à expressão e busca, como, por exemplo:

4.3.10.3.1. Caso o usuário busque a palavra “test”, o assistente de busca deve ser capaz de mostrar a quantidade de “matches” exatos, assim como das palavras que contenham o termo, tais como “testar”, “testando”, “testes”, “teste”;

4.3.10.3.2. O resumo de “matches” deve ser baseado em hyperlinks, ou seja, deve ser possível ao usuário clicar em uma das opções e iniciar outra busca a partir do termo clicado;

4.3.11. Os resultados das buscas devem apresentar o termo de busca em destaque (highlight);

4.3.12. A solução deve indicar quais os campos que mais apareceram nos resultados da busca;

4.3.13. Deve permitir selecionar a janela de tempo em que a busca será realizada;

4.3.14. Deve permitir buscas em janelas de tempo padrão previamente configuradas, tais como:

4.3.14.1. Última hora;

4.3.14.2. Últimos 15 minutos;

4.3.14.3. Últimas 24 horas;

4.3.14.4. Últimos 30 dias;

4.3.14.5. Hoje;

4.3.14.6. Semana até data atual;

4.3.14.7. Ano até dia data atual;

4.3.15. Deve permitir executar as buscas em tempo real, com atualização dinâmica dos resultados;

4.3.15.1. Deve permitir ao usuário selecionar o tempo de atualização dos resultados, desde o tempo real propriamente dito (na medida em que os eventos forem recebidos pela solução) até janelas maiores, de minutos ou mesmo uma hora;

4.3.16. Deve permitir customizar a janela de tempo de buscas,

4.3.17. Deve possuir mecanismos de controle da busca, com, no mínimo, as seguintes funções:

4.3.17.1. Enviar a busca para segundo plano (permitindo ao usuário iniciar outras buscas enquanto a primeira está sendo processada);

4.3.17.2. Pausar/reiniciar a busca;

4.3.17.3. Terminar a busca (os resultados parciais até o momento devem ser apresentados);

4.3.17.4. Cancelar a busca;

4.3.17.5. Imprimir os resultados;

4.3.17.6. Inspecionar a execução da busca, de modo a apresentar detalhes em modo real da execução da busca na solução;

4.3.18. Deve apresentar, junto com os resultados da busca, o referente gráfico de linha de tempo de modo a informar a distribuição dos resultados pelo tempo;

4.3.18.1. Deve permitir ao usuário selecionar com o ponteiro de mouse uma determinada janela de tempo de resultados diretamente a partir do gráfico de linha de tempo;

4.3.18.2. Deve apresentar picos e vales de quantidade de resultados na linha de tempo, de modo a demonstrar visualmente situações como picos de acessos, ou paradas de serviços;

4.3.18.3. Deve possuir controles de linha de tempo, permitindo, no mínimo:

4.3.18.3.1. Efetuar "zoom" a uma determinada parte da janela de tempo apresentada (ir de uma janela representada por meses, por exemplo, para determinados dias, ou de dias para horas, até);

4.3.18.3.1.1. O gráfico de linha de tempo deve ser dinamicamente reconstruído após aplicação de "zoom", de modo a reduzir o escopo de visualização somente à janela de tempo selecionada;

4.3.18.3.1.2. Deve permitir aplicação de "zoom", de modo a reduzir o escopo temporal até a casa de milissegundos;

4.3.18.3.1.2.1. O usuário deve ser capaz, por exemplo, de iniciar uma busca genérica, apresentando os resultados em escala de tempo de anos, e a partir daí aplicar o "zoom" diretamente no gráfico da linha de tempo repetidamente, alterando a escala da linha de tempo até mostrar os resultados dentro de um determinado segundo, distribuídos entre os respectivos milissegundos;

4.3.18.3.2. Remover o "zoom" aplicado, voltando passo a passo conforme a quantidade de reduções de escopo aplicadas;

4.3.18.3.3. Voltar à janela de tempo original;

4.3.19. A solução deve possuir linguagem para construção de expressões complexas de busca;

4.3.19.1. Deve possuir, no mínimo, comandos capazes de:

4.3.19.1.1. Ordenar os resultados (sort) por determinados campos;

4.3.19.1.2. Filtrar os resultados;

4.3.19.1.3. Deve suportar duplicação;

4.3.19.1.4. Deve suportar comando do tipo “onde” (where);

4.3.19.1.4.1. Deve suportar pesquisas do tipo: “Mostre todos os arquivos baixados na internet onde o tamanho do arquivo é maior que 200 mb”;

4.3.19.2. Deve suportar comandos de início e fim de resultados (head e tail);

4.3.19.3. Gerar gráficos e relatórios com base nos resultados;

4.3.19.4. Deve suportar comando para listar maior e menor quantidade de resultados (top e rare);

4.3.19.5. Deve suportar comando para gerar gráfico com base nos resultados;

4.3.19.5.1. Deve ser possível, por exemplo, executar comandos do tipo: “Plote em um gráfico a média de uso de CPU de cada servidor da DMZ por minuto”;

4.3.19.5.2. Deve suportar comando para gerar estatísticas com base nos resultados;

4.3.19.5.3. Deve ser possível, por exemplo, executar um comando do tipo: “Mostre a taxa média de transmissão de dados para cada servidor da DMZ”;

4.3.19.6. Agrupar resultados em transações;

4.3.19.6.1. Deve suportar comandos do tipo: “Agrupe os eventos resultantes da pesquisa que possuem o mesmo endereço IP de origem e que aconteceram com intervalo máximo de 10 segundos”;

4.3.19.7. Modificar os resultados;

4.3.19.7.1. Deve suportar comando para adicionar campos ao resultado;

4.3.19.7.2. Deve suportar comando para substituir campos do resultado;

4.3.19.7.3. Deve suportar comandos para adicionar campos aos resultados com base em operações, comparações ou cálculos matemáticos;

4.3.19.7.3.1. Deve ser possível, por exemplo, executar um comando do tipo: “Adicione o campo Velocidade_Média aos resultados, em que Velocidade_Média equivale à divisão do campo Distância pelo campo Tempo”;

4.3.19.8. Deve suportar o uso de expressões regulares para extração de campos;

4.3.19.9. Deve suportar sintaxe padrão “sed” para extração e transformação de campos;

4.3.19.9.1. Deve ser possível, por exemplo, executar uma expressão sed para trocar todos os números de CPF dos resultados por uma máscara anônima, tal como XXX.XXX.XXX-XX;

4.3.19.10. Deve ser possível transformar os resultados com uso de arquivos ou scripts;

4.3.19.10.1. Deve ser possível, por exemplo, executar um comando na busca que use um script de resolução de nomes para resolver todos os endereços IP de um determinado campo para os respectivos nomes de host;

4.3.20. A solução deve prover linguagem própria de modificadores de tempo, para uso em buscas complexas;

4.3.20.1. Deve possuir termos para referenciar unidades de tempo, tais como:

4.3.20.1.1. “s” para segundos;

4.3.20.1.2. “m” para minutos;

4.3.20.1.3. “h” para hora;

4.3.20.1.4. “d” para dia”;

4.3.20.2. Deve permitir referenciar os termos de unidades de tempo, de modo a construir janelas de tempo tais como (por exemplo):

4.3.20.2.1. Trazer resultados a partir da última hora;

4.3.20.2.2. Trazer resultados dos últimos 22 minutos;

4.3.20.2.3. Trazer resultados entre 22 e 23 horas de ontem;

4.3.20.2.4. Trazer resultados dos últimos 2 meses;

4.3.21. A interface de busca deve permitir adicionar novos termos de busca com base nos resultados da busca anterior;

4.3.21.1. Deve permitir ao usuário adicionar novos termos de busca com um clique de mouse sobre palavras ou campos do resultado;

4.3.21.2. Deve permitir a remoção dos novos termos adicionados mediante novo clique no mesmo termo;

4.3.22. A solução deve permitir exportar os resultados das buscas;

4.3.22.1. Deve ser possível limitar a quantidade de resultados a serem exportados;

4.3.22.2. De suportar, no mínimo, os seguintes formatos para exportação:

4.3.22.2.1. CSV;

4.3.22.2.2. XML;

4.3.22.2.3. JSON;

4.3.22.2.4. Raw data (formato original);

4.3.23. A solução deve permitir ao usuário salvar os resultados de uma busca na própria solução;

4.3.23.1. O resultado salvo deve ficar disponível para consultas futuras;

4.3.24. A solução deve permitir ao usuário salvar e compartilhar os resultados de uma busca com outros usuários da solução;

4.3.24.1. A solução deve prover a URL de referência do resultado salvo, visando facilitar a troca de informações;

4.3.25. A solução deve permitir ao usuário salvar os resultados de uma busca em formato PDF;

4.3.26. A solução deve permitir ao usuário salvar uma busca (salvar o termo de busca);

4.3.26.1. Deve ser possível definir, no momento de salvar o termo de busca, se é uma busca privada (exclusiva do usuário), ou se é passível de compartilhamento com outros usuários da solução;

4.3.26.2. A solução deve prover uma URL de acesso direto à busca salva, visando facilitar a troca de informações;

4.3.26.3. A solução deve possuir a funcionalidade de listar para o usuário somente as buscas às quais ele possui permissão de acesso/execução;

4.3.26.4. A solução deve diferenciar graficamente as buscas privadas das compartilhadas;

4.3.26.5. Deve permitir a edição de buscas previamente salvas;

4.3.27. A solução deve possuir nativamente a funcionalidade de definir agendamentos de execução de buscas;

4.3.27.1. Deve ser possível ao usuário definir os critérios de agendamento, incluindo, no mínimo:

4.3.27.1.1. Nome do agendamento;

4.3.27.1.2. Intervalos de tempo de execução (a cada hora, a cada dia, de 6 em 6 horas, etc.);

4.3.27.1.3. A janela de tempo da busca (últimos 60 minutos, último dia, etc.);

4.3.27.2. Deve ser possível ao usuário definir ações ao término da execução da busca agendada, incluindo, no mínimo:

4.3.27.2.1. Envio de e-mail com os resultados;

4.3.27.2.2. Execução de um script;

4.3.27.3. Deve ser possível ao usuário compartilhar um agendamento de busca com outros usuários da solução;

4.3.28. A solução deve possuir funcionalidade de "throttling", no sentido de reduzir a frequência das ações disparadas pela execução da busca;

4.3.29. Deve ser possível ao usuário configurar regras para reduzir a frequência de envio de alertas resultantes de uma mesma busca em um determinado intervalo de tempo;

4.3.30. A solução deve permitir ao usuário visualizar estatísticas em tempo real com base nos resultados das buscas;

4.3.31. Deve ser possível ao usuário escolher um determinado campo dos eventos resultantes da busca, como, por exemplo, o campo "usuário", e obter/gerar de imediato, no mínimo, as seguintes informações:

4.3.31.1. Lista baseada no conteúdo do campo (os nomes dos usuários, no exemplo), com a respectiva quantidade de ocorrências, percentual com base no total, e demonstração gráfica referente ao percentual de cada conteúdo em face ao total;

4.3.31.1.1. O objetivo dessa funcionalidade (que a solução deve prover) é permitir ao analista, diante de um resultado de busca que pode ter milhares de entradas, obter rapidamente informações tais como: "de todas as tentativas com falha de autenticação encontradas, quais usuários geraram mais eventos?".

4.3.32. Possibilidade de gerar gráficos com base no campo selecionado;

4.3.32.1. O objetivo dessa funcionalidade (que a solução deve prover) é permitir ao analista, diante de um resultado de busca que pode ter milhares de entradas, plotar graficamente informações tais como: "de todas as tentativas com falha de autenticação encontradas, quais usuários geraram mais eventos?".

4.3.33. No caso de busca por endereços/redes IP, a solução deve suportar nativamente o uso de formato CIDR, e também de coringas;

4.3.33.1. Deve ser possível ao usuário realizar pesquisas do tipo: 192.168.1.0/24, ou 192.168.1.* para referencias todos os endereços da rede 192.168.1.0/24;

4.3.34. A solução deve permitir o uso de arquivos nos termos/sintaxe de buscas;

4.3.34.1. Deve ser possível usar termos contidos em um arquivo para realizar as buscas;

4.3.34.2. Deve ser possível usar os termos contidos nos arquivos em modo de inclusão ou exclusão da busca;

4.3.35. A solução deve prover a funcionalidade de “sub buscas”, em que os resultados de uma busca são usados como argumento para outra busca;

4.3.36. A solução deve possuir a funcionalidade de reduzir o tempo de resposta de determinadas buscas e/ou relatórios;

4.3.36.1. Deve ser possível acelerar determinadas buscas e/ou relatórios, principalmente os executados sobre uma massa de dados muito grande;

4.3.36.2. A solução deve ser capaz de executar processos em background, de forma constante, para reduzir o tempo de resposta das busca/relatórios aceleradas assim definidas pelo usuário;

4.3.37. A solução deve possuir gerenciador de tarefas executadas ou em execução (incluindo buscas);

4.3.37.1. Usuários com privilégio de administração devem ser capazes de visualizar as tarefas executadas por todos os usuários da solução;

4.3.37.2. O gerenciador de tarefas deve listar todas as tarefas, ou discriminar a visualização por, no mínimo, os seguintes status:

4.3.37.2.1. Já finalizadas;

4.3.37.2.2. Em execução;

4.3.37.2.3. Em pausa;

4.3.37.3. Deve ser possível revisar tarefas executadas, mesmo que estas não tenham sido salvas, enquanto constarem no console do gerenciador de tarefas;

4.3.37.4. Deve ser possível determinar o tempo máximo em que as tarefas continuem a aparecer no console do gerenciador de tarefas (definição de prazo para expiração);

4.3.37.5. A console do gerenciador de tarefas deve mostrar o prazo de expiração de cada tarefa listada;

4.3.37.6. A console do gerenciador de tarefas deve mostrar para cada tarefa lista, no mínimo:

4.3.37.6.1. Data e horário em que a tarefa foi iniciada;

4.3.37.6.2. Usuário dono da tarefa;

4.3.37.6.3. Em qual aplicação interna (ambiente pré-configurado) a tarefa foi iniciada;

4.3.37.6.4. Qual a quantidade de eventos retornados pela tarefa;

4.3.37.6.5. Prazo de expiração;

4.3.37.6.6. Status;

4.3.37.7. Deve ser possível pausar ou finalizar tarefas em execução;

4.3.38. A solução deve possuir funcionalidade de compartilhamento de objetos criados;

4.3.38.1. Deve ser possível compartilhar entre usuários da solução, no mínimo, os seguintes tipos de objetos:

4.3.38.1.1. Buscas salvas;

4.3.38.1.2. Relatórios;

4.3.38.1.3. Tipos de eventos;

4.3.38.1.4. Campos de extração;

4.3.38.1.5. Identificadores;

4.3.38.1.6. Dashboards;

4.3.39. A solução deve ser capaz de automaticamente extrair pares campo/valor dos dados analisados, visando simplificar a interpretação das informações;

4.3.40. A solução deve ser capaz de classificar as informações, com base em agrupamentos de eventos em tipos, e também em transações, no caso de coleções de eventos conceitualmente relacionados em uma determinada janela de tempo;

4.3.41. A solução deve ser capaz de adicionar campos aos dados com base em informações coletadas de fontes externas.

4.3.42. A solução deve permitir ao usuário aplicar “tags” e identificadores para agrupar determinados tipos de dados;

4.3.42.1. Deve ser capaz de aplicar múltiplos identificadores a um mesmo tipo de dados;

4.3.42.2. Deve ser possível, por exemplo, identificar um determinado servidor com as tags “Regional_São_Paulo” e “Servidor_Web”;

4.3.42.3. A solução deve permitir o uso das tags nas pesquisas;

4.3.42.4. Deve ser possível, por exemplo, procurar um determinado termo em todos os servidores marcados com a tag “Servidor_Web”;

4.3.43. A solução deve possuir a funcionalidade de criação de Tipos de Eventos, de modo a categorizar determinados resultados que sejam importantes;

4.3.43.1. Deve ser possível ao analista, por exemplo, executar uma busca que agregue vários tipos de tentativas de acesso indevido a servidores, e então salvar esse tipo de resultado como “Acessos_Indevidos”, para posterior uso em novas buscas;

4.3.43.2. Deve ser possível ao analista, por exemplo, diferenciar entre as tentativas de acesso indevido aquelas com origens interna ou externa, com nomes como “Acessos_Indevidos_Externos” e “Acessos_Indevidos_Externos”;

4.3.43.3. A partir da definição/criação de Tipos de Eventos, estes passam a ser referenciados em todas as buscas feitas na solução, apresentando estatísticas quando ocorrerem “matches”;

4.3.43.3.1. Esta funcionalidade deve permitir, por exemplo, que numa pesquisa genérica para listar todos os eventos de um determinado servidor, seja possível identificar visualmente e rapidamente quantos “Acessos_Indevidos_Externos” ou “Acessos_Indevidos_Externos” foram tentados no servidor, mesmo que o objetivo inicial da busca fosse encontrar outras informações;

4.3.44. Deve ser possível a aplicação de Tags ou identificadores a Tipos de Eventos;

4.3.45. Deve ser possível ao usuário compartilhar Tipos de Eventos criados com outros usuários da solução;

4.3.46. A solução deve ser capaz de monitorar elementos do ambiente (ativos, dispositivos de rede, aplicações, sistemas, servidores, etc.) em tempo real, com base nos eventos gerados pelos elementos e permitir a geração de alertas com base em condições pré-definidas;

4.3.46.1. Deve ser possível disparar (com base na configuração do alerta), no mínimo, as seguintes ações:

4.3.46.1.1. Enviar um e-mail;

4.3.46.1.2. Executar um script;

4.3.46.1.3. Deve ser possível abrir tickets em soluções de gerenciamento de incidentes via scripts;

4.3.46.1.4. Mostrar alerta no console de gerenciamento de alertas da solução;

4.3.46.1.5. Adicionar a um feed RSS;

4.3.46.1.6. Enviar alerta via SNMP;

4.3.46.2. Deve ser possível definir o nível de severidade do alerta;

4.3.46.3. A solução deve possuir interface exclusiva para gerenciamento, visualização e análise dos alertas gerados;

4.3.46.3.1. Deve ser possível, na criação do alerta, definir se este constará ou não na console de alertas;

4.3.46.4. Deve ser possível definir alertas com base, no mínimo, nas seguintes situações:

4.3.46.4.1. Alertas em tempo real, disparado assim que o evento em questão é recebido na solução;

4.3.46.4.2. Alertas em tempo real baseados em uma determinada quantidade de eventos de um determinado tipo recebidos dentro de uma determinada janela de tempo;

4.3.46.4.2.1. Um exemplo seria enviar um alerta apenas após receber a terceira tentativa errada de logon de um usuário dentro de uma janela de tempo de 03 minutos;

4.3.46.5. Deve suportar, no mínimo, os seguintes operadores para disparar a ação, com base no número de resultados:

4.3.46.5.1. Quantidade maior que um determinado número;

4.3.46.5.2. Quantidade menor que um determinado número;

4.3.46.5.3. Quantidade igual a um determinado número;

4.3.46.5.4. Quantidade diferente de um determinado número;

4.3.46.5.5. Alertas baseados em buscas agendadas, em que a ação é disparada se uma determinada quantidade de eventos tiver acontecido em uma determinada janela de tempo;

4.3.46.5.5.1. Um exemplo seria enviar um alerta se as quantidades de acessos a um determinado site tiveram ultrapassado uma determinada quantidade na última hora;

4.3.46.5.6. Deve suportar, no mínimo, os seguintes operadores para disparar a ação, com base no número de resultados:

4.3.46.5.7. Quantidade maior que um determinado número;

4.3.46.5.8. Quantidade menor que um determinado número;

4.3.46.5.9. Quantidade igual a um determinado número;

4.3.46.5.10. Quantidade diferente de um determinado número;

4.3.46.6. A solução deve permitir o controle da quantidade de ações disparada pelo alerta em uma determinada janela de tempo;

4.3.46.6.1. Deve ser possível definir o campo do evento para controle;

4.3.46.6.1.1. Um exemplo dessa funcionalidade seria controlar a quantidade de ações com base no campo “usuário”, visando evitar alertas repetidos em uma terminada janela de tempo caso sejam gerados pelo mesmo usuário;

4.3.46.7. Deve ser possível compartilhar alertas criados com outros usuários da solução;

4.3.47. A solução deve suportar o recebimento e indexação de eventos SNMP;

4.3.48. A solução deve suportar correlacionamento de eventos distintos, visando gerar alertas baseados em eventos sem relação inicial;

4.3.48.1. Deve suportar buscas transacionais, de modo a criar um ponto único de observação sobre múltiplos eventos isolados;

4.3.48.2. Deve ser capaz de informar os eventos que compõem um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução, referenciando estes eventos básicos a partir do evento de alerta/incidente;

4.3.49. A solução deve possuir ferramenta para criação e edição de “dashboards”, de modo a combinar buscas, gráficos, alertas e relatórios em “dashboards” customizáveis para cada perfil de usuário (técnico, segurança, desenvolvimento, monitoração, executivo, marketing, auditoria, etc.);

4.3.50. A solução deve possuir sistema de autenticação e controle de acesso do tipo RBAC (role based access control), de modo a permitir a definição de funções, e atribuição de usuários a estas;

4.3.50.1. Deve permitir que um mesmo usuário pertença a várias funções distintas;

4.3.50.2. Deve permitir a definição de usuários com privilégios distintos, como, por exemplo:

4.3.50.2.1. Administradores da solução;

4.3.50.2.2. Usuários avançados;

4.3.50.2.3. Usuários comuns;

4.3.51. A solução deve suportar, no mínimo, os seguintes métodos de autenticação:

4.3.51.1. Autenticação na base de usuários própria da solução;

4.3.51.2. LDAP;

4.3.51.3. RADIUS;

4.3.51.4. PAM;

4.3.52. A solução deve suportar nativamente a criação de ambientes pré-configurados para interpretação e visualização de determinados tipos de eventos;

4.3.52.1. Deve prover, no mínimo, 300 tipos de ambientes pré-configurados;

4.3.52.2. Um ambiente pré-configurado deve ser entendido como muito mais que um conector/parser, no sentido de prover não apenas a interpretação de uma determinada categoria de evento, como também outros elementos como dashboards, relatórios gráficos, etc., que apresentem uma visão gráfica (e/ou combinada) das informações analisadas, contribuindo assim com o aumento da visibilidade do ambiente como um todo;

4.3.52.3. Deve permitir ao usuário compartilhar seus próprios ambientes pré-configurados, ou mesmo fazer o download e instalar ambientes pré-configurados desenvolvidos por terceiros (outros usuário, ou mesmo fabricantes de soluções de TI);

4.3.52.4. Deve possuir base disponível via web para download de ambientes pré-configurados gratuitos;

4.3.52.5. Deve possuir ambientes pré-configurados e gratuitos, para no mínimo, as seguintes soluções/tecnologias/produtos/aplicações:

4.3.52.6. Cisco;

4.3.52.7. VmWare;

4.3.52.8. NetFlow;

4.3.52.9. Firewalls Checkpoint, Palo Alto, Fortinet, Cisco;

4.3.52.10. Snort;

4.3.52.11. FireEye;

4.3.52.12. Postfix;

4.3.52.13. Squid

4.3.52.14. Windows;

4.3.52.15. Active Directory;

4.3.52.16. Linux;

4.3.52.17. Unix;

4.3.52.18. Google Maps;

4.3.52.19. Bind DNS;

4.3.52.20. SQL Server;

4.3.53. A solução deve possuir funcionalidade de arquivamento de dados indexados, com base, no mínimo, em tempo ou quantidade de dados;

4.3.53.1. Deve ser possível configurar uma política de arquivamento, em que os dados mais antigos, ou que ultrapassem os limites configurados, sejam apagados automaticamente ou arquivados em área separada;

4.3.53.2. A solução deve permitir o backup dos dados indexados;

4.3.53.3. Deve permitir backup de dados recentes via uso de soluções de backup de terceiros baseadas em snapshots;

4.3.53.4. Deve permitir ao usuário mover dados recentes para áreas de menor prioridade, de modo a suportar métodos tradicionais de backup (cópia simples, etc.);

4.3.54. A solução deve possuir APIs para integração com outras soluções;

4.3.54.1. Deve possuir API REST;

4.3.55. A solução deve suportar coleta remota de eventos de servidores Microsoft Windows via WMI;

5. GARANTIA

5.1. Para a solução envolvida na contratação, a CONTRATADA deverá prever garantia dos produtos, softwares e equipamentos, durante o período contratado, na modalidade *on site* sob o regime de 24h/7dias, a partir da data de aceite definitivo de toda a solução, fornecendo sem custo adicional todos os ajustes às falhas que porventura venham a ser encontradas.

6. RESPONSABILIDADES E DEVERES DO CONTRATANTE E DO CONTRATADO

6.1. **OBRIGAÇÕES DO CONTRATADO**

6.1.1. Na execução dos objetos do presente instrumento, obriga-se a empresa fornecedora a proceder com todo o empenho e dedicação necessários ao fiel cumprimento dos serviços que lhes são confiados, obrigando-se ainda a:

6.1.1.1. Responsabilizar-se pela fidelidade aos padrões tecnológicos utilizados, além de oferecer repasse tecnológico de operação aos técnicos do CONTRATANTE, bem como aos responsáveis pela manutenção e testes periódicos;

6.1.1.2. Responsabilizar-se pelos danos causados ao patrimônio do CONTRATANTE por culpa, dolo, negligência ou imprudência de seus profissionais;

6.1.1.3. Não transferir a outrem, no todo ou em parte, o objeto deste instrumento, sem prévia e expressa anuência do CONTRATANTE;

6.1.1.4. Indicar um preposto ou representante, para fins de contato e demais providências inerentes à execução do objeto deste instrumento;

6.1.1.5. Formalizar o encerramento dos serviços de instalação e configuração da solução com procedimentos e Termo de Aceite assinado pelas partes, observado o art. 69, da Lei n.º 8.666/93;

6.1.1.6. Manter, durante toda a execução dos serviços, as condições de habilitação e qualificação exigidas;

6.1.1.7. Disponibilizar um técnico junto ao CONTRATANTE, para suporte durante a instalação dos serviços;

6.1.1.8. Preencher um relatório detalhado ao ser entregue no final das instalações;

6.1.1.9. Efetuar instalação e configuração de todos os componentes de hardware e software que compõem a solução de modo a atender integralmente às características exigidas e às necessidades do CONTRATANTE, responsabilizando-se por todos os procedimentos necessários para tal.

6.1.1.10. Sujeitar-se, por si e por seus técnicos, às normas internas de segurança do CONTRATANTE, inclusive aquelas referentes à identificação, trânsito e permanência em suas dependências.

6.1.1.11. Obedecer às disposições do Código de Proteção e Defesa do Consumidor, instituído pela Lei n.º 8.078, de 11 de setembro de 1990.

6.2. **OBRIGAÇÕES DO CONTRATANTE**

6.2.1. O CONTRATANTE obriga-se a cumprir fielmente as condições e exigências contidas nesse instrumento, e em especial:

6.2.1.1. Acompanhar e fiscalizar a execução do contrato, nos termos do art. 67 da Lei nº 8.666/93;

6.2.1.2. Informar o CONTRATADO de atos que possam interferir direta ou indiretamente nos serviços prestados;

6.2.1.3. Comunicar formalmente qualquer anormalidade ocorrida na execução dos serviços pelo CONTRATADO;

6.2.1.4. Avaliar todos os serviços prestados pelo CONTRATADO;

6.2.1.5. Responsabilizar-se pelos pagamentos dos serviços prestados pelo CONTRATADO, mediante a apresentação de Nota Fiscal;

6.2.1.6. Permitir o acesso às instalações do CONTRATANTE dos técnicos habilitados e identificados pelo CONTRATADO, para os serviços de manutenção;

6.2.1.7. Promover o acompanhamento e a fiscalização desta contratação, sob os aspectos quantitativo e qualitativo, anotando em registro próprio as falhas detectadas, comunicando as ocorrências de quaisquer fatos que exijam medidas corretivas por parte do CONTRATADO;

6.2.1.8. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATADO;

6.2.1.9. Notificar o CONTRATADO, por escrito, sobre toda e qualquer irregularidade constatada na execução dos serviços e ocorrências de quaisquer fatos, que, a seu critério, exijam medidas corretivas;

7. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

7.1. **QUALIFICAÇÃO TÉCNICA DA EMPRESA PARA HABILITAÇÃO**

7.1.1. Poderão participar do certame os licitantes que:

7.1.1.1. Desempenham atividade pertinente e compatível com o objeto deste certame.

7.1.1.2. Atendam às exigências constantes nesse instrumento, inclusive quanto à documentação requerida para sua habilitação.

7.1.1.3. Não será admitida neste certame a participação de empresas que:

7.1.1.4. Estejam com falência declarada, sob concurso de credores, em dissolução ou em liquidação.

7.1.1.5. Estejam com o direito suspenso de licitar e contratar com o MCTI ou que tenham sido declaradas inidôneas por órgão da administração pública, bem como tenham sido descredenciadas do Sistema de Cadastro de Fornecedores - SICAF.

7.2. **ATESTADOS DE CAPACIDADE TÉCNICA.**

7.2.1. Com a finalidade de garantir que a licitante será capaz de fornecer os equipamentos, prestar os serviços envolvidos e a garantia técnica, bem como garantir a originalidade de todos os equipamentos, sua participação no certame está condicionada à comprovação de capacidade técnica. Assim, a licitante deverá, nos termos do Art. 30, § 1º, da Lei 8.666/93, apresentar atestado(s) expedido(s) por pessoa jurídica de direito público ou privado, indicado abaixo:

7.2.1.1. Possuir Atestado(s) de Capacidade Técnica(ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove fornecimento de solução de proteção de rede baseada em hardware especializado, não podendo ser servidor ou estação de trabalho de uso genérico;

7.2.1.2. Possuir Atestado(s) de Capacidade Técnica(ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove fornecimento de solução de análise de rede;

7.2.1.3. Possuir Atestado(s) de Capacidade Técnica(ACT) em nome da licitante, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove fornecimento de solução de análise de eventos;

7.2.2. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente.

7.2.3. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

7.2.4. Os documentos apresentados poderão ser tanto da matriz quanto da filial, exceto quando se tratar de documentos próprios da filial quanto à regularidade fiscal, desde que esta seja a executora ou a participante do certame.

7.2.5. A comprovação será realizada, exclusivamente, mediante a apresentação de cópia autenticada do certificado.

7.2.6. O CONTRATANTE poderá, em qualquer fase do processo licitatório, promover diligências com vistas a esclarecer ou a complementar a instrução do processo, obrigando as licitantes a prestar todos os esclarecimentos necessários.

7.2.7. Os atestados de capacidade técnica deverão contemplar, no mínimo, as seguintes informações:

7.2.7.1. Razão Social, CNPJ e Endereço Completo da Empresa Emitente;

7.2.7.2. Razão Social do CONTRATADO;

7.2.7.3. Número e vigência do contrato;

7.2.7.4. Objeto do contrato;

7.2.7.5. Declaração de que foram atendidas as expectativas do cliente quanto ao cumprimento de cronogramas pactuados;

7.2.7.6. Local e Data de Emissão;

7.2.7.7. Identificação do responsável pela emissão do atestado, Cargo, Contato (telefone e correio eletrônico);

7.2.7.8. Assinatura do responsável pela emissão do atestado; e

7.2.8. Devem ser originais ou autenticados, se cópias, e legíveis.

7.3. **DOCUMENTAÇÃO DE ATENDIMENTO AOS REQUSITOS TÉCNICOS**

7.3.1. A empresa declarada vencedora na etapa de lances do pregão deve anexar à sua proposta comercial adequada ao último lance a comprovação ponto a ponto de todos os requisitos técnicos do termo de referência.

7.3.2. A comprovação de cada item deve ser realizada com referência a manuais, datasheets e demais materiais produzidos pelo fabricante da solução ofertada.

7.3.3. A comprovação deve ser realizada em tabela de acordo com o modelo a seguir:

Número do Item original	**Texto do Item original**	**Comprovação**	**Observações**
(Referenciado pelo número do item publicado)	(Referenciado pelo texto do item publicado)	(Referência ao material fornecido pelo fabricante da solução)	(Informações para auxiliar no entendimento da comprovação do item)

Exemplo:

Número do Item original	Texto do Item original	Comprovação	Observações
1.1	<Colar aqui texto do item>	Manual_Produto.pdf, página 132 Site do fabricante: http://<URL>	Segundo parágrafo do documento, e imagem ao final da página no site

7.3.4. O material de referência utilizado no campo "Comprovação" (documentos, manuais, páginas do site, etc.) deve ser entregue junto com a proposta comercial adequada ao último lance, em formato digital (conforme instruções do edital e/ou informadas durante pregão).

7.4. **COMPROVAÇÃO DE ATENDIMENTO AOS REQUSITOS TÉCNICOS**

7.4.1. O CONTRATANTE poderá requisitar a seu critério "teste de bancada" da solução vencedora, a ser executado em até 05 (cinco) dias úteis após a realização do pregão.

7.4.2. O licitante vencedor deverá implantar (em escala de laboratório/testes), no ambiente do CONTRATANTE, a solução ofertada, de modo a demonstrar de forma prática o atendimento aos requisitos técnicos previstos no edital;

7.4.3. O licitante vencedor terá o prazo de 02 (dois) dias úteis para montar o ambiente de testes;

7.4.4. O CONTRATANTE irá apresentar um Plano de Testes a ser executado no ambiente montado, cujos requisitos serão restritos às funcionalidades previstas nesse instrumento;

7.4.5. O licitante vencedor não terá conhecimento prévio do Plano de Testes, e terá o prazo de 01 (um) dia útil para executá-lo após recebê-lo;

7.4.6. O CONTRATANTE irá acompanhar toda a execução do Plano de Testes, assim como coordenar o acesso de demais partes interessadas ao processo;

7.4.7. Cada item executado do Plano de Testes poderá ter apenas dois resultados: sucesso ou falha;

7.4.8. A falha em qualquer dos itens do Plano de Testes implicará na desclassificação do licitante do processo licitatório, com a convocação sequencial dos outros participantes do processo de acordo com o resultado do pregão;

8. NÍVEIS MÍNIMOS DE SERVIÇOS EXIGIDOS.

8.1. Visando a avaliar o desempenho dos serviços prestados pelo CONTRATADO para o CONTRATANTE, será estabelecida uma política de Nível Mínimo de Serviço Exigido - NMSE e respectivos indicadores objetivos e mensuráveis, que contemple as expectativas do CONTRATANTE em relação aos serviços contratados. O intuito é manter uma perfeita aderência destes indicadores frente ao escopo e objetivos da prestação dos serviços e às expectativas do CONTRATANTE.

8.2. O conjunto de indicadores tem por objetivo auxiliar a gestão dos serviços, provendo informação periódica.

8.3. Os NMSEs representam os Níveis Mínimos de Serviço Exigidos contratados e têm impacto financeiro, pois o seu não cumprimento pode acarretar multas e até rescisão do contrato.

8.4. **SOLUÇÃO INTEGRADA DE PROTEÇÃO E RESPOSTA DE INCIDENTES.**

8.4.1. Quando se tratar de entrega de equipamentos o não cumprimento do objeto conforme estabelecido neste instrumento configurará a inexecução do contrato, conforme disposto na Lei 8.666/93, devendo assim aplicar as penalidades nela prevista.

8.5. **SERVIÇOS DE GARANTIA.**

8.5.1. O não cumprimento do serviço de garantia e manutenção mensal estabelecido neste instrumento configurará a inexecução do contrato, conforme disposto na Lei 8.666/93, devendo assim aplicar as penalidades nela prevista.

8.6. **SERVIÇOS DE IMPLANTAÇÃO DE CADA MÓDULO**

8.6.1. O não cumprimento dos serviços de implantação de cada módulo estabelecido neste instrumento configurará a inexecução do contrato, conforme disposto na Lei 8.666/93, devendo assim aplicar as penalidades nela prevista.

8.7. **SERVIÇO DE TREINAMENTO.**

8.7.1. O objetivo do Nível Mínimo de Serviço de Treinamento $NMSE_{treinamento}$ é garantir a satisfação dos alunos (usuários e servidores).

8.7.2. O Nível Mínimo de Serviço de Treinamento será aplicado ao final do treinamento de cada turma, conforme as seguintes fórmulas:

$$M5 = \frac{\sum_{i=1}^{5} N_i * q_i}{n} \ (1)$$

8.7.3. Onde:

8.7.3.1. M5 = Média de cada item na escala de 1 a 5;

8.7.3.2. N = número de participante por nota, de 1 a 5;

8.7.3.3. q = quantidade de participantes por turma;

8.7.3.4. i = notas, na escala de 1 a 5;

$$M100 = \sum_{i=1}^{7} \frac{M5_i}{5} * 100 \ (2)$$

8.7.4. Onde:

8.7.4.1. M100 = média de cada item na escala de 1 a 100;

8.7.4.2. M5 = média de cada item na escala de 1 a 5, obtido na fórmula (1);

8.7.4.3. i = itens da avaliação, variando de 1 a 7.

$$NMSE_{treinamento} = \frac{\sum_{i=1}^{7} M100_i}{7} \ (3)$$

8.7.5. Onde:

8.7.5.1. $NMSE_{treinamento}$ = Percentual de aprovação do curso pelos alunos;

8.7.5.2. M100 = média das notas atribuídas pelos alunos em cada item, obtida na fórmula (2).

8.7.6. Os itens (i) constantes nas fórmulas do Fator de Nível de Serviço de Treinamento são descritos no Anexo I-H – Modelo de Ficha de Avaliação.

8.7.7. O $FDNS_{os}$ Fator de Dedução Nível de Serviço é determinado de acordo com o índice de aprovação do treinamento:

Tabela 5 – Fator de Nível de Serviço de Treinamento

$NMSE_{treinamento}$ *(Percentual de Aprovação do Treinamento)*	Registro Ocorrência de Não-Conformidade	$FDNS_{OS}$ *(Fator de Dedução)*
De 100% até 70%	Não	0,00
Abaixo de 70% até 60%	Sim	0,05
Abaixo de 60% até 50%	Sim	0,10
Abaixo de 50% (Reprovação)	Sim	O CONTRATADO é obrigada a repetir o treinamento sem ônus para o CONTRATANTE.

8.7.8. O FDNSos incidirá sobre o valor bruto da respectiva Ordem de Serviço, de acordo o índice obtido, aplicando-se a fórmula descrita no item 8.7.9 – Aplicação do NMSE.

8.7.9. **APLICAÇÃO DO NMSE - TREINAMENTO**

$$VlrFinal_{OS} = VlrBruto_{OS} X\ (1 - FDNS_{OS})$$

Legenda:

- Valor $Final_{os}$ = Valor Bruto da OS descontado o fator de NMSE.
- Valor $Bruto_{os}$ = Valor estimado da OS
- $FDNS_{OS}$= Fator de ajuste obtido a partir dos índices de aprovação

8.8. **SERVIÇO DE SUPORTE TÉCNICO MENSAL**

8.8.1. **DISPONIBILIDADE**

8.8.1.1. A indisponibilidade do Portal de Suporte em ambiente WEB e o número de discagem gratuito acarretará ajuste de 1% valor da ordem de serviço dos serviços de suporte técnico mensal, para cada hora de indisponibilidade.

8.8.2. **TEMPO DE INÍCIO PARA SOLUÇÃO DOS PROBLEMAS**

8.8.2.1. Os chamados de suporte técnico, independentemente do modo de abertura (e-mail, telefone ou portal web) devem ter seu tratamento iniciado em 30 minutos.

8.8.3. SOLUÇÃO DOS CHAMADOS

8.8.3.1. A solução dos chamados deverá atender aos seguintes níveis mínimos:

Tabela 6 - Níveis Mínimos de Serviços Exigidos

CLASSIFICAÇÃO DE SEVERIDADE	PRAZO MÁXIMO DE RESOLUÇÃO	AJUSTE SOBRE O VALOR MENSAL DOS SERVIÇOS DE SUPORTE TÉCNICO MENSAL
Baixa	8 horas	1% para cada hora de atraso
Média	4 horas	1,5% para cada hora de atraso
Alta	2 horas	1% para cada 30 minutos de atraso
Urgente	1 horas	2% para cada 30 minutos de atraso

8.8.3.2. APLICAÇÃO DOS NMSE – SUPORTE TÉCNICO MENSAL

8.8.3.2.1. O Fator de Nível de Serviço no mês será limitado a 20% – ainda que o somatório devido exceda este valor de acordo com a fórmula constante no item 8.8.3.2.4.

8.8.3.2.2. A aplicação do Fator de Nível de Serviço não exclui a aplicação das multas e sanções previstas neste documento. Salienta-se que no caso das multas estas serão aplicadas após extrapolar o limite imposto acima

8.8.3.2.3. Os índices de disponibilidade do NMSE não se aplicam às paradas de manutenção programadas ou casos fortuitos ou de força maior.

8.8.3.2.4. Fórmula:

$$Vlr_{mf} = Vlr_{bm} - \left(Vlr_{bm} \times \sum Ajuste_{NMSE}\right)$$

Vlr_{mf}	Valor Final a ser pago pelos serviços prestados no mês, após desconto dos ajustes do NMSE.
Vlr_{bm}	Valor Bruto Mensal do Serviço.

$Ajuste_{NMSE}$	Ajuste obtido a partir do somatório de nível de serviço descritos na tabela 4 – Nível Mínimo de Serviço Exigido.

8.8.4. SERVIÇO DE OPERAÇÃO ASSISTIDA

8.8.4.1. A entrega das atividades de operação assistida, após definição do cronograma, deverão atender aos seguintes níveis de serviço mínimo:

Tabela 7 - Níveis Mínimos de Serviços Exigidos

COMPLEXIDADE	AJUSTE SOBRE O VALOR MENSAL DOS SERVIÇOS DE SUPORTE TÉCNICO MENSAL
Baixa	0,5% para cada hora após o cronograma definido na ordem de serviço
Intermediária	1% para cada hora após o cronograma definido na ordem de serviço
Alta	2% para cada hora após o cronograma definido na ordem de serviço

8.8.4.2. Caso sejam detectados erros de qualidade nas entregas, a CONTRATADA será notificada, e o tempo de entrega voltará a contar do mesmo ponto de onde parou ao ser entregue. Assim, se o tempo total de entrega, somado ao tempo que a CONTRATADA utilizou para corrigir erros apontados pela CONTRATANTE após a entrega, ultrapassar o tempo útil definido no cronograma inicial, os índices de NMSE serão aplicados. Tal aplicação se dará sobre o tempo total utilizado.

8.8.4.2.1. Exemplo: É aberta uma ordem de serviço para o serviço de operação assistida, para uma configuração de complexidade intermediária. É definido que em cronograma acordado entre a CONTRATANTE e a CONTRATADA que o serviço será terminado em 18 horas. A CONTRATADA entrega o serviço em 15 horas. Após 2 dias a CONTRATANTE vê que houve uma falha na configuração realizada, e notifica a CONTRATADA para que esta corrija o erro da entrega. A CONTRATADA demora mais 5 horas para corrigir o erro. Assim, o tempo total do serviço foi de 20 horas, e haverá ajuste de 2% (1% por hora) sobre o valor total da ordem de serviço.

8.8.4.3. **REGRAS DE APLICAÇÃO DOS NMSES**

8.8.4.3.1. O Fator de Nível de Serviço no mês será limitado a 20% – ainda que o somatório devido exceda este valor de acordo com a fórmula constante no item 8.8.4.3.4.

8.8.4.3.2. A aplicação do Fator de Nível de Serviço não exclui a aplicação das multas e sanções previstas neste documento. Salienta-se que no caso das multas estas serão aplicadas após extrapolar o limite imposto acima

8.8.4.3.3. Os índices de disponibilidade do NMSE não se aplicam às paradas de manutenção programadas ou casos fortuitos ou de força maior.

8.8.4.3.4. Fórmula:

$$Vlr_{mf} = Vlr_{bm} - \left(Vlr_{bm} \times \sum Ajuste_{NMSE}\right)$$

Vlr_{mf}	Valor Final a ser pago pelos serviços prestados no mês, após desconto dos ajustes do NMSE.
Vlr_{bm}	Valor Bruto da Ordem de Serviço.
$Ajuste_{NMSE}$	Ajuste obtido a partir do somatório de nível de serviço descritos na tabela 4 – Nível Mínimo de Serviço Exigido.

8.9. **REVISÃO**

8.9.1. Os Níveis Mínimos de Serviços Exigidos serão revisados anualmente para a adequação da realidade do CONTRATANTE, considerando:

8.9.1.1. Normas e legislação vigentes;

8.9.1.2. Governança de TI;

8.9.1.3. Novas tecnologias disponíveis;

8.9.1.4. Necessidades de Negócio;

8.9.1.5. Novas metodologias e melhores práticas.

8.10. **CONSIDERAÇÕES**

8.10.1. Os períodos de suspensão de atendimento autorizados pelo CONTRATANTE não serão computadas dentro dos tempos calculados;

8.10.2. Não serão aplicados os Níveis Mínimos de Serviços Exigidos se, comprovadamente, o atraso da execução dos serviços advir de caso fortuito ou motivo de força maior.

8.10.3. Sempre que a meta não for alcançada o MCTI poderá emitir ofício de notificação ao CONTRATADO, que terá prazo máximo de 2 (dois) dias úteis para apresentar as justificativas para as falhas verificadas. Caso não haja manifestação do CONTRATADO dentro desse prazo ou caso o MCTI entenda serem improcedentes as justificativas, será iniciado processo de aplicação das sanções administrativas previstas no item referente às Sanções Administrativas.

9. DIRETRIZES PARA PLANO DE IMPLANTAÇÃO

9.1. O efetivo início dos fornecimentos previstos neste instrumento se dará após a emissão da(s) devida(s) Ordem(ns) de Serviço de Instalação, sendo que os totais contratados podem ser divididos em diversas Ordens de Serviço com descrições distintas, desde que não sejam extrapolados os valores e quantidades contratados. O prazo da prestação do serviço estará vinculado à data de emissão das Ordens de Serviço, respeitados os limites contratuais legais.

9.2. Podem ser emitidas Ordens de Serviço adicionais referentes a aditivos contratuais, uma vez que estes tenham sido devidamente assinados;

9.3. As Ordens de Serviços deverão conter, no mínimo:

9.3.1. A identificação de quem a emitiu (CONTRATANTE);

9.3.2. A identificação de quem a recebeu (CONTRATADO);

9.3.3. O objeto da Ordem de Serviço (o mesmo deste Edital / contrato);

9.3.4. O escopo da Ordem de Serviço (itens e quantidades a serem instaladas, locais de instalação);

9.3.5. Os valores a serem faturados;

9.3.6. A data de emissão;

9.3.7. O prazo de validade da Ordem de Serviço;

9.4. O CONTRATADO fornecedor da solução deverá proceder à instalação, configuração e testes dos componentes ofertados em um **prazo máximo de 90 (noventa) dias corridos**, contados da data de emissão da Ordem de Serviço.

9.5. Entende-se por instalação, a montagem física de todos os equipamentos e acessórios fornecidos, bem como a sua configuração lógica, de acordo como cenário proposto pelo CONTRATANTE.

9.6. O Recebimento Provisório relativo à entrega dos equipamentos realizar-se-á no prazo máximo de 5 (cinco) dias úteis, contados a partir do primeiro dia imediatamente posterior à comunicação escrita do CONTRATADO referente à conclusão da entrega.

9.6.1. O Recebimento Provisório consiste na verificação de conformidade dos equipamentos constantes da(s) Nota(s) Fiscal(is) de fornecimento, e a indicação de conteúdo dos volumes entregues em conjunto com a(s) Nota(s) Fiscal(is), observadas as especificações técnicas constantes neste instrumento.

9.7. O Recebimento Definitivo relativo à entrega dos equipamentos realizar-se-á no prazo máximo de (10) dez dias úteis após a emissão do Termo de Recebimento Provisório, desde que atendidas todas as eventuais solicitações da Comissão de Recebimento do MCTI.

9.7.1. O Recebimento Definitivo consiste na desembalagem e conferência visual de todos os itens fornecidos, e verificação de conformidade com as informações constantes neste instrumento. Caso exista execução de serviços de instalação na Ordem de Serviço esse Termo de Recebimento Definitivo será emanado após a conclusão dos serviços elencados e, concomitantemente, aprovação do técnico da CONTRATANTE de que os serviços foram prestados satisfatoriamente.

9.8. O CONTRATADO deverá enviar representante para acompanhar a desembalagem e conferência dos itens fornecidos, de forma a viabilizar a emissão do Termo de Recebimento Definitivo.

9.9. O CONTRATADO deverá fornecer toda a documentação técnica original, completa e atualizada, contendo os manuais e guias de utilização, no formato ".doc", ".rtf", ".pdf" ou outro que seja formalmente aceito pela unidade gestora do contrato.

9.10. Os equipamentos, juntamente com os documentos fiscais de cobrança, deverão ser entregues nas instalações do CONTRATANTE e em outras localidades fora do Distrito Federal de acordo com a origem da demanda.

9.11. As viagens para execução de serviços realizados fora do ambiente do CONTRATANTE serão executadas com recursos do CONTRATADO, conforme data e horário que o CONTRATANTE definir, respeitadas as condições descritas neste instrumento;

Tabela 8 - Localidades

Unidade	Localidade
MCTI	Esplanada dos Ministérios, Bloco E. CEP: 70067-900, Brasília, DF
	Setor Policial Sul - SPO, Área 5, Qd. 03. CEP: 70610-200 - Brasília/DF

10.TRANSIÇÃO CONTRATUAL

10.1. Em ocorrendo nova licitação, com mudança de fornecedor dos serviços, a CONTRATADA signatária do contrato em fase de expiração, assim considerado o período dos últimos três meses de vigência, deverá repassar para a vencedora do novo certame, para que haja transferência ordenada dos serviços, por intermédio de eventos formais, os documentos, procedimentos e conhecimentos necessários à continuidade da prestação dos serviços, incluindo a base de conhecimentos, bem como esclarecer dúvidas a respeito de procedimentos no relacionamento entre o MCTI e a nova CONTRATADA a fim de que os serviços continuem sendo prestados sem interrupção ou efeito adverso.

10.2. A falta de transferência de conhecimento caracterizará infração contratual, sujeitando a CONTRATADA às penalidades previstas na legislação vigente, no contrato e neste instrumento.

10.3. A CONTRATADA deverá participar de todas as reuniões marcadas pelo CONTRATANTE relacionadas à transição contratual, assim como deverá atender todas as solicitações do MCTI, referentes à execução contratual, tanto no que se refere à parte documental, como no tocante às demais informações julgadas necessárias.

10.4. A empresa CONTRATADA será responsável pela transição inicial e final dos serviços, absorvendo as atividades de forma a documentá-las minuciosamente para que os repasses de informações, conhecimentos e procedimentos, no final do contrato, aconteça de forma precisa e responsável.

10.5. A CONTRATADA compromete-se a fornecer para o CONTRATANTE toda a documentação relativa à prestação dos serviços que esteja em sua posse.

10.6. O conhecimento será transferido por meio de transferência de conhecimento disponibilizado pela CONTRATADA para o CONTRATANTE.

10.7. Ao final do contrato ou em caso de rescisão, a CONTRATADA deverá:

10.7.1. Devolver ao CONTRATANTE a capacidade para executar os serviços;

10.7.2. Devolver equipamentos e bens de propriedade do CONTRATANTE, incluindo, mas não limitado aos listados nas cláusulas do contrato e os bens intangíveis, como software, descrição de processos e rotinas de diagnóstico;

10.7.3. Devolver documentação de processos, procedimentos, scripts desenvolvidos com ou para o CONTRATANTE durante a prestação dos serviços;

10.7.4. Participar, em conjunto com o CONTRATANTE, sob sua solicitação, da elaboração do Plano de Transferência de Conhecimento.

10.8. **TRANSFERÊNCIA DE CONHECIMENTO**

10.8.1. A transferência de conhecimento tem o objetivo de auxiliar o MCTI na internalização do conhecimento técnico e operacional da solução desenvolvida.

10.8.2. É de responsabilidade da empresa que estiver prestando os serviços a execução de todos os procedimentos cabíveis para a efetiva transferência de conhecimento, assim a CONTRATADA deverá descrever a metodologia a ser utilizada, conforme o Plano de Transferência de Conhecimento, para transferir conhecimento aos técnicos do MCTI, os quais poderão ser multiplicadores do conhecimento transferido a outros técnicos ou a usuários finais.

10.8.3. A CONTRATADA deverá viabilizar a transferência de conhecimento, sem ônus adicionais para o MCTI, no prazo máximo de até 60 (sessenta) dias, a contar da notificação do CONTRATANTE, conforme Plano de Transferência de Conhecimento, em eventos específicos, preferencialmente em ambiente disponibilizado pela CONTRATADA, e baseado em documentos técnicos e/ou manuais específicos da solução desenvolvida. O cronograma e horários dos eventos deverão ser previamente aprovados pelo MCTI.

10.8.3.1. A CONTRATADA deverá entregar, no prazo máximo de 60 (sessenta) dias corridos, antes do termino do contrato, independente de notificação, o Plano de Transferência de Conhecimentos.

10.8.3.2. O Plano de Transferência de Conhecimento será executado pelas partes, quando da assinatura do Termo de Recebimento Definitivo da Solução, nas dependências do CONTRATANTE em horário previamente agendado.

11.TERMOS CONTRATUAIS

11.1. ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

11.1.1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, da Instrução Normativa SLTI/MPOG nº 04/2010 e, no que couber, da Instrução Normativa SLTI/MPOG nº 02/2008.

11.1.2. A CONTRATADA deverá possuir preposto, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao CONTRATANTE, incumbido de receber, diligenciar, encaminhar e receber as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

11.2. FORMA DE PAGAMENTO

11.2.1. O pagamento será conforme demanda, vinculada à emissão de Ordens de Serviços e seu Recebimento Definitivo, sendo sempre precedido na entrega da nota fiscal emitida em moeda corrente nacional, até o 5º (quinto) dia útil após a efetiva entrega da demanda.

11.2.2. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o montante de R$ 8.000,00 (oito mil reais), deverão ser efetuados no prazo de até 5(cinco), contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº8.666, de 1993.

11.2.3. O pagamento somente será efetuado após o Recebimento Definitivo da Solução de TI, vinculado à uma Ordem de Serviço, e consequente atesto da Nota Fiscal/Fatura apresentada pela CONTRATADA.

11.2.3.1. O atesto fica condicionado à verificação da conformidade da Nota Fiscal/Fatura apresentada pela CONTRATADA.

11.2.4. Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da

despesa, o pagamento ficará pendente até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

11.2.5. Caso o fornecimento dos serviços, executados pelo CONTRATADO, estiverem em desacordo com as especificações constantes neste Termo de Referência e seus anexos, o MCTI reserva-se no direito de suspender o(s) pagamento(s) até as devidas retificações/correções.

11.2.6. Nos termos do artigo 36, § 6°, da Instrução Normativa MPOG n° 02, de 2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que o CONTRATADO:

11.2.6.1. Não produziu os resultados acordados;

11.2.6.2. Deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

11.2.6.3. Deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

11.2.7. Antes do pagamento, a CONTRATANTE verificará, por meio de consulta eletrônica, a regularidade do cadastramento da Contratada no SICAF e/ou nos sites oficiais, especialmente quanto à regularidade fiscal e trabalhista (CNDT – Lei 12.440/2011), devendo seu resultado ser impresso, autenticado e juntado ao processo de pagamento.

11.2.8. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

11.2.8.1. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

11.2.9. O pagamento será efetuado por meio de Ordem Bancária de Crédito, mediante depósito em contracorrente, na agência e estabelecimento bancário indicado pela CONTRATADA, ou por outro meio previsto na legislação vigente.

11.2.10. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

11.2.11. A CONTRATANTE não se responsabilizará por qualquer despesa que venha a ser efetuada pela CONTRATADA, que porventura não tenha sido acordada no contrato

11.2.12. Nos casos de eventuais atrasos de pagamento, desde que o CONTRATADO não tenha concorrido, de alguma forma, para tanto, o valor devido deverá ser acrescido de encargos moratórios proporcionais aos dias de atraso, apurados desde a data limite prevista para o pagamento até a data do efetivo pagamento, à taxa de 6% (seis por cento) ao ano, aplicando-se a seguinte fórmula:

$$EM = I \times N \times VP$$

Onde:
EM = Encargos Moratórios a serem acrescidos ao valor originalmente devido;
I = Índice de atualização financeira, calculado segundo a fórmula:

$$I = \frac{(6 \div 100)}{365}$$

N = Número de dias entre a data limite prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso;

11.2.12.1. Na contagem dos prazos estabelecidos neste item excluir-se-á o dia do início e incluir-se-á o dia do vencimento, só se iniciando e se vencendo os prazos em dia de expediente no MCTI e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário.

11.2.12.2. Não haverá, sob hipótese alguma, pagamento antecipado ao CONTRATADO.

11.3. **FORMALIZAÇÃO E VIGÊNCIA DO CONTRATO**

11.3.1. Será formalizado instrumento contratual com vigência de 36 (trinta e seis) meses. A previsão desse prazo protegerá a entrega dos bens previstos neste

instrumento, bem como resguardará a excelência na execução de todos os serviços envolvidos por parte da CONTRATADA durante os serviços de caráter contínuo.

11.3.1.1. As políticas de garantia estendida contemplam o caráter acessório ao núcleo do contrato e, portanto, devem ser prestadas durante os prazos estabelecidos no instrumento contratual, sob pena da Administração invocar as cláusulas do contrato, mesmo após o encerramento de sua vigência.

11.3.2. Em razão do objeto, não haverá hipótese de renovação do Contrato.

11.3.3. Para assinatura do contrato, será exigida a apresentação de cópia do documento de identidade (RG), CPF e do instrumento público de procuração ou de instrumento particular com firma reconhecida do representante que irá assiná-lo, onde comprove a outorga de poderes, na forma da lei. Em sendo sócio, proprietário, dirigente ou assemelhado da empresa, deverá apresentar cópia do respectivo estatuto ou contrato social, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal.

11.3.3.1. Para a assinatura do contrato, será exigida a comprovação de que a empresa está autorizada a comercializar os produtos especificados.

11.4. **GARANTIA DE EXECUÇÃO CONTRATUAL**

11.4.1. Será exigida a prestação de garantia pela fornecedora, como condição para a celebração do contrato, no percentual de 5% (cinco por cento) do valor total do contrato, optando por uma das seguintes modalidades:

11.4.1.1. Caução em dinheiro ou títulos da dívida pública;

11.4.1.2. Seguro-garantia;

11.4.1.3. Fiança bancária

11.4.2. Não será aceita a prestação de garantia que não cubra todos os riscos ou prejuízos eventualmente decorrentes da execução do contrato, tal como a responsabilidade por multas, bem como apresentação de fiança que não seja emitida por instituições bancárias credenciadas junto ao Banco Central do Brasil.

11.4.3. No caso de caução em dinheiro, o depósito deverá ser efetuado na Caixa Econômica Federal mediante depósito identificado a crédito do CONTRATANTE.

11.4.4. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

11.4.5. A garantia prestada deverá ter validade durante a vigência do contrato.

11.4.6. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

11.4.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

11.4.8. Se o valor da garantia for utilizado, total ou parcialmente, pelo CONTRATANTE, para compensação de prejuízo causado no decorrer da execução contratual por conduta da CONTRATADA, esta deverá proceder à respectiva reposição no prazo de 5 (cinco) dias úteis, contados da data em que tiver sido notificada.

11.4.9. Após a execução do contrato, constatado o regular cumprimento de todas as obrigações a cargo da CONTRATADA, a garantia por ela prestada será liberada ou restituída e, quando em dinheiro, atualizada monetariamente, deduzidos eventuais valores devidos ao CONTRATANTE.

11.4.10. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa conforme o item Sanções Administrativas previstas neste instrumento.

11.4.11. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger o período da vigência do contrato, acrescida de 6 (seis) meses após o término contratual.

11.4.12. O uso da garantia poderá ser motivado por eventuais impropriedades detectadas durante o uso da solução, neste caso, caberá uma decisão conjunta, devidamente documentada, ressaltando os aspectos positivos ou imprescindíveis que justifiquem as correções. A documentação deverá ser atualizada para refletir eventuais mudanças realizadas.

11.4.13. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

11.4.13.1. Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

11.4.13.2. Prejuízos causados à CONTRATANTE ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

11.4.13.3. As multas moratórias e punitivas aplicadas pelo CONTRATANTE ao CONTRATADO;

11.4.14. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser adequada ou renovada nas mesmas condições.

11.4.15. O CONTRATANTE não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

11.4.15.1. Caso fortuito ou força maior;

11.4.15.2. Alteração unilateral das obrigações contratuais;

11.4.15.3. Descumprimento das obrigações pelo contratado decorrentes de atos ou fatos praticados pelo CONTRATANTE;

11.4.15.4. Atos ilícitos dolosos praticados por servidores do CONTRATANTE.

11.4.16. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas neste item.

11.4.17. A garantia somente será restituída após o integral cumprimento de todas as obrigações contratuais, inclusive no caso de aplicação de multa contratual e satisfação de prejuízos e, quando em dinheiro, atualizada monetariamente. (Art. 56, §4º, da Lei nº 8.666/1993).

11.4.18. Será considerada extinta a garantia:

11.4.18.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato;

11.4.18.2. No prazo de 6 (seis) meses, após o término da vigência, caso o CONTRATANTE não comunique a ocorrência de sinistros.

11.5. **SANÇÕES ADMINISTRATIVAS**

11.5.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, e do Decreto nº 5.450, de 2005, a licitante/Adjudicatária que:

11.5.1.1. Não assinar a Ata de Registro de Preços, não retirar a nota de empenho, ou não assinar o contrato, quando convocada dentro do prazo de validade da proposta ou da Ata de Registro de Preços;

11.5.1.2. Apresentar documentação falsa;

11.5.1.3. Deixar de entregar os documentos exigidos no certame;

11.5.1.4. Não mantiver a sua proposta dentro de prazo de validade;

11.5.1.5. Falhar ou fraudar na execução do Contrato;

11.5.1.6. Comportar-se de modo inidôneo;

11.5.1.7. Cometer fraude fiscal;

11.5.1.8. Fizer declaração falsa;

11.5.1.9. Ensejar o retardamento da execução da certamente.

11.5.2. A licitante/Adjudicatária que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

11.5.2.1. Advertência por escrito;

11.5.2.2. Multa de:

11.5.2.2.1. 2% (dois por cento) a hora sobre o valor da demanda para interrupção ou atraso dos prazos estabelecidos para o atendimento e/ou solução definitiva dos chamados abertos com severidade CRÍTICO, limitado a incidência de 8 (oito) horas;

11.5.2.2.2. 1,5% (dois por cento) a hora sobre o valor da demanda para interrupção ou atraso dos prazos estabelecidos para o atendimento e/ou solução definitiva dos chamados abertos com severidade ALTA, limitado a incidência de 8 (oito) horas;

11.5.2.2.3. 1% (um por cento) a hora sobre o valor da demanda para atraso dos prazos estabelecidos para o atendimento e/ou solução definitiva dos chamados abertos com severidade MÉDIA, limitado a incidência de 24 (vinte e quatro) horas;

11.5.2.2.4. 1% (um por cento) a hora sobre o valor da demanda para atraso dos prazos estabelecidos para o atendimento e/ou solução definitiva dos chamados abertos com severidade BAIXA, limitado a incidência de limitado a incidência de 15 (quinze) dias úteis;

11.5.2.2.5. 2% (dois por cento) sobre o valor do Contrato, no caso de atraso por período superior ao previsto no item 11.5.2.2.1, limitado à incidência de 24 (vinte e quatro) horas;

11.5.2.2.6. 1,5% (dois por cento) sobre o valor do Contrato, no caso de atraso por período superior ao previsto no item 11.5.2.2.2, limitado à incidência de 24 (vinte e quatro) horas;

11.5.2.2.7. 1% (um por cento) sobre o valor do Contrato, no caso de atraso por período superior ao previsto no item 11.5.2.2.3, limitado à incidência de 3 (três) dias úteis;

11.5.2.2.8. 1% (um por cento) sobre o valor do Contrato, no caso de atraso por período superior ao previsto no item 11.5.2.2.4, limitado à incidência de 30 (trinta) dias úteis;

11.5.2.2.9. 0,5% (cinco décimos por cento) sobre o valor do bem não entregue por dia de atraso injustificado até o limite de 30 (trinta) dias o que caracteriza inexecução parcial. Contar-se-á o prazo a partir do tempo máximo de entrega estipulado ou após o prazo concedido às substituições, quando o objeto licitado estiver em desacordo com as especificações previstas;

11.5.2.2.10. 20% (vinte por cento) sobre o valor dos bens não entregues, caso se tenha ocorrido a entrega de algum bem, ou sobre o valor total do Contrato, no caso de inexecução total das obrigações assumidas, contado a partir do limite do prazo estabelecido no item anterior.

11.5.2.3. Suspensão de licitar e de contratar com o Ministério da Ciência, Tecnologia e Inovação pelo prazo de até 2 (dois) anos.

11.5.2.4. Aquele que, quando convocado dentro do prazo de validade de sua proposta, não celebrar contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedido de licitar e contratar com a União e, será descredenciado no SICAF, ou nos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da lei n° 10.520/2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste Instrumento e no contrato e das demais cominações legais.

11.5.2.5. **Declaração de inidoneidade para licitar ou contratar** com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

11.5.2.5.1. A sanção de declaração de inidoneidade é de competência exclusiva do Ministro de Estado da Ciência e Tecnologia, facultada a defesa do interessado no respectivo processo, no prazo de 10 (dez) dias da abertura de vista, podendo a reabilitação ser requerida após 2 (dois) anos de sua aplicação

11.5.3. **Os valores de multa descritos nos itens 11.5.2.2.1 a 11.5.2.2.8 somente serão aplicados após atingido o limite de 20% do Nível Mínimo de Serviço Exigido, conforme item 8 desse instrumento.**

11.5.4. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

11.5.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

11.5.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado os princípios da proporcionalidade e razoabilidade.

11.5.7. As multas devidas e/ou prejuízos causados à CONTRATANTE serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso serão inscritos na Dívida Ativa da União e cobrados judicialmente.

11.5.8. As penalidades serão obrigatoriamente registradas no SICAF.

11.5.9. As multas serão recolhidas em favor da União, no prazo de 10 (dez) dias a contar da data do recebimento da comunicação enviada pela autoridade competente, ou, quando for o caso, inscritas na Dívida Ativa da União e cobradas judicialmente.

11.5.10. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou, no caso das multas, cumulativamente, sem prejuízo de outras medidas cabíveis.

11.5.11. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração. Havendo, ainda, alguma diferença remanescente, o valor será cobrado administrativamente, podendo, inclusive, ser inscrito como dívida ativa e cobrado judicialmente.

11.5.12. Não será aplicada multa se, comprovadamente, o atraso da execução dos serviços advir de caso fortuito ou motivo de força maior.

11.5.13. As sanções previstas neste item poderão ser aplicadas cumulativamente ou não às sanções advindas da aplicação dos Níveis Mínimos de Serviços Exigidos.

11.6. CONSIDERAÇÕES GERAIS

11.6.1. O integrante técnico 1 não analisa os aspectos técnicos da solução, suas ponderações limitam-se à complacência do Planejamento da Contratação com os artefatos previstos na IN04/2010. Isso porque, tais servidores não dispõem de formação e capacidade técnica para aferir se a ferramenta é a mais adequada para a demanda.

11.6.2. Assim, salvo melhor juízo, esses integrantes técnicos normativos citados no parágrafo anterior observaram que as determinações capitaneadas pela IN04/2010 estão presente no Planejamento da Contratação.

11.6.3. E mais, a análise desses técnicos normativos não exclui a apreciação da consultoria jurídica do MCTI, a quem cabe a última palavra em matéria normativa.

11.7. ADEQUAÇÃO ORÇAMENTÁRIA

11.7.1. As despesas decorrentes da contratação, objeto deste instrumento, correrão à conta de recurso específicos consignados no Orçamento Geral da União, para os seguintes planos de trabalho:

11.7.1.1. 19.122.0750.2000.0001 – MCTI

11.7.2. As autoridades signatárias deste instrumento são os responsáveis por garantirem a compatibilidade dos serviços a serem contratados com as ações ora indicadas.

12.HISTÓRICO DE ATUALIZAÇÃO DE VERSÕES.

12.1. Histórico que acompanha a atualização de Versões desse instrumento, conforme tabela:

	Planejamento da Contratação	Termo de Referência	Observações
Processo Iniciado em 2013	23/05/2013	23/05/2013	Discussões iniciais
	16/07/2013	16/07/2013	Discussões Complementares
	19/07/2013	19/07/2013	Finalização da primeira versão impressa.
	08/08/2013	08/08/2013	1. Alterar para 36 meses a vigência do contrato com a devida justificativa 2. Alterar texto da carta do fabricante, pois será apenas para o fornecimento. 3. Alterar o texto de fiscalização a fim de adequá-lo com a portaria de fiscalização. 4. Justificar o pedido dos atestados. 5. Conferir critérios de julgamento.
	27/08/2013	27/08/2013	Finalização da segunda versão impressa.

13.ASSINATURAS

13.1. **Integrantes Técnicos 1**

O presente Termo de Referência foi elaborado em harmonia com a Instrução Normativa nº 04/2010 – Secretaria de Recursos Logísticos e Tecnologia da Informação do Ministério do Planejamento Orçamento e Gestão.

Brasília-DF, de 2013.

Mirelle Mateus Corrêa
Integrante Técnico

13.2. **Integrantes Técnicos 2**

O presente Termo de Referência está em conformidade com os requisitos técnicos necessários ao cumprimento das necessidades e objeto da contratação.

Jorge Antônio de Carvalho
Integrante Técnico

13.3. **Responsável pelo Termo de Referência**

O presente Termo de Referência está de acordo com as necessidades técnicas, operacionais e estratégicas do Ministério da Ciência, Tecnologia e Inovação.

Brasília-DF, de 2013.

Coordenador-Geral de Gestão da Tecnologia da Informação - Substituto
Samih Naif Daibes Júnior

13.4. **Integrantes Administrativos**

O presente Termo de Referência está em conformidade com os requisitos administrativos necessários ao cumprimento do objeto:

Brasília-DF, de 2013

Hugo Marcus Silva Teixeirense
Integrante Administrativo

13.1. **Responsável Administrativo pelo Termo de Referência**

O presente Termo de Referência está de acordo com os requisitos administrativos necessários ao cumprimento do objeto.

Brasília-DF, de 2013

Humberto Luciano Schloegl
Autoridade Competente da Área Administrativa

13.2. **Integrante Requisitante**

O presente Termo de Referência 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 recomendamos a contratação proposta:

Brasília-DF, de 2013.

Integrante Requisitante

13.3. **Aprovação da Área Requisitante**

O presente Termo de Referência 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 recomendamos a contratação proposta.

Brasília-DF, de 2013

Área Requisitante

14. ANEXO I-A – TERMO ENCERRAMENTO DO CONTRATO

IDENTIFICAÇÃO DO CONTRATO	
Contrato Número:	
Objeto:	
CONTRATADO:	
CONTRATANTE:	

TERMOS

Por este instrumento, as partes acima identificadas resolvem registrar o encerramento do contrato em epígrafe e ressaltar o que segue:

O contrato está sendo encerrado por motivo de *<motivo>*.

As partes concedem-se mutuamente plena, geral, irrestrita e irrevogável quitação de todas as obrigações diretas e indiretas decorrentes deste contrato, não restando mais nada a reclamar de parte a parte.

Não estão abrangidas pela quitação ora lançada e podem ser objeto de exigência ou responsabilização mesmo após o encerramento do vínculo contratual:

- As obrigações relacionadas a processos iniciados de penalização contratual;
- As garantias sobre bens e serviços entregues ou prestados, tanto legais quanto convencionais;
- A reclamação de qualquer tipo sobre defeitos ocultos nos produtos ou serviços entregues ou prestados.
- *<inserir pendências, se houverem>*

E assim tendo lido e concordado com todos seus termos, firmam as partes o presente instrumento, em duas vias iguais, para que surta seus efeitos jurídicos.

DE ACORDO	
CONTRATANTE **Gestor do Contrato**	**CONTRATADO** **Preposto**
_____ *<Nome>* Matr.:	_____ *<Nome>* Matr.:

15.ANEXO I-B– MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO.

IDENTIFICAÇÃO			
CONTRATO:		**N° DA OS / OFB:**	
OBJETO:			
CONTRATANTE:			
CONTRATADO:			

Por este instrumento, atestamos para fins de cumprimento do disposto no artigo 25, inciso III, alínea "a" da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 12/11/2010, que os serviços (ou bens), relacionados na OS. acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo CONTRATANTE. Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até xx dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Planejamento da Contratação correspondente ao Contrato supracitado.

DE ACORDO	
CONTRATANTE	**CONTRATADO**
_____ ***<Nome>*** **Mat.:**	_____ ***<Nome>*** **Mat.:**

16.ANEXO I-C – MODELO DE TERMO DE RECEBIMENTO DEFINITIVO.

IDENTIFICAÇÃO					
CONTRATO:		**N° DA OS / OFB:**		**ITEM:**	
OBJETO:					
GESTOR DO CONTRATO:					
ÁREA REQUISITANTE DA SOLUÇÃO:					

Por este instrumento, as partes acima identificadas atestam para fins de cumprimento do disposto no artigo 25, inciso III, alínea "h" da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 12/11/20010, que os serviços (ou bens) identificados acima possuem a qualidade compatível com a especificada no Planejamento da Contratação / Projeto Básico do Contrato supracitado.

DE ACORDO	
CONTRATANTE	**CONTRATADO**
_____ ***<Nome>*** **Mat.:**	_____ ***<Nome>*** **Mat.:**

_____, _____ de _____ de 20____

17.ANEXO I-D – MODELO DE APRESENTAÇÃO DA PROPOSTA DE PREÇOS.

Ao Pregoeiro

PROPOSTA que faz a empresa _____ _____, CNPJ _____, para o Aquisição de Solução Integrada de Proteção e Resposta a Incidentes de Segurança, baseada em hardware e software, incluindo instalação, configuração, suporte técnico e operação assistida, para atender as necessidades corporativas do Ministério da Ciência, Tecnologia e Inovação – MCTI, em conformidade com o Edital do Pregão Eletrônico nº _____/2013.

Item	DESCRIÇÃO	QUANTITATIVOS TOTAIS PARA REGISTRO	VALOR UNITÁRIO	VALOR TOTAL ESTIMADO (R$)
1	**Módulo de Proteção de Rede**	1		
2	Garantia e Manutenção Mensal - Módulo de Proteção de Rede	36		
3	Serviço de Implantação - Módulo de Proteção de Rede	1		
4	Serviço de Treinamento - Módulo de Proteção de Rede	1		
5	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	36		
6	**Módulo de Análise de Rede**	1		
7	Garantia e Manutenção Mensal - Módulo de Análise de Rede	36		
8	Serviço de Implantação - Módulo de Análise de Rede.	1		
9	Serviço de Treinamento - Módulo de Proteção de Rede	1		
10	Serviço de Suporte Técnico Mensal - Módulo de Proteção de Rede	36		
11	**Módulo de Visibilidade e Análise de Dados**	1		
12	Garantia e Manutenção Mensal - Módulo de Visibilidade e Análise de Dados	36		
13	Serviço de Implantação - Módulo de Visibilidade e Análise de Dados	1		
14	Serviço de Treinamento - Módulo de Visibilidade e Análise de Dados	1		
15	Serviço de Suporte Técnico Mensal - Módulo de Visibilidade e Análise de Dados	36		
16	**Serviços de Operação Assistida (UST)**	2000		

O prazo de validade de nossa proposta é de 60 (sessenta) dias corridos, contados da data da abertura da licitação.

Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas nos documentos de contratação.

Declaramos que no preço estão inclusos todos os custos, despesas, tributos, para a perfeita execução do objeto.

Caso nos seja adjudicado o objeto da licitação, comprometemos a assinar o Contrato no prazo determinado no documento de convocação, e para esse fim fornecemos os seguintes dados:

Razão Social: _____CNPJ/MF: _____

Endereço:_____ Tel./Fax: _____

CEP: _____ Cidade: _____ UF: _____

Banco: _____ Agência: _____ nº c/c: _____

Dados do Representante Legal da Empresa para assinatura do Contrato:

Nome: _____

Endereço:_____

CEP: _____ Cidade: _____`_____ UF: _____

CPF/MF: _____ Cargo/Função: _____

Cart. ldent nº: _____ Expedido por: _____

Naturalidade: _____ Nacionalidade: _____

Local e Data._____

[Nome do Representante da Empresa Emitente]

18.ANEXO I-E – MODELO DE ABERTURA DE CHAMADO.

Nº do CHAMADO		**Data e Hora de Emissão:**	
Nº DO REGISTRO			
SOLICITANTE			
DESCRIÇÃO DA OCORRÊNCIA			
DADOS DO EQUIPAMENTO			

DE ACORDO	
CONTRATANTE	**CONTRATADO**
_____ ***<Nome>*** **Mat.:**	_____ ***<Nome>*** **Mat.:**

19.ANEXO I-F – MODELO DE DECLARAÇÃO DE PLENO CONHECIMENTO E ATENDIMENTO ÀS EXIGÊNCIAS DE HABILITAÇÃO

_____, inscrita no CNPJ nº _____, por intermédio do seu representante legal abaixo assinado, declara sob as penalidades legais, para fins do disposto no § 2º, art. 32, da Lei 8.666/93, que até a presente data inexiste fato superveniente impeditivo para sua habilitação no presente processo licitatório, estando ciente da obrigatoriedade de declarar ocorrências posteriores.

_____, ___ de _____de _____

_____

Assinatura e nome do representante legal da empresa

Cargo/Função

20.ANEXO I-G – MODELO DE TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, com sede em Brasília-DF, inscrito no CNPJ sob o nº 01263896/0003-26**,** doravante denominado MCTI e .....**NOME DA EMPRESA.....,** pessoa jurídica com sede na ....., inscrita no CNPJ/MF sob o n.º ..., doravante denominada NOME DA EMPRESA e, sempre que em conjunto referidas como PARTES para efeitos deste TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO, doravante denominado simplesmente TERMO, e,

CONSIDERANDO que, em razão do atendimento à exigência do Contrato MCTI Nº ..., celebrado pelas PARTES, doravante denominado CONTRATO, cujo objeto é a ....., mediante condições estabelecidas pelo MCTI;

CONSIDERANDO que o presente TERMO vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de INFORMAÇÕES, que a NOME DA EMPRESA tiver acesso em virtude da execução contratual;

CONSIDERANDO a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do MCTI de que a NOME DA EMPRESA tomar conhecimento em razão da execução do CONTRATO, respeitando todos os critérios estabelecidos aplicáveis às INFORMAÇÕES; O MCTI estabelece o presente TERMO mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DO OBJETO

O objeto deste TERMO é prover a necessária e adequada proteção às INFORMAÇÕES do MCTI, principalmente aquelas classificadas como CONFIDENCIAIS, em razão da execução do CONTRATO celebrado entre as PARTES.

CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS

a) As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer INFORMAÇÕES reveladas pelo MCTI;

b) A NOME DA EMPRESA se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer INFORMAÇÕES que venham a ser fornecidas pelo MCTI, a partir da data de assinatura deste TERMO, devendo ser tratadas como INFORMAÇÕES CONFIDENCIAIS, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo MCTI;

c) A NOME DA EMPRESA se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das INFORMAÇÕES do MCTI;

d) O MCTI, com base nos princípios instituídos na Segurança da Informação, zelará para que as INFORMAÇÕES que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela NOME DA EMPRESA.

CLÁUSULA TERCEIRA – DAS LIMITAÇÕES DA CONFIDENCIALIDADE

a) As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

a1) Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES;

a2) Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

a3) Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as PARTES cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES ADICIONAIS

a) A NOME DA EMPRESA se compromete a utilizar as INFORMAÇÕES reveladas exclusivamente para os propósitos da execução do CONTRATO;

b) A NOME DA EMPRESA se compromete a não efetuar qualquer cópia das INFORMAÇÕES sem o consentimento prévio e expresso do MCTI;

b1) O consentimento mencionado na alínea “b”, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das PARTES;

c) A NOME DA EMPRESA se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste TERMO e da natureza confidencial das INFORMAÇÕES do MCTI;

d) A NOME DA EMPRESA deve tomar todas as medidas necessárias à proteção das INFORMAÇÕES do MCTI, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo MCTI;

e) Cada PARTE permanecerá como única proprietária de todas e quaisquer INFORMAÇÕES eventualmente reveladas à outra parte em função da execução do CONTRATO;

f) O presente TERMO não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

f1) Os produtos gerados na execução do CONTRATO, bem como as INFORMAÇÕES repassadas à NOME DA EMPRESA, são única e exclusiva propriedade intelectual do MCTI;

g) A NOME DA EMPRESA firmará acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao CONTRATO, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento;

h) A NOME DA EMPRESA obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às INFORMAÇÕES que venham a ser reveladas durante a execução do CONTRATO;

CLÁUSULA QUINTA – DO RETORNO DE INFORMAÇÕES

a) Todas as INFORMAÇÕES reveladas pelas PARTES permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

CLÁUSULA SEXTA – DA VIGÊNCIA

a) O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até 5 (cinco) anos após o término do contrato.

CLÁUSULA SÉTIMA – DAS PENALIDADES

a) A quebra do sigilo e/ou da confidencialidade, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO firmado entre as PARTES. Neste caso, a NOME DA EMPRESA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo MCTI, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial.

CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS

a) Este TERMO constitui vínculo indissociável ao CONTRATO, que é parte independente e regulatória deste instrumento;

b) O presente TERMO constitui acordo entre as PARTES, relativamente ao tratamento de INFORMAÇÕES, principalmente as CONFIDENCIAIS, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas PARTES em ações feitas direta ou indiretamente;

c) Surgindo divergências quanto à interpretação do pactuado neste TERMO ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os princípios da legalidade, da equidade, da razoabilidade, da economicidade, da boa fé, e, as preencherão com estipulações que deverão corresponder e resguardar as INFORMAÇÕES do MCTI;

d) O disposto no presente TERMO prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à confidencialidade de INFORMAÇÕES;

e) A omissão ou tolerância das PARTES, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA NONA - DO FORO

a) O MCTI elege o foro de Brasília-DF, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, é assinado o presente TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO, pela NOME DA EMPRESA, sendo em 2 (duas) vias de igual teor e um só efeito.

Nome

Diretor

NOME DA EMPRESA

21. ANEXO I-H – MODELO DE FICHA DE AVALIAÇÃO

Entregue aos participantes no final do último dia pode ser vista abaixo.

Ficha de Avaliação

Marque com um "X" o conceito que melhor representa sua opinião sobre este curso:
1=Deficitário; 2=Regular; 3=Bom; 4=Muito Bom; 5=Excelente

Item de Avaliação	ITENS DE VERIFICAÇÃO	Notas				
		1	2	3	4	5
1	Metodologia utilizada					
2	Distribuição da programação					
3	Desempenho dos instrutores					
4	Adequação da carga horária					
5	Contribuição para a melhoria da qualidade do seu trabalho					
6	Adequação do conteúdo das aulas ao objetivo do curso					
7	Aulas práticas					
8	Participação pessoal					
9	Material audiovisual					
10	Instalações das aulas práticas					

Registre:
A. Aspectos Positivos
B. Aspectos Negativos
C. Sugestões