ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO (ETP)
Documento nº 02500.035284/2023-44

DEMANDA	Contratação de empresa especializada para a prestação de serviços de segurança cibernética para a Agência Nacional de Águas e Saneamento Básico – ANA.
DATA	16/05/2023

INTRODUÇÃO
De acordo com o Art. 1 da IN SGD/ME Nº 1/2019, o Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação. Além disso, segundo o Art.12 da mesma IN, cabe à Equipe de Planejamento da Contratação a elaboração do Estudo Técnico Preliminar da Contratação.

1 Descrição da Demanda

Contratação de empresa especializada para a prestação de serviços de segurança cibernética para a Agência Nacional de Águas e Saneamento Básico – ANA. Esta contratação visa oferecer condições para se garantir a disponibilidade, confidencialidade, sigilo e a continuidade dos serviços e programas institucionais sustentados pelo ambiente de Tecnologia da Informação e Comunicação (TIC) da ANA, sendo necessário:

- Gerar relatórios que permitam garantir a efetividade de controles de segurança, assim como uma visão do estado atual e histórico de ocorrências;
- Analisar o ambiente, coletando informações e evidências de suspeitas de ataques possibilitando o tratamento e a tomada de decisão em caso de identificação de ataques;
- Permitir a identificação de tentativas ou acessos, aceitos ou rejeitados, ao ambiente computacional da ANA;
- Implantar níveis de segurança alinhados aos padrões ISO-27001, ISO-27002, ISO-27005, ISO-27011 e ISO 27014;

- Monitoramento completo dos eventos de segurança dos ativos de informação;
- Manutenção de análise histórica dos eventos de segurança, coletando e correlacionando os eventos;
- Detectar atividades não autorizadas de processamento de informações;
- Dispor de meios para operação, administração e atendimento de requisições relacionadas às ferramentas e soluções de segurança disponíveis no ambiente tecnológico da ANA;
- Dispor de meios para identificação e correção de vulnerabilidades de segurança da informação no ambiente e sistemas críticos da ANA a fim de evitar que ataques cibernéticos obtenham sucesso explorando vulnerabilidades conhecidas;
- Operacionalizar a Gestão de Riscos de Segurança da Informação;
- Facilitar a identificação preventiva de ameaças emergentes ou invasões externas além de prevenir eventuais vazamentos de informações antes da divulgação pública;
- Implantar processo estruturado e instrumentalizado de gerenciamento de incidentes de segurança da informação, em que as etapas de triagem, classificação, análise, resposta e comunicação sigam as melhores práticas internacionais;
- Redução dos riscos de interrupção dos serviços e sistemas em decorrência da ataques cibernéticos;
- Criar bases históricas e estatísticas de incidentes, permitindo traçar tendências ou pontos que necessitam de aprimoramento;
- Responder mais rapidamente aos ataques cibernéticos;
- Desenvolver resiliência e melhorar a capacidade da TI de enfrentar eventos adversos relacionados a cibersegurança;
- Investir no desenvolvimento de processos de trabalho seguros, ao invés de apenas investir em tecnologia;
- Definição clara dos objetivos, produtos, prazos, custos, padrões de qualidade, responsabilidades das partes, além de indicadores de desempenho; e
- Melhoria da percepção do adequado gerenciamento de segurança de Segurança da Informação por parte da alta administração e dos usuários internos e externos, deixando transparente que há efetivo gerenciamento dos incidentes de segurança de tecnologia da informação.

Visto que, no quadro funcional da Agência, ainda não há servidores especializados e qualificados para a prestação dos serviços em questão, torna-se necessária a imediata alocação dos serviços demandados. Essa alocação é essencial para garantir o bom andamento dos serviços da ANA. Em caso de incidentes, a falta desses serviços pode acarretar graves consequências para toda a infraestrutura de informática que depende deles, resultando em falhas catastróficas nos equipamentos do datacenter. Essas falhas causariam perdas físicas e paralisariam parte essencial dos serviços prestados à sociedade, colocando em risco tanto as atividades meio quanto as atividades finalísticas da ANA. Diante dessa situação, fica evidente a urgência na contratação e o alto risco de danos e prejuízos caso a contratação não seja bem-sucedida.

A seguir, são apresentados os Serviços Continuados de Segurança para atender às necessidades e requisitos da ANA:

- **Serviços de Gestão de Vulnerabilidades,** o objetivo desse serviço é identificar as possíveis vulnerabilidades de segurança da informação no ambiente da **ANA** (infraestrutura e aplicações), que seriam vetores de ataques e fixar uma blindagem contra a exploração dessas vulnerabilidades, evitando que ataques cibernéticos obtenham sucesso. Espera-se da **CONTRATADA** as orientações, o acompanhamento e a verificação das aplicações das correções de vulnerabilidade.
- **Serviços de Gestão de Segurança para Infraestrutura e Sistemas Críticos**, esse serviço visa avaliar continuamente e ininterruptamente os acessos aos sistemas críticos por meio de credenciais administrativas. Os eventos gerados serão analisados, sendo em caso positivo, transformados em um incidente de segurança da informação, obedecendo um processo rigoroso de gestão de eventos.
- **Serviços de Monitoramento de Ataques Cibernéticos,** o objetivo desse serviço é monitorar todo e qualquer tipo de ataque cibernético direcionado à **ANA**, através da análise de correlações de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, e em casos positivos, transformados em um incidente de segurança da informação, obedecendo um processo rigoroso de gestão de eventos.
- **Serviços de Resposta a Incidentes de Segurança Cibernética,** o objetivo desse serviço é analisar, remediar, conter e documentar os eventos de segurança da informação, e caso descubra um ataque iminente, deve transformar em um incidente de segurança da informação. Esse serviço é executado por um **CSOC** do inglês *Cyber Security Operations Center*, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas.
- **Serviços de Gestão de Proteção de Endpoints e Servidores de Rede**, seu objetivo é proteger as estações de trabalho e os equipamentos servidores de rede corporativos, de forma eficiente, bloqueando a entrada e saída de informações críticas ou sensíveis, bem como examinar todo o conteúdo em busca de vírus, malwares, botnets ou outras ameaças avançadas.
- **Serviços de Proteção de Mensageria Proativa**, seu objetivo é proteger o serviço de mensageria utilizado pelos usuários internos, de forma eficiente, bloqueando a entrada e saída de e-mails indesejáveis, bem como examinar todo o conteúdo em busca de vírus, spams, phishing, botnets, ameaças avançadas, vazamento de informações, entre outros.
- **Serviços de Inteligência Aplicada a Segurança Cibernética**, tem por objetivo o monitoramento e a eliminação das informações, de qualquer tipo, relativa a **ANA**, suas autoridades e demais servidores que estejam trafegando ou sendo negociadas nas redes web consideradas perigosas ou seja nas **Dark Web e Deep Web**.
- **Serviços de Testes de Invasão (Pentest)** terá como objetivo identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas,

processos e ativos de infraestrutura tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas especificas para tentar obter acesso não autorizado e privilegiado aos ativos e informações da Instituição.

- **Serviços de Conscientização da Segurança da Informação,** para conscientização de todos os usuários do parque tecnológico do **ANA**, sobre a importância de seguir as políticas de segurança da informação estabelecidas. Identificando proativamente os usuários que seriam vetores de ataques, e tornando-os elegíveis para um programa de capacitação interna, sobre boas práticas de segurança da informação no ambiente corporativo do **ANA**.

Anexo a este ETPC se apresenta o escopo e o modelo de execução pretendido para o objeto.

2 Definição e Especificação das Necessidades

A Superintendência de Tecnologia da Informação e Comunicação da ANA sustenta diversos sistemas que são disponibilizados aos usuários internos e externos por meio de portais e sistemas acessíveis via internet. Essa dinâmica de uso está fortemente ligada à infraestrutura tecnológica, sendo que a interação com a população ocorre principalmente por meio desses canais online. Embora esse modelo traga inúmeros benefícios em termos de disponibilidade e facilidade de acesso, também expõe a Agência a diversos riscos cibernéticos, como acesso indevido a informações restritas e indisponibilidade dos sistemas devido a eventos adversos resultantes de ações maliciosas orquestradas por hackers ou grupos com interesses diversos.

Nesse contexto, considerando que alguns desses sistemas são baseados em dados pessoais de terceiros e outros tipos de dados sensíveis, a proteção dessas informações se torna um desafio ainda maior. Além disso, a entrada em vigor da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) em setembro de 2020, o Plano de Dados Abertos (PDA) e o Marco Civil da Internet (Lei n° 12.965/2014) estabelecem regras para o acesso e o uso adequado dessas informações pessoais. Essas regulamentações atualizaram as diretrizes de segurança no ambiente de Tecnologia da Informação, visando à proteção e conservação dos dados, bem como à privacidade das pessoas. Instituições que não cumprem adequadamente essas normas estão sujeitas a sanções, incluindo multas significativas. Portanto, a fim de proteger os dados pessoais dos usuários da Rede ANA e cumprir as exigências legais mencionadas, é essencial investir em ferramentas e recursos tecnológicos para segurança da informação.

Diante dos desafios impostos pela transformação digital das organizações públicas e pela dependência tecnológica exacerbada pela pandemia de Covid-19, que levou as organizações a expandir seus ambientes de trabalho no formato remoto, tornou-se ainda mais visível e vulnerável a ameaças, como roubo de informações e aumento expressivo de casos de *ransomware*. Para mitigar esses riscos e garantir a segurança de nossos sistemas e dados, é imprescindível contar com um serviço especializado de SOC e segurança cibernética.

Por meio do TC 001.873/2020-2, relatado pelo Ministro Vital do Rêgo, o Tribunal de Contas da União (TCU) destacou a importância de atenção governamental em relação aos ataques cibernéticos. Tal avaliação, registrada no Acórdão 4.035/2020-TCU-Plenário, disponível no link, o órgão de controle conduziu um

levantamento com o objetivo de conhecer a macroestrutura de governança e gestão de segurança da informação e segurança cibernética na Administração Pública Federal (APF). Esse levantamento abrange aspectos relacionados à legislação, políticas, normativos, atores, papéis e responsabilidades no contexto dessas áreas.

Essas fontes de referência evidenciam a relevância e a necessidade de priorizar a segurança cibernética na Administração Pública Federal. As conclusões e recomendações apontadas pelo TCU destacam a importância de fortalecer a governança e a gestão da segurança da informação, bem como a adoção de medidas preventivas e corretivas para mitigar os riscos cibernéticos.

Diante desse contexto, é fundamental que a Agência Nacional de Águas (ANA) reconheça a importância estratégica de investir em serviços de SOC (Security Operations Center) e segurança cibernética. Esses serviços desempenham um papel fundamental na detecção, prevenção e resposta a possíveis ataques cibernéticos, protegendo os sistemas da Agência contra ameaças e garantindo a continuidade das operações de forma segura.

Considerando as recomendações do TCU e a crescente sofisticação dos ataques cibernéticos, é imprescindível que a ANA inclua em sua licitação a contratação de serviços especializados de SOC e segurança cibernética, a fim de fortalecer sua infraestrutura de tecnologia da informação e garantir a proteção de dados sensíveis, bem como o cumprimento das normas e regulamentos aplicáveis.

O investimento nesses serviços permitirá à ANA criar uma cultura de segurança cibernética sólida, protegendo os sistemas e dados da Agência contra possíveis ameaças, além de atender às recomendações do TCU e às exigências legais pertinentes. Dessa forma, a Agência estará alinhada com as melhores práticas de segurança da informação e poderá enfrentar os desafios cibernéticos com maior eficácia e confiança.

Em decorrência das deliberações expostas no Acórdão supra o TCU está realizando acompanhamento de controles críticos de Segurança Cibernética (SegCiber) das organizações públicas federais em total aderência com a versão 8 do framework do Center for Internet Security (CIS) (https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/).

Diante disso o TCU, conforme visto acima, adotou o ecossistema de controles CIS como base para a autoavaliação do grau evolutivo a respeito da maturidade de Segurança da Informação. Este acompanhamento será subdividido em sete ciclos sendo que cada um desses ciclos irá privilegiar disciplinas distintas. No final todas as 153 medidas de segurança contidas no framework do CIS v8.

O objetivo principal aqui é realizar uma análise aprofundada do modelo de contratação em que o provedor de serviços assume a responsabilidade pela gestão dos profissionais e suas entregas, ajustando sua equipe de acordo com as necessidades para cumprir as metas de Níveis Mínimos de Serviços estabelecidas pelo CONTRATANTE.

Esse modelo tem como finalidade não apenas atender às exigências legais, mas também estabelecer padrões de qualidade e indicadores de fácil mensuração, visando melhorias na qualidade e produtividade dos serviços. Além disso, busca facilitar o processo de custeio e orçamentação, bem como simplificar a gestão e fiscalização do CONTRATO.

Ao adotar esse modelo de contratação, espera-se alcançar os seguintes benefícios:

- Melhoria na qualidade dos serviços: Através da definição de padrões de qualidade e indicadores mensuráveis, será possível elevar o nível de excelência na entrega dos serviços contratados.
- Aumento da produtividade: Ao adequar o quadro de profissionais de acordo com as demandas específicas, haverá uma maior eficiência na execução das tarefas, resultando em um aumento da produtividade.
- Facilidade de custeamento e orçamentação: Esse modelo de contratação proporciona uma maior facilidade na estimativa de custos e no planejamento orçamentário, uma vez que os serviços são contratados com base em metas e indicadores pré-definidos.
- Simplificação da gestão e fiscalização: Com a responsabilidade pela gestão dos profissionais e suas entregas sob a responsabilidade do provedor de serviços, a tarefa de gerenciar e fiscalizar o contrato torna-se mais simples e eficiente para o CONTRATANTE.

Dessa forma, ao adotar esse modelo de contratação, busca-se uma maior eficácia na prestação dos serviços, aliada a uma gestão mais simplificada e um melhor controle dos resultados obtidos. Isso contribuirá para o alcance dos objetivos estabelecidos pelo CONTRATANTE, proporcionando um ambiente de trabalho mais eficiente e produtivo.

Considerando as necessidades demandadas se faz necessária a Contratação de empresa especializada para o fornecimento de serviços continuados de segurança cibernética, compreendendo:

Lote	Item	Descrição	Unid. Referência	Quant. Anual
1	1	Serviços de Gestão de Vulnerabilidades	mês	12
	2	Serviços de Gestão de Segurança para Infraestrutura e Sistemas Críticos	mês	12
	3	Serviços de Monitoramento de Ataques Cibernéticos	mês	12
	4	Serviços de Resposta a Incidentes de Segurança Cibernética	mês	12
	5	Serviços de Gestão de Segurança de Endpoints e Servidores de Rede	mês	12
	6	Serviços de Segurança de Mensageria Proativa	mês	12
	7	Serviços de Inteligência Aplicada a Segurança Cibernética	mês	12
	8	Serviços de Conscientização da Segurança da Informação	mês	2
2	9	Serviços de Testes de Invasão (Pentest)	mês	6

Justificativa para o não fracionamento do objeto,

Embora a Lei 8666/1993 estabeleça o parcelamento como regra geral para obras, serviços e compras, a presente licitação justifica a divisão do objeto em

dois lotes distintos: um destinado ao *pen test* (item 9) e outro contendo as demais ferramentas.

A decisão de adotar essa abordagem leva em consideração as seguintes justificativas:

- Dificuldade logística e operacional: Caso o objeto fosse fracionado e diferentes empresas fossem contratadas para fornecer os serviços separadamente, haveria desafios significativos em termos de logística e coordenação operacional. A integração e a gestão entre essas empresas poderiam ser complexas e demandariam esforços adicionais para garantir a sincronia das atividades.
- Necessidade de trabalho integrado: A natureza dos serviços em questão exige uma abordagem integrada, em que as diversas ferramentas e serviços sejam interligados de forma harmoniosa. Ao manter esses elementos em um único lote, é possível assegurar uma implementação mais eficiente e uma melhor integração entre as soluções.
- Custo de gestão: A contratação de várias empresas para fornecer serviços fracionados resultaria em um aumento dos custos de gestão, uma vez que seria necessário coordenar e monitorar o desempenho de cada fornecedor individualmente. Consolidar o objeto em dois lotes reduz a complexidade administrativa e facilita a gestão dos contratos.
- Segregação de funções e fiscalização: A separação do *pen test* em um lote distinto se justifica pelo princípio de segregação de funções, de certa maneira amparado no artigo 67 da Lei 8.666/1993 que prevê a possibilidade de contratação de empresa especializada para exercer a função de fiscalização dos contratos firmados pela Administração Pública. O pen test, além de avaliar a segurança da infraestrutura e sistemas, também funciona como uma forma de fiscalização da qualidade dos demais serviços. Ao manter o pen test separado, é possível garantir uma avaliação imparcial e independente, fortalecendo a fiscalização e a qualidade dos serviços contratados.

Dessa forma, baseado nas disposições legais vigentes, a divisão do objeto em dois lotes visa atender às necessidades de integração, qualidade, eficiência e fiscalização, proporcionando a solução mais adequada e vantajosa para a contratação dos serviços em questão.

Justificativa para vedação de participação de consórcios e cooperativas na presente licitação,

Embora não seja aplicável ao caso (conforme explanado acerca da norma vigente), vale citar que a nova Lei nº 14.133/2021, que estabelece o novo regime jurídico das licitações e contratos administrativos, manteve a possibilidade de a Administração Pública exigir a formação de consórcios em licitações para a execução de obras e serviços, nos termos do seu artigo 184.

No escopo da Lei nº 8.666/93, a adesão de consórcios em processos licitatórios é uma prerrogativa discricionária do poder público, o qual deve examinar com atenção as circunstâncias e peculiaridades de cada situação para determinar se permitirá, ou não, a criação de consórcios. A possibilidade de permitir a participação de

consórcios e cooperativas em processos licitatórios é uma escolha discricionária do poder público, tal como estabelecido no artigo 33 da Lei nº 8.666/93.

Isso significa que a Administração pode decidir se permitirá ou não a participação de consórcios e cooperativas em suas licitações, levando em consideração as peculiaridades e necessidades de cada caso específico.

Essa decisão discricionária pode ser fundamentada em diversos fatores, como a complexidade do objeto licitado, a disponibilidade de empresas ou organizações que atendam aos requisitos do edital, a capacidade técnica e financeira dos consórcios e cooperativas interessados, entre outros. Entre as **vantagens** da formação de consórcios para participação em licitações, que em tese poderiam beneficiar esta Casa, caberia destacar:

- Maior capacidade técnica e financeira: a união de empresas em consórcio pode resultar em uma maior capacidade técnica e financeira para a execução do objeto licitado, o que pode ser especialmente útil em casos de obras e serviços de grande porte ou complexidade.
- Redução de riscos: a formação de consórcios pode ajudar a reduzir os riscos da execução do objeto licitado, uma vez que os consorciados respondem solidariamente pelos atos praticados em conjunto.
- Ampliação da concorrência: a formação de consórcios pode ampliar a concorrência em licitações, permitindo que empresas de menor porte ou com menor capacidade técnica e financeira participem de forma conjunta.

No entanto, é importante destacar que a formação de consórcios também apresenta **desvantagens**, como a dificuldade de gestão do consórcio e a necessidade de estabelecer uma boa comunicação e alinhamento entre os consorciados. Dentre outras desvantagens que se deve ressaltar:

- Falta de responsabilização: a participação de um consórcio pode dificultar a responsabilização de uma única empresa pelo cumprimento do contrato, em caso de problemas ou falhas. Isso pode resultar em disputas sobre a responsabilidade entre as empresas do consórcio, atrasos na entrega do serviço ou obra, ou mesmo na falta de solução para um problema.
- Dificuldades na gestão do contrato: a gestão de um contrato que envolve um consórcio pode ser mais complexa e trabalhosa do que a gestão de um contrato com uma única empresa. Isso ocorre porque há várias empresas envolvidas, com diferentes culturas organizacionais e modos de operação, o que pode resultar em dificuldades de comunicação, falta de harmonia e dificuldade de coordenação das atividades.
- Riscos de conflitos de interesses: em alguns casos, a formação de consórcios pode levar a situações em que as empresas do consórcio têm interesses conflitantes. Isso pode ocorrer, por exemplo, quando as empresas participantes do consórcio são concorrentes em outras áreas de atuação, ou quando há diferenças de objetivos ou metas entre as empresas.

- Possibilidade de concentração de mercado: a formação de consórcios pode resultar em uma concentração de mercado em algumas áreas, especialmente quando há poucas empresas capazes de formar um consórcio para disputar determinados contratos. Isso pode resultar em prejuízos para a concorrência, prejudicando a competitividade e reduzindo as opções disponíveis para a administração pública.

Em conclusão, tendo em vista os argumentos expostos (e a magnitude do risco e das desvantagens), a vedação atual da participação de consórcios e cooperativas se justifica plenamente.

Requisitos Legais,

O presente Termo de Referência foi elaborado em conformidade com os seguintes regramentos e demais normas pertinentes:

- Lei Federal Nº 8.666, de 21 de junho de 1993 e alterações: institui normas para licitações e contratos da Administração Pública e dá outras providências;
- Lei Nº 10.520, 17 de julho de 2002: institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;
- Decreto Nº 10.024, de 20 de setembro de 2019: regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;
- Decreto Nº 3.722, de 9 de janeiro de 2001 e alterações: dispõe sobre o Sistema de Cadastramento Unificado de Fornecedores - SICAF;
- Instrução Normativa SLTI/MPOG Nº 3, de 26 de abril de 2018: estabelece regras de funcionamento do Sistema de Cadastramento Unificado de Fornecedores – SICAF, no âmbito do Poder Executivo Federal;
- Decreto Nº 7.174, 12 de maio de 2010: regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal;
- Instrução Normativa SGD/ME Nº 01, de 4 de abril de 2019 (IN 01/2019): dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação – TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal;
- Instrução Normativa ME Nº 73, de 5 de agosto de 2020: dispõe sobre os procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral;
- Lei Nº 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD);
- Portaria Normativa Nº 5, de 14 de julho de 2005 SLTI/MP – Padrões de interoperabilidade;
- Instrução Normativa N° 05, de 26 de maio de 2017, a qual dispõe sobre regras e diretrizes do procedimento de contratação de serviços sob o regime de

execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

- Decreto Nº 9.637, de 26 de dezembro de 2018: institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação; Instrução Normativa GSI/PR N° 01, de 13 de junho de 2008: disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências e suas normas complementares, Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020: dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
- Instrução Normativa PR/GSI nº 5, de 30 de agosto de 2021: Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

Requisitos de Manutenção,

- Suporte técnico: O licitante selecionado deve fornecer suporte técnico abrangente para os serviços adquiridos durante o período contratual. O suporte deve incluir assistência para instalação, configuração, solução de problemas e atualizações de software.
- Atualizações e Patches: O licitante deve garantir que todas as atualizações de software e patches lançados sejam prontamente disponibilizados aos usuários finais. Isso inclui a implementação de medidas para garantir que os sistemas estejam sempre atualizados e protegidos contra vulnerabilidades de segurança.
- Monitoramento e Relatórios: O licitante deve possuir sistemas de monitoramento adequados para rastrear o uso das ferramentas e fornecer relatórios precisos e transparentes sobre a conformidade e o uso efetivo das licenças.
- Gestão de Ativos: O licitante deverá fornecer soluções e práticas eficientes para a gestão de ativos de software, garantindo o licenciamento adequado, a conformidade com os termos de uso e a otimização dos investimentos nos serviços.
- Vigilância de Licenças: O licitante deve estar preparado para realizar auditorias de licenças de software, conforme necessário, para garantir a conformidade contínua com os termos de licenciamento.
- Atualizações de Tecnologia: O licitante deverá manter-se atualizado sobre as tendências e desenvolvimentos tecnológicos relacionados aos serviços prestados, a fim de fornecer recomendações relevantes para aprimorar a eficiência e o valor dos ativos de software.

Requisitos Temporais,

- Prazo Contratual: O contrato terá um prazo específico indicado no edital. Os licitantes devem estar cientes do período exato de duração do contrato e garantir que possuam a capacidade de fornecer suporte e serviços durante todo o período estabelecido.

- Implementação: O licitante selecionado deverá apresentar um cronograma detalhado para a implementação dos serviços. Isso inclui prazos para a entrega das licenças, instalação, configuração e integração com os sistemas existentes.
- Atualizações e Patches: O licitante deve fornecer atualizações e patches de software de forma oportuna. Deve haver um compromisso claro com a disponibilização regular de atualizações e patches durante todo o período contratual.
- Renovações: O edital deve estabelecer os procedimentos e prazos para renovação das licenças ao final do contrato inicial. Os licitantes devem estar preparados para gerenciar esse processo de renovação e garantir que seja concluído dentro do prazo estabelecido.
- Suporte Técnico: O licitante selecionado deve fornecer suporte técnico contínuo durante todo o período contratual. Isso inclui a disponibilidade de pessoal qualificado para responder a consultas, resolver problemas e fornecer assistência técnica de acordo com os termos estabelecidos no contrato.
- Vigência de Licenças: O licitante deve garantir que os serviços adquiridos tenham uma vigência adequada, de acordo com as necessidades da organização.

Requisitos de Segurança,

- A CONTRATADA deve seguir as orientações de segurança da ANA e legislação pertinente ao assunto.
- A CONTRATADA deverá submeter-se aos procedimentos contidos nas normas de segurança corporativa da ANA e da Administração Pública em todos os eventos em que for necessária a presença de seus prepostos e/ou funcionários nas dependências da Agência.
- A CONTRATADA deverá exigir dos seus empregados, quando em serviço nas dependências da CONTRATANTE, o uso obrigatório de uniformes e crachás de identificação.
- A CONTRATADA não poderá se utilizar da presente contratação para obter qualquer acesso não autorizado as informações de propriedade da CONTRATANTE.
- A CONTRATADA deverá assinar o Termo de Compromisso, e seus funcionários alocados na prestação de serviços, o Termo de Ciência, conforme modelos que estarão anexos ao Termo de Referência.
- A CONTRATADA deverá comunicar imediatamente a CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão de funcionários envolvidos diretamente na execução do objeto, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do CONTRATANTE, porventura colocados à disposição para realização dos serviços contratados.

Requisitos Sociais, Ambientais, Culturais e de Sustentabilidade,

Durante a execução de tarefas no ambiente do CONTRATANTE ou das demais instituições públicas envolvidas, os colaboradores da empresa fornecedora

deverão observar, no trato com os servidores e o público em geral, a urbanidade e os bons costumes de comportamento, tais como: asseio, pontualidade, cooperação, respeito mútuo, discrição e zelo com o patrimônio público. Deverão ainda portar identificação pessoal, de acordo com as normas internas das instituições.

Os produtos gerados em função da prestação dos serviços, bem como todas as documentações, deverão ser entregues no idioma português do Brasil (pt-BR), com exceção de termos técnicos usuais que poderão ser apresentados em língua estrangeira.

E ainda com o objetivo de promover uma relação contratual responsável e alinhada com os princípios de sustentabilidade, respeito aos direitos humanos, valorização da cultura e ética empresarial deverá observar na execução do objeto (sempre que couber) os seguintes requisitos:

- Responsabilidade Social: a) Observar e respeitar os direitos humanos, garantindo igualdade de oportunidades e não-discriminação em todas as suas atividades. b) Promover a diversidade e a inclusão, valorizando a equidade de gênero, etnia, idade, orientação sexual e demais características individuais. c) Estimular a contratação de mão de obra local e a capacitação de profissionais da região, contribuindo para o desenvolvimento econômico e social.
- Sustentabilidade Ambiental: a) Adotar práticas sustentáveis em suas operações, promovendo a economia de recursos naturais, a redução da emissão de gases de efeito estufa e o uso eficiente de energia. b) Gerenciar de forma adequada os resíduos gerados durante a prestação dos serviços, priorizando a coleta seletiva, a reciclagem e a destinação correta. c) Respeitar e adotar normas ambientais vigentes, visando à preservação dos ecossistemas e à mitigação de impactos ambientais adversos.
- Preservação Cultural: a) Respeitar e valorizar a diversidade cultural local, observando as tradições, costumes e patrimônio histórico. b) Promover ações que valorizem a cultura regional.
- Transparência e Ética: a) Cumprir rigorosamente as leis, regulamentos e normas éticas relacionadas à prestação dos serviços, garantindo a integridade e a transparência em todas as atividades. b) Assegurar a confidencialidade das informações da Agência e dos dados dos usuários, implementando medidas adequadas de segurança da informação.

Requisitos de Arquitetura Tecnológica,

A presente contratação busca garantir que as ferramentas de segurança cibernética e SOC atendam às demandas específicas da Agência, proporcionando uma estrutura sólida e efetiva para a proteção dos sistemas e dados contra ameaças cibernéticas. A seguir, estão alguns requisitos arquitetônicos que devem ser observados pelas licitantes:

- Escalabilidade: A arquitetura das ferramentas deve ser dimensionada para lidar com o crescimento do ambiente de TI da organização. Deve permitir o aumento da capacidade de processamento, armazenamento e análise de dados, acompanhando as demandas em constante evolução.

- Resiliência: A arquitetura deve ser projetada para garantir a continuidade dos serviços de segurança mesmo diante de falhas ou interrupções. Deve incluir mecanismos de redundância, recuperação e alta disponibilidade para minimizar o impacto de eventos adversos no funcionamento das ferramentas.
- Integração: As ferramentas de segurança cibernética e SOC devem ter a capacidade de se integrar com outros sistemas e dispositivos presentes no ambiente de TI da organização. A arquitetura deve suportar a troca de informações e a interoperabilidade com diferentes plataformas e tecnologias, garantindo uma visão abrangente da segurança.
- Segurança: A arquitetura deve seguir boas práticas de segurança e adotar medidas robustas para proteger os dados e garantir a confidencialidade, integridade e disponibilidade das informações. Deve incluir recursos de criptografia, autenticação, controle de acesso e detecção de ameaças, entre outros aspectos essenciais para a segurança cibernética.
- Monitoramento e análise: A arquitetura deve permitir o monitoramento em tempo real, a coleta de dados relevantes e a análise avançada para identificar possíveis ameaças e incidentes de segurança. Deve oferecer recursos de correlação de eventos, análise comportamental, detecção de anomalias e geração de relatórios detalhados.
- Usabilidade: A arquitetura deve ser intuitiva e de fácil utilização, permitindo que os usuários interajam com as ferramentas de maneira eficiente. Deve fornecer uma interface amigável, recursos de visualização de dados claros e personalização das configurações de acordo com as necessidades da organização.

Recomenda-se que os licitantes realizem a vistoria prévia ao processo licitatório, a fim de conhecer o parque tecnológico da agência e obter informações detalhadas sobre a infraestrutura existente. Essa vistoria permite que os licitantes tenham uma visão mais precisa das necessidades e requisitos específicos da organização, facilitando a elaboração de propostas alinhadas com as demandas reais.

Durante a vistoria, os licitantes podem ter a oportunidade de avaliar a atual arquitetura de TI, a rede de comunicação, os sistemas e aplicativos em uso, bem como a infraestrutura de segurança existente. Essa análise detalhada possibilita uma compreensão mais completa do ambiente em que as ferramentas de segurança cibernética e SOC serão implantadas, permitindo que os licitantes adequem suas soluções de acordo com as características específicas da agência.

Além disso, a vistoria prévia também proporciona aos licitantes a chance de esclarecer dúvidas, obter informações adicionais e interagir diretamente com os responsáveis pela área de tecnologia da agência. Essa troca de informações contribui para um melhor entendimento das expectativas da organização e permite que os licitantes ofereçam propostas mais personalizadas e alinhadas com as necessidades reais da agência.

Requisitos de Projeto e de Implementação,

Na execução do objeto deverão ser observados os seguintes requisitos:

- Escalabilidade: O software deve ter capacidade de escalonamento para atender às demandas futuras da agência, garantindo que possa lidar com o aumento do volume de dados e usuários sem comprometer o desempenho.
- Integração: Os serviços devem permitir a integração com outras ferramentas e sistemas existentes na agência, como firewalls, sistemas de gerenciamento de identidade, bancos de dados, entre outros. A capacidade de interoperabilidade é essencial para uma gestão eficiente da segurança cibernética.
- Personalização: As soluções SaaS devem permitir a personalização de acordo com as necessidades e requisitos específicos da agência. Isso inclui a capacidade de configurar políticas de segurança, alertas, relatórios e outros recursos de acordo com os padrões e políticas internas.
- Usabilidade: A interface do software disponibilizado deve ser intuitiva, amigável e de fácil utilização, facilitando o acesso e a operação por parte dos usuários. Recursos como painéis de controle, visualizações gráficas e relatórios devem ser apresentados de maneira clara e acessível.
- Segurança: O sistema deve atender aos mais altos padrões de segurança, incluindo criptografia de dados, autenticação de usuários, controle de acesso granular, detecção de ameaças e prevenção de intrusões. Além disso, é importante que as licitantes cumpram as regulamentações de proteção de dados, como a LGPD (Lei Geral de Proteção de Dados).
- Monitoramento e análise: O software deve oferecer recursos avançados de monitoramento em tempo real, detecção de anomalias, análise de dados e geração de relatórios detalhados. Essas funcionalidades permitem uma visão abrangente do ambiente de segurança e facilitam a tomada de decisões baseadas em informações relevantes.
- Suporte e manutenção: A licitante deve fornecer suporte técnico adequado, incluindo treinamento, assistência na configuração e manutenção contínua das soluções contratadas. Também é importante definir acordos de nível de serviço (SLAs) que garantam a disponibilidade e a resposta rápida em casos de falhas ou incidentes.

Além dos requisitos de arquitetura e implementação mencionados anteriormente, é fundamental considerar a necessidade de integração entre o Security Operations Center (SOC), o Network Operations Center (NOC) que estará cargo de outra contratada e a empresa responsável pelos serviços de Penetration Test (pen test).

A integração do SOC com o NOC é de extrema importância para garantir uma abordagem holística na gestão da segurança cibernética. O SOC é responsável por monitorar, detectar e responder a ameaças em tempo real, enquanto o NOC é responsável pela gestão e monitoramento contínuo da infraestrutura de rede e sistemas. A colaboração e troca de informações entre essas duas equipes são essenciais para uma resposta efetiva a incidentes e para a identificação de vulnerabilidades de segurança em tempo hábil.

Da mesma forma, a empresa responsável pelos serviços de pen test desempenha um papel crítico na avaliação da segurança dos sistemas, redes e aplicativos. O pen test é um processo que busca identificar e explorar vulnerabilidades existentes, simulando ataques reais. Essa atividade auxilia na identificação de falhas de

segurança e permite que medidas corretivas sejam implementadas antes que sejam exploradas por agentes maliciosos. A integração entre o SOC e a empresa de pen test é necessária para compartilhar informações sobre as descobertas e resultados dos testes, bem como para garantir ações adequadas de remediação.

Requisitos de Garantia,

Garantia Contratual

O adjudicatário, no prazo de trinta (30) dias após a assinatura do Termo de Contrato ou aceite do instrumento equivalente, prestará garantia no valor correspondente a cinco por cento (5%) do valor do Contrato, que será liberada de acordo com as condições previstas no Edital, conforme disposto no art. 56 da Lei Nº 8.666, de 21 de junho de 1993, desde que cumpridas as obrigações contratuais.

Caberá ao contratado optar por uma das seguintes modalidades de garantia:

I. caução em dinheiro ou em títulos da dívida pública, devendo estes 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;
II. seguro-garantia;
III. fiança bancária.

A garantia em dinheiro deverá ser efetuada em favor da CONTRATANTE, na Caixa Econômica Federal, com correção monetária, em favor do CONTRATANTE.

No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de trinta (30) dias úteis, contados da data em que for notificada.

A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

A garantia prestada pelo contratado será liberada ou restituída após a execução do contrato e, quando em dinheiro, atualizada monetariamente (artigo 56, §4º da Lei Nº 8666/93).

Deverão ainda ser observadas as demais disposições contidas no Edital.

Garantia do Produto,

A empresa fornecedora dos serviços será responsável por fornecer suporte e serviços adicionais durante o período de utilização da solução contratada. O suporte terá início no primeiro dia útil após a aceitação definitiva da solução e terá duração mínima de 1 (um) ano, correspondendo ao prazo mínimo de garantia dos serviços.

Os benefícios do serviço de suporte incluem fornecimento de

atualizações para novas versões do software, disponibilização de correções e atualizações durante o período de utilização, suporte telefônico e chat em regime 24x7 (vinte e quatro horas por dia, sete dias por semana). Além disso, a empresa fornecedora deverá disponibilizar uma base de conhecimento com soluções de problemas e documentos técnicos para auxiliar a contratante.

A CONTRATADA também será responsável por fornecer o suporte necessário para utilização dos serviços contratados, auxiliando a contratante no registro e ativação dos serviços no portal da empresa fornecedora. Além disso, a CONTRATADA deverá acompanhar e atender todas as solicitações de suporte remoto por meio dos canais de comunicação estabelecidos.

É importante ressaltar que todos os serviços contratados contemplarão atualizações e melhorias durante a vigência do contrato, garantindo assim a evolução contínua da solução. A garantia dos serviços será válida pelo mesmo período de vigência do contrato e, caso haja renovação do contrato, a garantia também será renovada, de acordo com as quantidades, requisitos e especificações constantes no documento.

Dessa forma, a CONTRATADA se compromete a fornecer suporte completo e contínuo, garantindo o pleno funcionamento e a atualização dos serviços contratados durante todo o período de utilização, visando atender às necessidades e demandas da contratante.

Requisitos de Experiência Profissional,

A equipe responsável pela execução do objeto deve ser composta por profissionais qualificados e capacitados na área de segurança cibernética, de acordo com os requisitos estabelecidos. A qualificação da equipe é de extrema importância para garantir a excelência na prestação dos serviços e a obtenção dos resultados esperados.

A fornecedora dos serviços de segurança cibernética deve contar com profissionais especializados e experientes no campo de atuação relacionado ao objeto da contratação. Esses profissionais devem possuir conhecimento técnico aprofundado nas soluções e ferramentas de segurança cibernética, bem como experiência comprovada na implementação e gestão dessas soluções.

É essencial que a equipe tenha as competências e habilidades necessárias para lidar com a complexidade e as demandas específicas do ambiente em que serão executadas as tarefas. Isso inclui o domínio das tecnologias e metodologias de segurança cibernética, a capacidade de solucionar problemas de forma eficiente, a habilidade de comunicação e trabalho em equipe, bem como a capacidade de se adaptar a novas situações e cumprir prazos estabelecidos.

A equipe de segurança cibernética deve estar atualizada em relação às melhores práticas e tendências do mercado, buscando constantemente aprimorar seus conhecimentos e habilidades para garantir uma prestação de serviços de alta qualidade. A presença de profissionais capacitados e experientes contribuirá para a efetividade das soluções implementadas e para a mitigação de riscos de segurança.

Portanto, é imprescindível que a equipe de segurança cibernética seja composta por profissionais altamente qualificados, especializados e experientes, capazes de oferecer um serviço de excelência, atendendo às necessidades e demandas da contratante.

Requisitos de Formação da Equipe,

Não se aplica, pois fica totalmente a cargo da contratada.

Requisitos de Metodologia de Trabalho,

- Conhecimento e Experiência: A licitante deve possuir um profundo conhecimento das soluções e ferramentas de segurança cibernética, bem como experiência comprovada no fornecimento desses serviços para organizações similares. É aconselhável que a licitante demonstre uma compreensão abrangente das diferentes opções de soluções de segurança cibernética e suas respectivas vantagens.
- Orientação ao Cliente: A licitante deve adotar uma abordagem centrada no cliente, priorizando o entendimento das necessidades e requisitos específicos da organização contratante na área de segurança cibernética. É importante que a licitante seja capaz de oferecer orientações adequadas sobre as soluções de segurança cibernética mais adequadas às necessidades da Agência, levando em consideração fatores como tamanho, tipo de negócio e orçamento disponível.
- Implementação Correta: A licitante deve garantir que todas as soluções de segurança cibernética fornecidas estejam de acordo com as melhores práticas de implementação e segurança da informação. É fundamental que a licitante possua um profundo entendimento das políticas de segurança cibernética e as leis de proteção de dados aplicáveis, a fim de fornecer as soluções corretas e evitar quaisquer brechas de segurança.
- Suporte Técnico: A licitante deve oferecer suporte técnico adequado para auxiliar a organização contratante na implementação, configuração e solução de problemas relacionados às soluções de segurança cibernética. É importante que a licitante possua uma equipe de suporte qualificada, capaz de lidar com consultas e problemas técnicos de maneira eficiente e eficaz, visando manter um ambiente seguro e protegido.
- Atualizações e Renovações: A licitante deve fornecer informações claras sobre as atualizações e renovações das soluções de segurança cibernética, garantindo que a contratante esteja ciente dos prazos e processos necessários para manter seu ambiente de segurança atualizado e em conformidade com as melhores práticas de segurança cibernética.

É essencial que a licitante possua uma equipe especializada em segurança cibernética, com profissionais qualificados e experientes, capazes de fornecer soluções e suporte técnico adequados para garantir a proteção dos ativos e dados da contratante. A adoção de uma abordagem centrada no cliente e o cumprimento das melhores práticas de segurança cibernética são elementos essenciais para uma contratação de sucesso nessa área.

Requisitos de Segurança da Informação,

A CONTRATADAé responsável por fornecer os serviços em conformidade com a Política de Segurança da Informação e Comunicação da ANA (POSIC/ANA), instituída por meio da Resolução ANA Nº 1099, de 26 de junho de 2017.

Deverá atender às seguintes normas:

- Lei Nº 13.708, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;
- Decreto Nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação;
- Instrução Normativa GSI/PR N° 1, de 13 de junho de 2008 e suas normas complementares - Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;
- Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020 e suas normas complementares - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
- Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021 e suas normas complementares - Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal
- Norma Complementar Nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012 - Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;
- Norma Complementar Nº 13/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, - Diretrizes para gestão de mudanças nos aspectos relativos à segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal;
- Norma Complementar Nº 07/IN01/DSIC/GSIPR, de 15 de julho de 2014 - Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;
- ABNT NBR ISO 22301:2013 - Sistemas de gestão de continuidade de negócios;
- ABNT NBR ISO 22313:2015 - Sistemas de gestão de continuidade de negócios;
- ABNT NBR ISO 27031:2015 - Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação;
- ABNT NBR 11515:2007 - Guia de práticas para segurança física relativas ao armazenamento de dados;
- ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 - Governança de segurança da informação;
- Instrução Normativa PR/GSI nº 5, de 30 de agosto de 2021: Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade da CONTRATANTE, sem autorização.

A CONTRATADA deverá atender as Políticas de Segurança da Informação e demais normativos correlatos publicados pela CONTRATANTE, bem como assinar Termo de Compromisso e seus funcionários alocados na prestação de serviços, o Termo de Ciência e Termo de compromisso e manutenção de sigilo em contrato, conforme modelos que estarão anexos ao Termo de Referência.

A propriedade intelectual e os direitos autorais dos dados e informações e qualquer tipo de trabalho relacionado às demandas da CONTRATANTE, serão de sua titularidade. A CONTRATADA deve-se abster de divulgar ou repassar quaisquer dados ou informações, salvo se expressamente autorizado pela CONTRATANTE.

Outras medidas indicadas durante a vigência do contrato pela CONTRATANTE.

Benefícios e resultados esperados

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

- Identificação de possíveis vulnerabilidades de segurança da informação, na infraestrutura e aplicações da ANA;
- Gestão de vulnerabilidade, quando estas forem identificadas nos equipamentos e soluções de segurança;
- Monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados à ANA;
- Detecção avançada de malwares por meio de inteligência artificial e análise de comportamento de arquivos e/ou scripts;
- Prevenção de ataques, intrusão ou acesso indevido a dados e informações da agência;
- Manter a integridade os ativos de TI, permitindo uma redução do tempo de resposta às demandas de incidentes de segurança da informação.
- Aumentar a eficiência de monitoração de eventos de segurança (consolidação de monitoração), provendo acesso centralizado e consistente a todos os logs e eventos;
- Promover a continuidade dos serviços e melhorar os atuais níveis de segurança e disponibilidade dos servidores e desktops na rede corporativa da ANA;
- Manter o ambiente tecnológico da ANA protegido, provendo segurança ao ambiente, com respostas rápidas de vacinas e procedimentos de configuração no caso de disseminação de novos vírus pela Internet.

3 Estimativa da Demanda – Quantidade de Bens e Serviços

Para cumprimento do objetivo proposto pela referida contratação é necessária a contratação, conforme detalhado abaixo.

Lote	Item	Descrição	Quant.	Unid. Referência	Valor Unit.	Valor Anual
	1	Serviços de Gestão de Vulnerabilidades	12	Mês	R$40.022,80	R$480.273,62

1	2	Serviços de Gestão de Segurança para Infraestrutura e Sistemas Críticos	12	Mês	R$45.004,68	R$540.056,10
	3	Serviços de Monitoramento de Ataques Cibernéticos	12	Mês	R$59.434,12	R$713.209,39
	4	Serviços de Resposta a Incidentes de Segurança Cibernética	12	Mês	R$45.937,15	R$551.245,85
	5	Serviços de Gestão de Segurança de Endpoints e Servidores de Rede	12	Mês	R$51.197,42	R$614.369,04
	6	Serviços de Segurança de Mensageria Proativa	12	Mês	R$39.437,21	R$473.246,56
	7	Serviços de Inteligência Aplicada a Segurança Cibernética	12	Mês	R$23.712,31	R$284.547,75
	8	Serviços de Conscientização da Segurança da Informação	2	Mês	R$24.643,33	R$147.860,00
2	9	Serviços de Testes de Invasão (Pentest)	6	Unid.	R$25.278,93	R$151.673,59

Considerando os preços obtidos na tabela supracitada, o valor estimado máximo anual é de **R$ 3.956.481,84 (três milhões, novecentos e cinquenta e seis mil, quatrocentos e oitenta e um reais e oitenta e quatro centavos)**.

4 Análise de Soluções

O objetivo da presente contratação é prover a Agência de serviços continuados de segurança cibernética, seguindo as especificações, padrões de governança e qualidade estabelecidos pela Agência Nacional de Águas e Saneamento Básico (ANA).

Considerando as diretrizes do Decreto Nº 9.507, de 21 de setembro de 2018, a Superintendência de Tecnologia da Informação (STI) tem buscado atribuir a terceiros a execução operacional das atividades de segurança cibernética, concentrando seus esforços na gestão, planejamento, supervisão, fiscalização e controle dos processos de negócio.

Este processo licitatório tem como objetivo suprir as atividades atualmente realizadas de forma limitada pela equipe interna da STI, as quais são essenciais para atender plenamente as demandas existentes do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e cumprir as normas de governança relacionadas à gestão do desenvolvimento de TI. Isso garante a obtenção dos resultados mais vantajosos para a Administração Pública e para a sociedade, seguindo o princípio da economia processual.

Alternativamente a essa proposta, considerando que além das atividades específicas do objeto descritas alternativa 2 (ID 2) deste documento, não licitadas pela ANA em contratos anteriores, seria necessário criar pelo menos três novos contratos para atender a todo o escopo desejado (ferramentas de vulnerabilidade, ferramentas de SIEM, ferramentas de NDR, entre outras). Além disso, devido ao volume de trabalho, a equipe interna da STI não tem condições de realizar essas atividades, e a realização de um concurso específico para as áreas de TI pela ANA é inviável a curto prazo.

Diante dessas circunstâncias, não há outra alternativa viável e mais vantajosa para a execução do objeto do que a apresentada neste documento. Portanto, justifica-se a indicação dessa proposta como a melhor alternativa existente para a execução do escopo, considerando sua viabilidade técnica, operacional e econômica.

Soluções Identificadas

01	Contratação de empresa especializada para prestação de serviços de segurança cibernética.
02	Execução interna.

Análise de Soluções (As respostas se aplicam às duas soluções)

Requisito	ID da Solução	Sim	Não	Não se aplica
A solução contém item presente nos Catálogos de Soluções de TIC com Condições Padronizadas (SGD)?			x	
			x	
A solução encontra-se implantada em outro órgão da Administração Pública?		x		
		x		
Há alternativas no mercado?		x		
		x		
A solução está disponível no Portal do Software Público Brasileiro?			x	
			x	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos padrões e-PING, e-MAG e e-Pwg?				x
				x
A Solução é aderente às regulamentações da ICP-Brasil? (Quando houver necessidade de certificação digital)				x
				x
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (Quando a solução abranger documentos arquivísticos)				x
				x
Há necessidade de adequação do ambiente do órgão para viabilizar a execução contratual?			x	
			x	

Análise de Viabilidade

“Solução Viável”

A opção de "Contratação de empresa especializada para prestação de serviços de segurança cibernética" foi considerada viável tanto do ponto de vista técnico quanto econômico, além de estar alinhada às boas práticas e atender ao melhor interesse público.

Ao analisar minuciosamente as necessidades da Agência e as demandas específicas relacionadas à segurança cibernética, verificou-se que essa alternativa apresenta diversas vantagens. A contratação de uma empresa especializada proporcionará acesso a conhecimentos e recursos atualizados no campo da segurança

cibernética, garantindo uma abordagem profissional e especializada para lidar com os desafios cada vez mais complexos desse setor.

Além disso, a contratação de uma empresa especializada permitirá a implementação de soluções e práticas de segurança cibernética de ponta, que podem ser adaptadas de acordo com as necessidades e peculiaridades da Agência. Essa abordagem contribuirá para o fortalecimento e aprimoramento dos controles de segurança, proteção de dados e prevenção de incidentes, proporcionando maior tranquilidade e confiança à organização.

Do ponto de vista econômico, essa alternativa se mostrou favorável, uma vez que a contratação de uma empresa especializada elimina a necessidade de investimentos significativos em infraestrutura, treinamento e desenvolvimento interno de uma equipe de segurança cibernética. Além disso, permite a flexibilidade de ajustar os serviços contratados de acordo com as demandas e necessidades específicas da Agência, evitando custos fixos desnecessários.

Considerando todos esses aspectos, fica evidente que a contratação de uma empresa especializada para a prestação de serviços de segurança cibernética é a opção mais viável e benéfica para a Agência. Essa abordagem garantirá a obtenção de resultados eficientes, de acordo com as melhores práticas do setor, e promoverá a proteção e a integridade dos ativos digitais da organização, salvaguardando a confidencialidade, a disponibilidade e a integridade das informações críticas.

“Solução Inviável”

A alternativa de "Execução interna" se mostrou inviável do ponto de vista técnico para a prestação de serviços de segurança cibernética. Essa opção seria extremamente prejudicial para a Administração Pública, levando em consideração as diretrizes estabelecidas para a terceirização desse tipo de serviço.

A complexidade e a especificidade do tema de segurança cibernética exigem conhecimentos atualizados e especializados, que nem sempre podem ser facilmente mantidos pela equipe interna. A rápida evolução das ameaças e das tecnologias requer um constante acompanhamento e atualização, o que pode representar um desafio significativo para a equipe interna, que já está envolvida em outras atividades essenciais.

Além disso, a realização de concursos específicos para contratar profissionais com expertise em segurança cibernética pode ser uma tarefa difícil e demorada, levando em consideração a escassez de profissionais qualificados nesse campo. A burocracia e o tempo necessário para a realização do concurso podem comprometer a agilidade e a eficácia das ações de segurança cibernética.

Ao considerar esses aspectos, é evidente que a alternativa de execução interna não é viável para atender às demandas de segurança cibernética da Administração. Ter uma equipe interna responsável por essa área pode resultar em lacunas de conhecimento e expertise, comprometendo a eficiência e a eficácia das medidas de proteção adotadas.

Além disso, a contratação de uma empresa especializada proporciona a vantagem de contar com profissionais que se dedicam exclusivamente à segurança cibernética, possuem experiência comprovada no campo e mantêm-se atualizados com as últimas tendências e ameaças. Isso garante uma abordagem profissional e especializada, capaz de enfrentar os desafios cada vez mais complexos da segurança cibernética.

Portanto, considerando todos esses aspectos, a opção de execução interna se mostra inviável e não é comparável do ponto de vista econômico. A terceirização dos serviços de segurança cibernética é uma abordagem mais adequada para garantir a proteção dos ativos digitais da Administração Pública e atender às exigências técnicas e especializadas desse campo em constante evolução.

Sistema de Registro de Preços - SRP

É caso de SRP?

( ) SIM (X) NÃO

Descrição e justificativa da solução escolhida

Considerando todas as razões, benefícios e justificativas expostas ao longo desta análise, é amplamente recomendada a adoção da solução "Contratação de empresa especializada para prestação de serviços de segurança cibernética" como a opção mais vantajosa para a Administração Pública. Essa escolha se baseia em diversos aspectos que foram minuciosamente avaliados, resultando em uma clara evidência de sua superioridade.

A contratação de uma empresa especializada traz consigo uma série de benefícios e vantagens inegáveis. Primeiramente, ao terceirizar os serviços de segurança cibernética, a Administração poderá contar com uma equipe altamente qualificada, experiente e especializada nesse campo específico. Esses profissionais dedicados e atualizados poderão oferecer um nível de expertise que seria difícil de ser alcançado por uma equipe interna, garantindo uma abordagem profissional e eficiente para a proteção dos ativos digitais da organização.

Além disso, a contratação de uma empresa especializada elimina a necessidade de investimentos em infraestrutura, equipamentos e treinamento interno, reduzindo os custos e os riscos associados à manutenção de uma equipe interna de segurança cibernética. Essa abordagem também permite maior flexibilidade para ajustar os serviços de acordo com as necessidades específicas da Administração, bem como acesso a recursos avançados e tecnologias de ponta disponibilizadas pela empresa contratada.

Outro aspecto relevante é a complexidade e a dinamicidade do cenário de segurança cibernética, que requer atualizações constantes e acompanhamento das tendências e ameaças emergentes. A contratação de uma empresa especializada garante que a Administração esteja sempre atualizada e protegida contra as mais recentes ameaças, mitigando os riscos de possíveis ataques e vulnerabilidades.

Por fim, é importante destacar que a solução de contratação de uma empresa especializada é respaldada pelas melhores práticas e diretrizes da Administração Pública, que preconizam a terceirização de serviços não essenciais para permitir que a equipe interna se concentre nas atividades de gestão, supervisão e controle. Essa abordagem está alinhada com a eficiência administrativa, a otimização de recursos e a busca pela excelência na prestação de serviços públicos.

Com base em todas essas considerações, o modelo de execução da contratação da empresa especializada para prestação de serviços de segurança cibernética se apresenta como a opção mais vantajosa e adequada para atender às demandas da Administração Pública. Sua implementação proporcionará um ambiente protegido, atualizado e confiável, garantindo a segurança dos dados e sistemas da organização.

No anexo deste documento, é apresentado de forma detalhada o modelo de execução dessa contratação, evidenciando todos os aspectos relevantes, etapas e requisitos necessários para sua efetivação. A adoção dessa solução representa um passo significativo em direção à proteção cibernética efetiva e ao cumprimento das exigências governamentais e das melhores práticas de segurança da informação.

5 Estimativa de Custo Total da Contratação

O memorial de cálculo e respectiva metodologia adotada se encontra detalhada no documento Pesquisa de Preços, anexo ao presente processo.

Considerando os preços obtidos na tabela supracitada, o valor estimado máximo anual é de **R$ 3.956.481,84 (três milhões, novecentos e cinquenta e seis mil, quatrocentos e oitenta e um reais e oitenta e quatro centavos)**.

6 Declaração de Viabilidade

Diante de todo o exposto a solução em tela “Contratação de empresa especializada para prestação de serviços de segurança cibernética”, refletida na **alternativa 1** proposta é a única viável do ponto de vista técnico e econômico.

7 Aprovação e Assinatura

Conforme o Art. 11º da IN SGD/ME nº 1/2019, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC.

(assinado eletronicamente)
FABIANO COSTA DE ALMEIDA
Coordenador de Segurança da Informação e Comunicações
Integrante Requisitante

(assinado eletronicamente)
CLÁUDIO PEREIRA
Coordenador de Infraestrutura e Operações de Tecnologia da Informação

Integrante Técnico

(assinado eletronicamente)
RAFAEL CUNHA ALVES MOREIRA
Superintendente de Tecnologia da Informação

ANEXO I – DETALHAMENTO DO OBJETO

O presente objeto se trata da aquisição de serviços e software-as-a-service (SaaS) e não implica em contrato de fornecimento de licenças ou mão-de-obra, salientando que:

- A CONTRATANTE se resguarda o direito de solicitar a substituição de qualquer profissional designado para atendimento do objeto bastando para isso à comunicação formal à CONTRATADA, que deverá providenciar a troca em no máximo 48h (quarenta e oito horas).
- Na execução do objeto a CONTRATADA deve estar ciente que haverá permanente interlocução entre ela, a equipe gestora de segurança da CONTRATANTE e a equipe da empresa responsável pelo fornecimento de serviços de apoio e suporte de infraestrutura de TIC (e NOC).

A seguir serão apresentados os detalhes dos serviços que compõem o objeto da contratação, a fim de proporcionar uma compreensão clara e abrangente das atividades a serem executadas.

1.1 SERVIÇOS DE GESTÃO DE VULNERABILIDADES

Tem por objetivo de forma proativa e recorrente, identificar possíveis vulnerabilidades de segurança da informação, na infraestrutura e nas aplicações da ANA, para evitar que ataques cibernéticos direcionados obtenham sucesso no ambiente tecnológico (hardware e software). se espera da contratada as correções de vulnerabilidade.

Sobre as ferramentas a serem utilizadas,

As ferramentas e soluções utilizadas para prestação do serviço supracitado deverão ser agrupadas, a saber:

- Gestão de vulnerabilidades de ambiente crítico: Soluções e/ou ferramentas utilizadas pela CONTRATADA para gerir todo ciclo de vida das vulnerabilidades encontradas. Ou seja, desde a sua descoberta até sua correta mitigação;
- Gestão de vulnerabilidade de ambiente não crítico: Soluções e/ou ferramentas utilizadas pela CONTRATADA para realizar o processo de blindagem de vulnerabilidades conhecidas em sistemas web.

Independente do grupo das soluções supracitadas, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos:

- Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderão ser do tipo open source (software livre);
- Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço.;
- O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

O hardware necessário para instalação e configuração do ferramental será fornecido pela infraestrutura da ANA, para aquelas ferramentas que serão executadas em ambiente da ANA.

As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Gestão de vulnerabilidades de ambiente crítico e não crítico,

A CONTRATANTE nomeará 1000 (mil) ativos a serem monitorados como ambiente crítico e 2000 (dois mil) ativos a serem monitorados como ambiente não crítico, sendo necessário gerir todo o ciclo de vida das vulnerabilidades encontradas neles.

O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

A CONTRATADA deverá compor ao ambiente de segurança da informação atualmente implementadas na ANA, soluções de gestão de vulnerabilidades capazes de identificar vulnerabilidades de infraestrutura e aplicações, que possam comprometer a disponibilidade, integridades e confiabilidade dos dados e serviços da ANA

Deverá ser utilizada ferramenta de análise de vulnerabilidade com foco em infraestrutura e em aplicações web.

Apesar de ser necessária e permitida a utilização de ferramentas para descoberta de vulnerabilidades no ambiente da ANA, a CONTRATADA também deve utilizar métodos e técnicas assistidas, para identificar possíveis vulnerabilidades no ambiente da ANA.

A fim de mitigar e prever possíveis impactos durante as rotinas de validação de vulnerabilidade, antes do início da execução do serviço, as ferramentas adotadas para execução deverão ser apresentadas ao time de segurança da informação da ANA, que poderá ou NÃO aprovar.

A solução deve possibilitar varreduras (scans) de vulnerabilidades, avaliação de configuração e conformidade (baseline e compliance) e indícios e padrões de códigos maliciosos conhecidos (malware);

A solução deve possuir recurso de varredura ativa, onde o scanner comunica-se com os alvos (ativos) através da rede. As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Processo de atendimento para gestão de vulnerabilidade,

A ANA deverá apresentar uma lista de ativos e recursos que deverão fazer parte do processo de gestão de vulnerabilidade. Tal lista poderá ser revisitada e atualizada durante todo o período de vigência de contrato.

A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional da ANA, a fim de consultivamente sugerir e complementar a lista de ativos e recursos disponibilizado à ANA, de acordo com as variáveis e critérios estabelecidos no catálogo

de serviços da ANA, e também na lista de ativos e recursos da ANA, a CONTRATADA deverá realizar checagens (scans) e varreduras, buscando encontrar vulnerabilidades de segurança no ambiente da ANA, utilizando as ferramentas e soluções definidas no presente termo de referência.

Após o término das rotinas de checagens (scans) e varreduras no ambiente, deverá realizar uma análise de falso positivo das vulnerabilidades descobertas, isso quer dizer, que devem ser informadas à ANA apenas vulnerabilidades que existam de fato em seu ambiente.

Após análise de falso positivo, a CONTRATADA deverá informar à ANA as vulnerabilidades encontradas, obedecendo os critérios e requisitos estabelecidos no tópico ENTREGAS A SEREM REALIZADAS.

A ANA possui um processo rigoroso de gestão de configuração e mudança, sobre sua governança, logo cabe única e exclusivamente à ANA liberar e/ou autorizar toda e qualquer mudança sugerida para contenção e mitigação de uma vulnerabilidade encontrada. Sendo assim, nenhuma mudança deve ser realizada, sem que antes haja essa liberação.

Uma vez autorizada a mudança para correção de uma determinada vulnerabilidade, caberá a CONTRATADA apenas as correções de vulnerabilidades encontradas no ambiente listado no tópico AMBIENTE TECNOLÓGICO DA ANA (Hardware e Software), obrigatoriamente obedecendo as definições proposta pelo comitê de mudança da ANA.

Para as vulnerabilidades encontradas no ambiente e que ainda não tiverem soluções conhecidas, caberá a CONTRATADA apresentar medidas de contorno, que para aplicá-las ao ambiente, deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.

Como último passo a CONTRATADA deverá atualizar todos os controles e indicadores, estabelecidos no tópico ENTREGAS A SEREM REALIZADAS.

O processo descrito é mínimo esperado a ser seguido e executado pela CONTRATADA, todavia espera-se da CONTRATADA a apresentação de melhoria contínua deste, a qual pode ser alterado desde que aprovado pela ANA.

O ciclo de vida do processo de gestão de vulnerabilidade, deve ser executado de forma recorrente.

Grupo técnico de gestão de vulnerabilidade,

Através do seu CSOC (Cyber Security Operations Center) definidos no tópico a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), com objetivo e foco de trabalhar no processo de gestão de vulnerabilidade.

Este grupo deverá ser exclusivo para trabalhar no SERVIÇO DE GESTÃO DE VULNERABILIDADES, sendo que os profissionais pertencentes a este grupo não podem ser compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO (SLA) do presente termo de referência.

A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de gestão de vulnerabilidades da ANA, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), com ao menos 1 (um) perfil de cada que segue descrito a seguir:

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	ComTIA Cybersecurity Analyst (CySA+)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação

Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team).

No momento da assinatura do contrato será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE ATAQUE CIBERNÉTICO CONTROLADO (Red Team), os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: curriculum vitae para comprovação de habilidades, termo de confidencialidade e sigilo assinados e as devidas certificações técnicas para comprovação do conhecimento.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a ANA definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do um portal de segurança preferencialmente, a saber:

- Período em que foi realizado o serviço;
- Quantitativo total de vulnerabilidade;
- Quantitativo de vulnerabilidades por severidade;
- Quantitativo de vulnerabilidades corrigidas por severidade;
- Quantitativo de novas vulnerabilidades em aplicações Web;
- Quantitativo de vulnerabilidades corrigidas em aplicações Web;
- Quantitativo de certificados digitais expirados;
- Top 10 dos ativos mais vulneráveis;
- Top 10 das vulnerabilidades mais comuns nos ativos;
- Top 10 das aplicações Web mais vulneráveis;
- Top 10 das aplicações Web mais vulneráveis em comparação com OWASP.

Tais relatórios e indicadores serão apresentados e discutidos em reunião mensal, com a presença do preposto da CONTRATADA e toda a equipe técnica que seja necessária para esclarecer quaisquer dúvidas pertinentes aos eventos ocorridos no período. A apresentação poderá ser de forma presencial nas dependências da ANA de forma virtual, por meio de solução de videoconferência.

1.2 SERVIÇOS DE GESTÃO DE SEGURANÇA PARA INFRAESTRUTURA E SISTEMAS CRÍTICOS

Visa o monitoramento contínuo e ininterrupto de acesso aos sistemas críticos por meio de credenciais administrativas no ambiente da ANA, de auditoria e de segurança, cujo eventos gerados devem ser analisados, podendo estes serem transformado em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos. A CONTRATADA deve prover este serviço no parque tecnológico descrito no tópico AMBIENTE TECNOLÓGICO DA ANA (Hardware e Software).

Sobre as ferramentas a serem utilizadas,

Independente do grupo das soluções supracitadas, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos:

- Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre).

- Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.
- Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço.
- O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.
- O hardware necessário para instalação e configuração do ferramental será fornecido pela infraestrutura da ANA.

As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Processo de atendimento para gestão de segurança para infraestrutura e sistemas críticos

A ANA deverá apresentar uma lista de usuários e dispositivos que deverão fazer parte do processo de gestão de segurança para sistemas críticos. Tal lista poderá ser revisitada e atualizada durante todo o período de vigência de contrato.

A definição de usuário e dispositivo estão definidas da seguinte forma:

- Um dispositivo alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, cujas credenciais de acesso passem a ser gerenciadas pelo serviço de gestão de segurança para sistemas críticos;
- Um usuário da solução é definido como qualquer pessoa que acesse um dispositivo alvo mediante logon (autenticação) protegido pelo serviço de gestão de segurança para sistemas críticos, assim como, o uso de credenciais protegidas por este serviço.

A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional da ANA, a fim de consultivamente sugerir e complementar a lista de ativos e recursos disponibilizado.

De acordo com as variáveis e critérios estabelecidos no catálogo de serviço, e na lista disponibilizada pela ANA, a CONTRATADA deverá iniciar os serviços de monitoramento, armazenamento e gravação de acesso.

Como último passo a CONTRATADA deverá atualizar todos os controles e indicadores, estabelecidos no tópico ENTREGAS A SEREM REALIZADAS.

O processo descrito é mínimo esperado a ser seguido e executado pela CONTRATADA, todavia espera-se da CONTRATADAa apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela ANA.

Grupo técnico de gestão de segurança para infraestrutura e sistemas críticos,

Para o serviço de Gestão de Segurança para Sistemas Críticos, não haverá um grupo exclusivo para execução. O grupo responsável por tal execução poderá ser do SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela **CONTRATADA**, foi definido os seguintes indicadores de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do portal de segurança:

- Período em que foi realizado o serviço;
- Quantitativo total de requisições abertas;
- Quantitativo de requisições concluídas;
- Quantitativo de requisições e, backlog;
- Top 10 dos riscos por usuário;
- Top 10 dos acessos por usuários;
- Top 10 dos sistemas mais acessados.

Tais relatórios e indicadores serão apresentados e discutidos em reunião mensal, com a presença do preposto da CONTRATADA e toda a equipe técnica que seja necessária para esclarecer quaisquer dúvidas pertinentes aos eventos ocorridos no período. A apresentação poderá ser de forma presencial nas dependências da ANA ou de forma virtual, por meio de solução de videoconferência.

1.3 SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS

Tem por objetivo o monitoramento contínuo e ininterrupto de ataques cibernéticos direcionados ao CONTRATANTE, através de correlacionamento de logs, pacotes de redes, e/ou comportamento anômalo de aplicações, serviços e infraestrutura do CONTRATANTE, que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

Outro objetivo desse item, é sustentar e operar as ferramentas de antivírus do CONTRATANTE, caso possua, realizando a gestão e configuração das funcionalidades e ações proativas de acompanhamento.

Sobre as ferramentas a serem utilizadas,

As ferramentas e soluções utilizadas para prestação do serviço supracitado que poderão ser agrupadas ou não, a saber:

- Gestão de Logs e operação de incidentes (SIEM): Soluções e/ou ferramentas utilizadas pela CONTRATADA para realizar a análise de logs e no caso de ocorrência de ação positiva de risco gerenciada como incidente;
- Gestão de Dispositivos de Rede (NDR): Soluções e/ou ferramentas utilizadas pela CONTRATADA para gerir avaliar continuamente e ininterruptamente os acessos aos elementos de rede passíveis da operação de segurança.

Independente do grupo das soluções supracitadas, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

- Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre);
- Deverá ser prestado por meio de solução provida através de nuvem do fabricante ou da CONTRATADA.
- Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço.
- O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

Caso seja necessário a instalação on-premise de software, o hardware para instalação e configuração será fornecido pela infraestrutura da ANA. No caso de uso da solução NDR, o hardware será fornecido pela CONTRATADA.

As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Processo de monitoramento de ataques cibernéticos,

Será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição de linha de base de eventos monitorados.

A ANA deverá participar ativamente no processo de construção dessa linha de base de forma consultiva, porém se ratifica que é de responsabilidade da CONTRATADA a sua definição e colocá-la em operação.

A linha de base deverá ser revista de forma mensal, contudo este tempo não está limitado, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e atualize a linha de base.

O produto de um evento é a correlação dos insumos: logs e pacotes de rede, gerados pelos itens de configurações do parque da ANA

Após a definição da linha de base de eventos, será de responsabilidade da CONTRATADA avaliar se todos os ativos estão enviando corretamente para a ferramenta definida no tópico SOBRE AS FERRAMENTAS A SEREM UTLIZADAS.

Caso a CONTRATADA identifique a ausência dos insumos (logs e pacotes de rede) a ser gerado por um item de configuração, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo dos itens de configuração descritos no tópico AMBIENTE TECNOLÓGICO DA ANA (Hardware e Software). Caso o item de configuração não pertencer ao objeto contratado, porém necessário para a correta geração do evento, deverá a CONTRATADA solicitar à ANA a correção e/ou habilitação de tal insumo no item de configuração em questão.

Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de ataques da CONTRATADA deve focar as ações nos eventos que são significativos, logo tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

- Eventos de Informação: Estes eventos não requerem qualquer ação. São usados para fazer verificação de funcionalidade dos itens de configuração de segurança. Ou seja, tem por objetivo puro e simples, identificar se a ferramentas e soluções, estão funcionando dentro do esperado. Estes eventos são também uteis para gerar estatísticas como por exemplo, porcentagem de hosts com a última vacina de antivírus do dia.
- Eventos de Aviso: Este grupo de eventos deve ser utilizado, quando existe algum comportamento anômalo se comparado a linha de base de operação padrão do ambiente (serviço, trafego e/ou solução), porém ainda não gerou algum tipo de impacto ao ambiente (serviço, trafego e/ou solução) da ANA, como por exemplo fictício: É esperado que exista 1000 (mil) ataques do tipo port scan bloqueados pelo firewall, porém na última hora este número passou para 10000 (dez mil) ataques, todavia o firewall ainda continua bloqueando sem que haja degradação da performance do ambiente (serviço, trafego e/ou solução).
- Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e confidencialidade), foram impactados, como por exemplo: Uma infecção gerada por um malware do tipo *ransomware*, onde a mesma não tenha sido bloqueada pela solução de antivírus da ANA. Este é o único tipo de evento que pode iniciar o processo de resposta a incidente de segurança, descrito no tópico PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO.do presente termo de referência.

Uma vez classificado o evento se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

- Para eventos do tipo Informação, não é requerido qualquer tipo de ação, porém como já mencionado no presente termo de referência, tais eventos são utilizados para verificação do perfeito funcionamento das soluções de segurança, portanto se espera que a CONTRATADA os utilize para tal.

- Para eventos do tipo Aviso, deve existir a garantia por parte da CONTRATADA, que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de ataques, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomando as ações cabíveis para identificar a causar raiz da mudança de comportamento do ambiente.
- Para eventos do tipo Exceção, deverá a CONTRATADA transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação, definida no PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, descrito no presente termo de referência. Após a abertura do incidente de segurança obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status "aberto" ou "encerrado", ou seja, após o correto tratamento o evento deverá ter seu status alterado na ferramenta de "aberto" para "encerrado".

Importante ressaltar que todo processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

Grupo técnico de monitoramento de ataques cibernéticos,

Através do seu CSOC do inglês Cyber Security Operations Center definidos no tópico CSOC - CYBER SECURITY OPERATIONS CENTER. a CONTRATADA deverá manter uma torre de operação denominada GRUPO DE MONITORAMENTO DE ATAQUES, com objetivo e foco de trabalhar no processo de monitoramento de ataques cibernéticos.

Este grupo deverá ser exclusivo para trabalhar no serviço em questão, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.

A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo monitoramento de ataques cibernéticos da ANA, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE MONITORAMENTO DE ATAQUES, com ao menos 1 (um) perfil de cada que segue descrito a seguir.

Perfis	Certificações	Descrição

Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança II	ComTIA Cybersecurity Analyst (CySA+)	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação
Analista de Segurança III	Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE MONITORAMENTO DE ATAQUES, porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE MONITORAMENTO DE ATAQUES.

No momento da assinatura do contrato será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE MONITORAMENTO DE ATAQUES, os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: curriculum vitae para comprovação de habilidades, termo de confidencialidade e sigilo assinados e as devidas certificações técnicas para comprovação do conhecimento.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a ANA definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do portal de segurança descrito através do anexo III do presente termo de referência, a saber:

- Período em que foi realizado o serviço;
- Quantitativo total de eventos correlacionados;
- Quantitativo total de pacotes correlacionados;
- Quantitativo total de incidentes abertos;
- Quantitativo total de solicitações por grupo de tecnologia;
- Quantitativo total de regras de correlacionamento;
- Top 10 de regras de correlacionamento;
- Top 10 de IPs de destino de regras de correlacionamento;
- Top 10 de regras de correlacionamento por pais de origem;
- Top 10 dos tipos de ataques.
- Relatório técnico pró-ativo do ambiente de estações de trabalho, notebooks e servidores de rede).

Tais relatórios e indicadores serão apresentados e discutidos em reunião mensal, com a presença do preposto da CONTRATADA e toda a equipe técnica que seja necessária para esclarecer quaisquer dúvidas pertinentes aos eventos ocorridos no período. A apresentação poderá ser de forma presencial nas dependências da ANA ou de forma virtual, por meio de solução de videoconferência.

1.4 SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA

Tem por objetivo, analisar, remediar, conter e documentar os eventos de segurança da informação, que após analisados se descobriu que de fato era um ataque iminente a, e foram transformados em um incidente de segurança da informação. Tal serviço deverá ser executado através de um **CSOC** do inglês Cyber Security Operations Center, obedecendo os principais frameworks de resposta a incidente de segurança da informação, e boas práticas de mercado já conhecidas.

Sobre as ferramentas a serem utilizadas,

Todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

- Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre);

- Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço.
- O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

O hardware necessário para instalação e configuração do ferramental será fornecido pela infraestrutura da ANA.
As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Anexo III.

Processo de resposta a incidente de segurança da informação,

Um incidente de segurança é definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação da ANA, levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Logo o início do processo de resposta a incidente de segurança se dará, sempre que um evento adverso for submetido pelo SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICOS descrito no presente termo de referência, porém não se limitando a este. Poderá o corpo técnico da ANA a qualquer tempo, abrir um incidente de segurança.

Após o incidente de segurança aberto, será de responsabilidade do grupo de resposta a incidente de segurança, analisar os logs e artefatos enviados, a fim de no primeiro instante identificar as fontes geradoras de tais logs.

Uma vez realizado as análises iniciais do incidente gerado, o grupo de resposta a incidente de segurança, deverá identificar quais foram os principais vetores de ataque ao ambiente da ANA.

Como próximo passo o grupo de resposta a incidente de segurança, deverá comunicar ao time de segurança da informação da ANA as informações iniciais sobre o incidente de segurança gerado, e quais serão as linhas de atuação para solução do incidente.

Juntamente com a ANA o grupo de resposta a incidente de segurança, deverá definir qual a severidade do incidente de segurança. A severidade do incidente de segurança da informação será definida através da combinação de urgência e impacto, onde impacto é definido como a medida de criticidade do negócio referente ao incidente, e urgência refere-se à velocidade necessária para resolver um incidente. Mais detalhes sobre definição da severidade se encontram no tópico ACORDO DE NÍVEIS DE SERVIÇO.

Após análises iniciais do incidente, caberá ao o grupo de resposta a incidente de segurança, realizar uma análise mais profunda do incidente baseando-se no comportamento do ataque e/ou artefato (malware).

Todo o processo de análise e resultados obtidos, devem ser documentados a todo tempo na ferramenta de gestão de incidente da segurança da informação, para que a ANA acompanhe todos os passos para a solução do incidente.

Uma vez identificado comportamento e os principais vetores de ataque, o grupo de resposta a incidente de segurança, deverá definir e executar uma estratégia para a mitigação e contenção do ataque em questão. Caso seja necessário qualquer tipo de alteração no parque computacional da ANA, para contenção e mitigação do incidente, deverá antes ser autorizado tal alteração pelo corpo técnico de segurança do ANA.

Mitigado o incidente de segurança, o próximo passo exigido é que a CONTRATADA através do grupo de resposta a incidente de segurança, inicie o processo de recolhimento de toda e quaisquer evidências, e identificação dos serviços afetados. Tais evidências serão utilizadas até a finalização do processo, para execução de análise forense do caso.

Inicia-se então o processo de restauração dos serviços e soluções afetadas. Todo este processo é de responsabilidade da CONTRATADA, sendo realizado pelo grupo de resposta a incidente de segurança.

Deve-se reunir os dados coletados durante o processo de tratamento de incidente, para iniciar o processo de análise forense do mesmo, ainda pelo grupo de resposta a incidente de segurança. Tal análise deve ser realizada com o objetivo de identificar (pessoas, locais e/ou eventos), correlacionando todas as informações reunidas, e gerando como produto final um laudo sobre o incidente de segurança em questão.

O grupo de resposta a incidente de segurança, deve documentar na ferramenta de incidente de segurança, as lições aprendidas do incidente de segurança em questão, formando durante todo o período de vigência do contrato uma grande base de conhecimento sobre ataques adversos.

Grupo técnico de incidente de segurança da informação,

Este grupo deverá ser exclusivo para trabalhar no SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA, não podem os profissionais pertencentes a este grupo serem compartilhados e/ou atuarem, com os demais serviços descritos no objeto do presente termo de referência.

Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.

A fim de garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de resposta a incidente de segurança do ANA, a CONTRATADA obrigatoriamente deverá compor o GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT – Blue Team), com ao menos 1 (um) perfil de cada que segue descrito a seguir.

Perfis	Certificações	Descrição

Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.
Analista de Segurança III	Certified Ethical Hacker	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 5 (cinco) anos em segurança da informação

Não existe restrição ou limite para acúmulo de perfis em um mesmo profissional, uma vez que é de responsabilidade da CONTRATADA definir o quantitativo de profissionais envolvidos no GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT), porém conforme já fora mencionado no presente termo de referência, este(s) deve(m) compor único e exclusivamente o time denominado GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT).

No momento da assinatura do contrato será exigido da CONTRATADA, as seguintes documentações do(s) profissionais que participarão do GRUPO DE RESPOSTA A INCIDENTE DE SEGURANÇA (CSIRT), os quais devem comprovar as exigências e obrigações descritas no presente termo de referência: curriculum vitae para comprovação de habilidades, termo de confidencialidade e sigilo assinados e as devidas certificações técnicas para comprovação do conhecimento.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela **CONTRATADA**, a **ANA** define os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do portal de segurança descrito através do anexo III do presente termo de referência, a saber:

- Período em que foi realizado o serviço;
- Quantitativo total de incidentes abertos;
- Quantitativo de incidentes que resultaram em comprometimento da segurança;

- Quantitativo de incidentes que tenham potencial de comprometer a segurança;
- Quantitativo de incidentes que não tenham potencial de comprometer a segurança;
- Top 10 de IPs de destino de incidentes de segurança;
- Top 10 de incidentes de segurança por origem;
- Top 10 dos tipos de incidentes;
- Relatório de Incidentes.

Tais relatórios e indicadores serão apresentados e discutidos em reunião mensal, com a presença do preposto da CONTRATADA e toda a equipe técnica que seja necessária para esclarecer quaisquer dúvidas pertinentes aos eventos ocorridos no período. A apresentação poderá ser de forma presencial nas dependências da ANA ou de forma virtual, por meio de solução de videoconferência.

1.5 SERVIÇO DE GESTÃO DE SEGURANÇA DE ENDPOINTS E SERVIDORES DE REDE

Com objetivo proteger as estações de trabalho e os equipamentos servidores de rede corporativos, de forma eficiente, bloqueando a entrada e saída de informações críticas ou sensíveis, bem como examinar todo o conteúdo em busca de vírus, malwares, botnets ou outras ameaças avançadas.

Sobre as ferramentas a serem utilizadas,

Todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

- Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre);
- Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço;
- O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

O hardware necessário para instalação e configuração do ferramental será fornecido pela infraestrutura da ANA.
As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Processo de gestão de segurança de endpoint e servidores de rede,

Será de responsabilidade da CONTRATADA compatibilizar a proteção de endpoints e servidores de rede de acordo com as premissas estabelecidas na tal política de segurança da informação no ambiente da ANA.

Diante do exposto, como primeiro passo nos processos de proteção de endpoints e servidores, será de responsabilidade da CONTRATADA a instalação dos agentes da solução de antivírus.

A ANA deverá apresentar uma lista de endpoints e servidores de rede que deverão fazer parte do processo de proteção. Tal lista poderá ser revisitada e atualizada durante todo o período de vigência de contrato.

A CONTRATADA deverá realizar de forma continuada uma avaliação prévia no ambiente computacional da ANA, a fim de consultivamente sugerir melhorias nas regras de utilização das estações de trabalho da ANA.

O passo que segue será a definição e adoção de linha de base para avaliação do ambiente de endpoints e servidores de rede. Essa avaliação não se deterá apenas a está ação, mas também adicionará as análises das linhas de base de fabricantes e frameworks de segurança focados nesse tipo de serviço específico.

Após definição de linha de base, a CONTRATADA deverá submeter tal linha de base para aprovação do ANA, antes de iniciar o processo de instalação dos agentes da solução de antivírus. Caberá único e exclusivamente ao time de segurança da informação da ANA, a aprovação de tal linha de base.

Alcançada a aprovação da linha de base, será de responsabilidade da CONTRATADA a instalação dos agentes em todo ambiente de endpoints e servidores de rede da ANA comparando os itens de controle da linha de base estabelecida.

Após o término das instalações no ambiente, deverá a CONTRATADA realizar uma análise do resultado do escaneamento de todos os endpoints e servidores de rede para a montagem do cenário inicial dos serviços.

Após análise dos resultados, a CONTRATADA deverá informar a ANA as não conformidades encontradas.

Cabe único e exclusivamente a ANA liberar e/ou autorizar toda e qualquer mudança, sugerida para correção de uma não conformidade. Sendo assim, nenhuma mudança deve ser realizada, sem que antes haja a liberação da mesma pela ANA.

Uma vez autorizada a mudança para correção de uma determinada não conformidade, caberá a CONTRATADA apenas as correções de não conformidade encontradas no ambiente listado no tópico AMBIENTE TECNOLÓGICO DA ANA (Hardware e Software), obrigatoriamente obedecendo as definições proposta pelo comitê de mudança da ANA.

Para as não conformidades encontradas no ambiente que ainda não tiverem soluções conhecidas, caberá a CONTRATADA apresentar medidas de contorno, que para aplicá-las ao ambiente, deverá obedecer ao ciclo de mudança estabelecido nos parágrafos anteriores.

O processo descrito é mínimo esperado a ser seguido e executado pela CONTRATADA, todavia como o objeto do presente termo de referência se trata de serviço, se espera da CONTRATADA a apresentação da melhoria contínua deste, a qual pode ser alterado desde que aprovado pela ANA.

É importante que a CONTRATADA, atente-se ao cumprimento de todo o atendimento as leis, políticas, normas regulatórias e processos de auditoria no âmbito da ANA, bem como no auxílio da governança e da tomada de decisões do negócio. Caso encontre alguma discordância das aplicações será necessário a rápida intervenção, com a devida anuência da ANA, para o restabelecimento da ordem.

Grupo técnico de gestão de segurança de endpoints e servidores de rede,

Para o serviço de Gestão de Segurança de Endpoints e Servidores de Rede, não haverá um grupo exclusivo para execução. O grupo responsável por tal execução poderá ser do SERVIÇOS DE MONITORAMENTO.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela **CONTRATADA**, foi definido os seguintes indicadores de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do portal de segurança:

- Período em que foi realizado o serviço;
- Quantitativo de estações de trabalho atualizadas com os agentes;
- Quantitativo de estações de trabalho não atualizadas;
- Quantitativo de servidores de rede atualizados;
- Quantitativo de servidores de rede não atualizados
- Top 10 dos malwares encontrados nas estações de trabalho;
- Top 10 dos malwares encontrados nos servidores de rede;
- Top 10 das estações de trabalho mais infectadas;
- Top 10 dos servidores de rede mais infectados.

Tais relatórios e indicadores serão apresentados e discutidos em reunião mensal, com a presença do preposto da CONTRATADA e toda a equipe técnica que seja necessária para esclarecer quaisquer dúvidas pertinentes aos eventos ocorridos no período. A apresentação poderá ser de forma presencial nas dependências da ANA ou de forma virtual, por meio de solução de videoconferência.

1.6 SERVIÇO DE GESTÃO DE SEGURANÇA DE MENSAGERIA PROATIVA

Com objetivo proteger os serviços de mensageria utilizado pelos usuários da **ANA**, deverá bloquear de forma eficiente a entrada e saída de e-mails indesejados, bem como examinar todo o conteúdo em busca de vírus, phishing, botnets, ameaças avançadas, vazamento de informações, entre outros.

Sobre as ferramentas a serem utilizadas,

Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de proteção de mensageria que atendam o descritivo técnico a seguir.

Independente do grupo das soluções supracitadas, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

- Deverá ser obrigatoriamente de propriedade da CONTRATADA, não poderá ser do tipo open source (software livre);
- Os softwares ofertados devem ser instalados em sua versão mais estável e atualizada e estar cobertos por contratos de suporte e atualização de versão do fabricante durante a vigência do respectivo item de serviço;
- O conjunto de requisitos especificados para cada serviço pode ser atendido por meio de composição com outros equipamentos ou softwares utilizados no atendimento aos demais itens, de maneira integrada, desde que não implique alteração da topologia de rede ou na exposição de ativos a riscos de segurança da informação, em termos de integridade, confidencialidade ou disponibilidade.

O hardware necessário para instalação e configuração do ferramental será fornecido pela infraestrutura da ANA.

As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Processo de gestão de segurança de mensageria proativa,

A fim de balizar todo o processo de proteção de mensageria da ANA, influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis litteris.

O processo será divido em duas etapas, primeiramente será levantado as informações do ambiente da ANA, como os servidores de DNS, políticas de proteção atualmente em funcionamento, definições de White list e Black List já existentes etc. tais definições serão coletas junto à ANA para subsidiar a configuração da solução, bem como mitigara falsos positivos.

A etapa seguinte está fundamentada no processo inicial de configuração e testes, para averiguação da capacidade da solução nesta etapa será seguido a seguinte trilha, contudo não limita aos itens subsequentes:

- Implementação das políticas;
- Testes de conectividade.
- Consolidação e tuning das políticas implementadas;
- Testes de White List e Black List;

- Testes com a Quarentena;
- Testes de geração de relatórios;
- Backup das configurações.

Pós processo das etapas anteriores, a CONTRATADAdeve informar a ANA qual melhor estratégia de mudança para migração do serviço atual de e-mail para a solução contratada.

Pós autorização da ANA, a CONTRATADA terá a responsabilidade de iniciar a execução dos serviços, observando e seguindo as definições acordadas e autorizadas previamente.

Após término das implementações a contratada deve sustentar a configuração, suporte, manutenção e atualização da solução oferecida durante toda a vigência do contrato.

Grupo técnico de gestão de segurança de mensageria proativa,

Para o serviço de proteção de mensageria, não haverá um grupo exclusivo para execução. O grupo responsável por tal execução poderá ser do SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a ANA define os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do portal de segurança descrito através do anexo II do presente termo de referência, a saber:

- Período em que foi realizado o serviço;
- Quantidade de mensagens bloqueadas;
- Quantidade de mensagens seguras entregues;
- Relação dos domínios / regiões de onde se encaminham as mensagens;
- Top 10 dos países com mensagens bloqueadas;
- Top 10 dos domínios com mensagens bloqueadas.

Tais relatórios e indicadores serão apresentados e discutidos em reunião mensal, com a presença do preposto da CONTRATADA e toda a equipe técnica que seja necessária para esclarecer quaisquer dúvidas pertinentes aos eventos ocorridos no período. A apresentação poderá ser de forma presencial nas dependências da ANA ou de forma virtual, por meio de solução de videoconferência.

1.7 SERVIÇO DE INTELIGÊNCIA APLICADA A SEGURANÇA

Visa o monitoramento continuo e ininterrupto de ameaças cibernéticas acessíveis na internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS e páginas de comércio eletrônico, identificando e reconhecendo os eventos de segurança da informação, aos quais devem ser

analisados e processados, podendo estes serem transformados em um incidente de segurança da informação, obedecendo um processo cíclico e rigoroso de gestão de eventos.

O Serviço de Inteligência Aplicada à Segurança Cibernética deve ser provido por meio de plataforma SaaS (software as a service) ou on-premisse.

Sobre as ferramentas a serem utilizadas,

Para execução deste serviço, a CONTRATADA deverá utilizar e ser capaz de fornecer, operar, sustentar e suportar soluções de monitoramento de riscos digitais.

Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.

As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Processo de atendimento para inteligência aplicada a segurança,

A CONTRATADA será responsável por implantar, operar e suportar toda a plataforma ofertada.

A fim de balizar todo o processo de monitoramento de riscos digitais da ANA, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis litteris.

É sabido que para o sucesso de um monitoramento de riscos digitais, a primeira definição se deve a que tipo de ocorrência de eventos de segurança, se deseja detectar e tomar algum tipo de ação, logo será de responsabilidade da CONTRATADA como primeiro passo deste processo, a definição dos ativos digitais que deverão ser monitorados. Entenda-se por ativos digitais, marcas, domínios, aplicativos móveis e/ou usuários a serem monitorados;

Tal definição da relação de ativos digitais a ser monitorada, não deve ser tomada de forma unilateral pela CONTRATADA. A ANA deverá participar ativamente no processo de construção de forma consultiva. Porém, se ratifica que é de responsabilidade da CONTRATADA a definição, e colocar em operação tal linha de base.

Espera-se que a relação de ativos digitais monitorados, seja revista de forma mensal, contudo, não se limitando a este tempo, pois todos os dias novos ataques são projetados no mundo, e se espera que a CONTRATADA tome ciência destes ataques, e por sua vez atualize a relação de ativos digitais, para que em um cenário onde estes novos ataques sejam direcionados à ANA, sejam detectados através dos serviços em questão.

O produto de um evento é a detecção de citações, termos ou referências aos ativos monitorados, seja na deep/dark web, na internet aberta, em páginas de compartilhamento, redes sociais e aplicativos monitorados, gerados pela solução de proteção de riscos digitais utilizada pela CONTRATADA para execução deste serviço. Uma vez definida a relação de ativos digitais monitorados, será também de responsabilidade da CONTRATADA avaliar se todos os insumos para a correta geração do evento, estão sendo enviados corretamente para a ferramenta.

Caso a CONTRATADA identifique a ausência dos insumos (ativos) a ser gerado, será de reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo, restaurando a monitoração do ativo.

Dar-se-á então o passo de classificação do evento, também de responsabilidade da CONTRATADA. O grupo de monitoramento de riscos digitais da CONTRATADA deve focar as ações nos eventos que são significativos. Logo, tal grupo deve analisar todos os eventos apresentados, classificando-os nos seguintes grupos, a saber:

- Eventos de Informação: Estes eventos não requerem qualquer ação. Este grupo de eventos deve ser utilizado quando há menção não criminosa a um ativo digital monitorado, por exemplo, uma menção simples em uma rede social contendo o nome da ANA;
- Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento suspeito em relação a um ativo digital monitorado, por exemplo, uma menção na internet, deep ou dark web, ou qualquer outro meio monitorado, com contexto de ameaças e/ou ataques direcionados a CONTRATADA;
- Eventos de Exceção: Estes eventos são aqueles que sugere que os pilares de segurança da informação (confidencialidade, integridade e conformidade), foram impactados como, por exemplo: Detecção de um vazamento de dados da ANA e venda de informações em canais de fraude.

Uma vez classificado o evento, se inicia o passo de resposta ao mesmo, que também é de responsabilidade da CONTRATADA. As respostas são baseadas nos grupos de classificação de eventos, a saber:

- Para eventos do tipo informação, não é requerido qualquer tipo de ação, porém, os eventos devem ser armazenados durante a vigência do contrato;
- Para eventos do tipo Aviso, a CONTRATADA deverá garantir que uma interface humana, ou seja, uma analista que pertence ao grupo de monitoramento de riscos digitais, esteja validando se tal evento pode se transformar em um evento do tipo exceção, e obviamente tomar as ações cabíveis para identificar a causa raiz;
- Para eventos do tipo Exceção, a CONTRATADA deverá transformar tal evento em um incidente de segurança, realizando, portanto, a abertura do mesmo na ferramenta de incidente de segurança da informação definida no PROCESSO DE RESPOSTA A INCIDENTE DE SEGURANÇA DA INFORMAÇÃO, descrito no presente termo de referência. Após a abertura do incidente de segurança, obedecendo os critérios estabelecidos para tal, se encerra a participação do grupo de monitoramento de ataques.

Como último passo do processo, a CONTRATADA deve encerrar os eventos após as devidas ações tomadas, conforme definido no parágrafo acima. Eventos podem ter apenas dois tipos de status “aberto” ou “encerrado”, ou seja, após o correto tratamento, o evento deverá ter seu status alterado na ferramenta de “aberto” para “encerrado”.

Importante ressaltar que todo o processo de tratamento do evento, independente de qual fase e/ou status, deve ser registrado no módulo de tratamento de eventos da ferramenta. Também é responsabilidade da CONTRATADA a segurança dos eventos, e fica expressamente proibido a remoção de qualquer evento, independentemente de sua classificação e fase de tratamento.

Grupo técnico de serviço de inteligência aplicada a segurança,

Deverá ser de responsabilidade da CONTRATADA dimensionar o número de profissionais adequado para entrega de tal serviço, sem que haja impacto no acordo de nível de serviço estabelecido no tópico ACORDO DE NÍVEIS DE SERVIÇO do presente termo de referência.

A fim de garantir que os profissionais envolvidos tenham conhecimento e habilidade para executar o processo de monitoramento de ataques cibernéticos da ANA, a CONTRATADA deverá, obrigatoriamente, compor o GRUPO DE MONITORAMENTO DE RISCOS DIGITAIS, com ao menos 01 (um) perfil de cada profissional que segue descrito a seguir.

Perfis	Certificações	Descrição
Analista de Segurança I	ISFS ISO27001	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.
Analista de Segurança II	Certified Ethical Hacker	Conhecimento avançado em segurança da informação, com experiência em monitoramento de ataques cibernéticos utilizando ferramentas e soluções de SIEM e ATD. Experiência comprovada de no mínimo 12 (doze) meses em segurança da informação.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a ANA definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on line e em tempo de execução, através do portal de segurança descrito através do anexo III do presente termo de referência, a saber:

- Período em que foi realizado o serviço;
- Quantitativa de Menções;
- Quantitativo de pacotes correlacionados;
- Quantitativo de incidentes abertos;
- Quantitativo de solicitações por grupo de tecnologia;
- Quantitativo de regras de correlacionamento;
- TOP 10 – Regras de correlacionamento;
- TOP 10 – IP de destino de regras de correlacionamento;

- TOP 10 – Regras de correlacionamento por país de origem;
- TOP 10 – Tipos de ataques.

Tais relatórios e indicadores devem ser apresentados e discutidos em reunião mensal, com presença de profissional que conheça todos os serviços. Nesse contexto, o profissional deve apresentá-lo de forma presencial nas dependências da ANA ou de forma virtual, por meio de solução de videoconferência.

1.8 SERVIÇO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Com o objetivo de conscientização de todos os usuários do parque tecnológico do CONTRATANTE, sobre a importância de seguir as políticas de segurança da informação estabelecidas. Identificando proativamente os usuários que seriam vetores de ataques, e tornando-os elegíveis para um programa de capacitação interna, sobre boas práticas de segurança da informação no ambiente corporativo do CONTRATANTE.

Sobre as ferramentas a serem utilizadas,

Soluções e/ou ferramentas utilizadas pela CONTRATADA para realizar o processo de capacitação do usuário, através de envio de e-mails falsos controlados e programa de capacitação interna.

Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.

Deverá ser obrigatoriamente de propriedade da CONTRATADA, não podendo der do tipo open source (software livre).

As ferramentas de apoio a este serviço deverão atender os requisitos apresentados no Edital.

Mecanismos de conscientização de segurança da informação,

A CONTRATADA deverá prover mecanismo de conscientização de ataque Phishing aos usuários que utilizam os sistemas da ANA, com intuito de mitigar riscos aos principais sistemas de comunicações e educar usuários quanto as normas internas da ANA e boas práticas de segurança da informação.

A solução deve possuir sua própria estrutura de envio de e-mails (Servidores SMTP), não onerado os recursos do CONTRATANTE para o envio dos e-mails de simulação.

A solução deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos.

A solução educacional contra-ataque de Phishing deve ser capaz de criar templates educacionais exclusivos para a ANA, em português com a logo marca da ANA.

A solução educacional contra-ataque de Phishing deve possibilitar na visão do usuário atacado a inserção de dados, no entanto, sejam eles quais forem os dados não devem ser armazenados de nenhuma forma, em nenhuma área de armazenamento, sejam internas a solução quanto externa.

A solução educacional contra-ataque de Phishing deve ser capaz de, durante a criação do e-mail template customizado para a ANA, conter no mínimo as parametrizações abaixo:

- Seleção de usuário e de grupo de usuários que farão parte da simulação;
- Seleção de agendamento com data e horário para início e fim de cada campanha de conscientização, especifica por grupo a ser atingido;
- Definição de assunto do e-mail de simulação do ataque Phishing;
- Definição do nome do remetente que enviará o e-mail de simulação do ataque Phishing; Definição do endereço (usuário e domínio) do e-mail de simulação do ataque Phishing;
- A solução deve possibilitar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do e-mail conteúdos dinâmicos, para no mínimo:
    - Nome do usuário;
    - Sobrenome;
    - Endereço de e-mail.
- A solução educacional contra-ataque de Phishing deve ser capaz de criar relatórios executivos e mostrar de forma gráfica no console do produto no mínimo:
    - Verificação de quantas simulações foram enviadas para a **ANA**;
    - Verificação de quantos usuários acessaram o e-mail de simulação de ataque Phishing;
    - Verificação de quantos usuários abriram o arquivo anexo do e-mail de simulação de ataque Phishing;
    - Verificação de quantos usuários inseriram os dados solicitados no e-mail de simulação de ataque Phishing; Verificação de quantos usuários reportaram para a área de TI a existência de um ataque Phishing;
    - Verificação de quantos usuários executaram os módulos de conscientização educacional Anti-Phishing.

A solução educacional contra-ataque de Phishing deve ser capaz de construir uma mensagem de conscientização, informando que usuário foi pego em uma simulação de ataque Phishing, a qual deve ser mostrada no momento que seja caracterizado como se o usuário estivesse realmente sofrido um ataque.

A solução educacional contra-ataque de Phishing deve ser capaz de indicar a necessidade de o usuário participar de uma campanha para conscientização, a partir da mensagem de conscientização (item anterior) na qual deverá existir um link direcionando para a campanha indicada para o usuário e grupos de usuários.

A solução educacional contra-ataque de Phishing deve ser capaz de apresentar de forma gráfica o progresso na conscientização dos usuários, executando gráficos comparativos entre

campanhas já realizadas pela ferramenta, onde poderá ser observado o declínio e a ascensão na maturidade e conscientização da ANA.

Processo de conscientização de segurança da informação,

A fim de balizar todo o processo de conscientização de segurança da informação da ANA, e influenciado pelos principais frameworks de boas práticas de serviços de segurança da informação, foi arquitetado o processo que será descrito nos parágrafos que seguem, o qual obrigatoriamente a CONTRATADA deve seguir ipsis litteris.

O início do processo de conscientização de segurança da informação, dar-se-á através de uma reunião envolvendo o grupo de resposta a incidente da CONTRATADA e o time de segurança da ANA. Esta reunião terá a seguinte pauta, a saber:

- Definição do período de execução da campanha de conscientização;
- Definição do tema do phishing controlado a ser enviados para os usuários;
- Definição do grupo alvo da ANA, que receberá o phishing controlado;
- Definição do alcance, isso quer dizer, se a campanha apenas validará quais usuários receberam e clicaram no phishing controlado, ou também terá a possibilidade de captura dos dados dos usuários do grupo alvo.

Pós agenda, será de responsabilidade da CONTRATADA a criação de um relatório de abertura de campanha, a qual documentará as definições acordadas. Tal relatório deverá ser enviado para o time de segurança da ANA, a qual terá a responsabilidade de aprovar a execução do serviço, conforme definições previstas em tal relatório.

Pós autorização do CONTRATANTE, a ANA terá a responsabilidade de iniciar a execução dos serviços, observando e seguindo as definições acordadas e autorizadas previamente.

Ao término da campanha será de responsabilidade da CONTRATADA, apresentar os resultados dos serviços, de tal forma que a ANA consiga compreender:

- Quais e quantos usuários clicaram no phishing, e informaram seus dados;
- Quais e quantas usuários apenas clicaram no phishing;
- Quais e quantos usuários apenas receberam o phishing e não clicaram.

Os usuários que clicaram e/ou informaram seus dados na campanha, serão elegíveis para uma palestra de segurança da informação para usuários finais, que deve abordar os temas que tem realização com a política de segurança da informação da ANA.

A criação e aplicação desta palestra será de responsabilidade da CONTRATADA. A modalidade dos treinamentos pode ser presencial, e/ou do tipo e-learning (modalidade de educação através da qual se faz necessário o uso de um ambiente virtual de aprendizagem).

A definição de execução dos treinamentos pelos funcionários elegíveis é de responsabilidade da ANA, cabendo a CONTRATADA ter o ambiente preparado sempre que solicitado pela ANA.

Grupo técnico de conscientização de segurança da informação,

Para o serviço de conscientização de segurança da informação, não haverá um grupo exclusivo para execução. O grupo responsável por tal execução poderá ser do SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA.

Entregas a serem realizadas,

Para acompanhamento e avaliação do serviço a ser ofertado pela CONTRATADA, a ANA definiu os seguintes indicadores chave de desempenho, que reunidos vão compor um único relatório a ser entregue de forma on-line e em tempo de execução, através do portal de segurança descrito através do anexo II do presente termo de referência, a saber:

- Período em que foi realizado o serviço;
- Quantitativo de campanhas realizadas;
- Dos usuários que interagiram com a campanha:
    - IP público de origem dos usuários;
    - Localização;
    - Tipo de navegador;
    - Data e Hora que o usuário clicou.
- Quantitativo total de usuários conscientes;
- Quantitativo total de usuários parcialmente conscientes;
- Quantitativo total de usuários não conscientes;
- Quantitativo total de conscientizações por meio de cartilhas educacionais.

Tais relatórios e indicadores serão apresentados e discutidos em reunião mensal, com a presença do preposto da CONTRATADA e toda a equipe técnica que seja necessária para esclarecer quaisquer dúvidas pertinentes aos eventos ocorridos no período. A apresentação poderá ser de forma presencial nas dependências da ANA ou de forma virtual, por meio de solução de videoconferência.

1.9 SERVIÇOS DE TESTES DE INVASÃO - PENTEST

A CONTRATADA deverá prover aos ambientes de aplicações, servidores e soluções de segurança da informação atualmente implementadas na ANA, mecanismo de Teste de Invasão capaz de explorar as vulnerabilidades identificadas;

A atividade de Testes de Invasão poderá ser do tipo Externo e/ou Interno na totalidade de 6 testes anuais, sendo 04 na tipologia White que é um ataque mais profundo por possuir mais informações do alvo e 02 na tipologia Black que são testes a cegas, sem qualquer informação do ambiente alvo, ambos testes terão como objetivo principal identificar, mapear, documentar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura

tecnológica. Esses testes envolvem, necessariamente, o uso de técnicas e ferramentas especificas para tentar obter acesso não autorizado e privilegiado aos ativos e informações.

Para a realização dos testes de invasão deverão ser observadas as orientações e técnicas emanadas pelos padrões internacionais, além de outros apresentados pela CONTRATADA, caso haja em seu portfólio normativos que comprovadamente complementem os demonstrados abaixo:

- OSSTMM 3 (The Open-Source Security Testing Methodology Manual);
- ISSAF/PTF (Information Systems Security Assessment Framework);
- NIST Special Publication 800-115 (Technical Guide to Information Security Testing and Assessment);
- NIST Special Publication 800-42 (Guideline on Network Security Testing);
- OWASP Web Security Testing Guide (WSTG);
- OWASP Mobile Security Testing Guide (MSTG);
- PTES Technical Guidelines (Penetration Testing Execution Standard)

Neste documento os termos “pentest”, teste de penetração, teste de intrusão e testes de invasão, são considerados sinônimos.

Os alvos dos “Testes de Invasão” bem como as premissas e condições para realização dos mesmos serão, necessariamente, definidos e aprovados através de Ordem de Serviço (OS).

A Contratada deverá observar que os testes de invasão serão executados internamente (qualquer ponto da rede corporativa da ANA) ou externamente (através da Internet).

Todas as fases dos “Testes de Invasão” serão acompanhadas e supervisionadas a critério da ANA.

Quaisquer atividades que possa comprometer ou prejudicar algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos;

O teste de invasão deverá obedecer às seguintes fases:

- Planejamento;
- Descoberta;
- Ataque;
- Relatório Teste de Invasão;
- Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste; Reavaliação, novo teste pós remediação;
- Relatório Final do Teste de Invasão.

Planejamento,

Todas as premissas, processos, atividades descritas e aprovadas na OS, inclusive os cronogramas serão detalhados e apresentados na fase de planejamento;

Informações sobre o ambiente corporativo, utilizando-se das seguintes técnicas (podendo ser utilizadas ambas, conforme definição do escopo):

- Técnica da caixa-preta (pouco ou nenhum conhecimento sobre o ambiente a ser avaliado. O ambiente deverá ser descoberto pelo especialista);
- Técnica da caixa branca (o avaliador tem acesso irrestrito a qualquer informação que possa ser relevante ao teste).

Descoberta,

Deverá ser utilizada, pelo menos, ferramentas de Análise de Vulnerabilidades, descritas no objeto, gestão de vulnerabilidades, além de técnicas manuais de análise de vulnerabilidade. As ferramentas deverão ser apresentadas para ciência e aprovação antes de sua efetiva utilização, assim como a metodologia para análise manual de vulnerabilidades.

Na fase da DESCOBERTA deverão ser atendidos os seguintes quesitos e apresentado juntamente no "RELATÓRIO TESTE DE INVASÃO" (quando necessário):

a) Coleta passiva, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

- Whois e nslookup (consultas DNS);
- Sites de busca;
- Listas de discussão;
- Blogs de colaboradores;
- Dumpster diving ou trashing;
- Informações livres;
- Packet sniffing "passive eavesdropping";
- Captura de banner.

b) Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas:

- Port scanning (Mapeamento de rede);
- Varredura de vulnerabilidade.

c) A varredura de vulnerabilidade deverá verificar/identificar, entre outros:

- Hosts ativos na rede;
- Portas e serviços em execução;
- Serviços ativos e vulneráveis nos hosts;
- Sistemas operacionais;
- Vulnerabilidades associadas com sistemas operacionais e aplicações descobertas; Configurações feitas nos hosts sem observância de boas práticas em segurança computacional;
- Identificação de rotas e estimativa de impacto, caso estas sejam modificadas/desconfiguradas;
- Identificação de vetores de ataque e cenários para exploração;
- Vulnerabilidades Detectadas (CVE);
- Vulnerabilidades de Alto Risco;
- Vulnerabilidades de Médio Risco;
- Vulnerabilidades de Baixo Risco;
- Informações a serem aplicadas na fase de ataques.

d) Dos serviços e aplicações web:

- Uso indevido de sistema de arquivos e arquivos temporários;
- Evasão de informação por configurações default de tratamento de erros;
- Tratamento indevido de entrada;
- Problemas relacionados à má configuração dos serviços;
- Gerenciamento inseguro de sessões web.

Ataque (exploração),

Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo deverá ser imediatamente reportada, antes de sua execução, haja vista a necessidade de manter a disponibilidade dos ambientes e serviços ativos.

Deverá realizar testes de vulnerabilidades e invasão em endereços IP's, URL´s, aplicações, ou outro ativo definido do ambiente computacional, composto por servidores, banco de dados, ativos de rede, ativos de segurança e outros equipamentos relacionados ao teste de invasão.

Deverão ser aplicados, no mínimo, os seguintes tipos de ataques:

- Violações do protocolo HTTP;

- SQL Injection;
- LDAP Injection;
- Cookie Tampering;
- Cross-Site Scripting (XSS); Directory Transversal;
- Buffer Overflow;
- OS Command Execution;
- Command Injection;
- Remote Code Inclusion;
- Server Side Includes (SSI) Injection; File disclosure;
- Information Leak;
- Zero day attacks;
- DDos (Distribuited Denial of Service);
- Dos (Denial of Service);
- Contra protocolo TCP;
- Ataques contra a aplicação.

Os ataques de negação de serviços, contra protocolo TCP e em nível da aplicação deverão, cada qual, explorar/demonstrar/utilizar as seguintes técnicas:

a) Bugs em serviços, aplicativos e sistemas operacionais;

b) SYN flooding;

c) Fragmentação de pacotes de IP;

d) Smurf e fraggle;

e) Teardrop, nuke e land;

f) Para ataques contra o protocolo TCP:

- Sequestro de conexões;
- Prognóstico de número de sequência do protocolo TCP.

g) Ataque de Mitnick;

- Source routing.

h) Para ataques em nível da aplicação:

- Buffer Overflow;
- Problemas com o SNMP;
- Vírus, worms e cavalos de Tróia.

i) Injeção de Código:

- Ataques XSS (Cross-site Script); Comprometimento do acesso remoto;
- Manutenção de acesso;
- Encobrimento de rastros da invasão.

Para testes de invasão direcionados, especificamente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, os seguintes testes baseados na publicação OWASP TESTING GUIDE 3.0 ou superior (The Open Web Application Security Project):

- Para testes de coleta de informações, aplicar padrão: OWASP-IG-001, OWASP-IG-002, OWASPIG-003, OWASP-IG- 004, OWASP-IG-005 e OWASP-IG-006;
- Para testes de gerenciamento de configuração, aplicar padrão: OWASP-CM001, OWASP-CM-002, OWASP-CM-003, OWASP-CM-004, OWASP-CM005, OWASP-CM-006, OWASP-CM-007, OWASPCM-008;
- Para testes de autenticação, aplicar padrão: OWASP-AT-001, OWASP-AT002, OWASP-AT-003, OWASP-AT-004, OWASP-AT-005, OWASP-AT-006, OWASP-AT-007, OWASP-AT-008, OWASP-A e OWASP-AT-010;
- Para testes de gerenciamento de sessão, aplicar padrão: OWASP-SM-001, OWASP-SM-001, OWASP-SM-002, OWASP-SM-003, OWASP-SM-004, OWASPSM-005;
- Para testes de autorização, aplicar padrão: OWASP-AZ-001, OWASP-AZ-002 e OWASP-AZ-003;
- Para testes de negócio lógico, aplicar padrão: OWASP-BL-001;
- Para testes de validação de dados, aplicar padrão: OWASP-DV-001; OWASPDV-002, OWASPDV-003, OWASP-DV- 004, OWASP-DV-005, OWASP-DV-006, OWASP-DV-007, OWASP-DV-008, OWASPDV-009, OWASP-DV-010, OWASP-DV-011, OWASP-DV-012, OWASP-DV-013, OWASP-DV-014, OWASPDV-015 e OWASP-DV-016;
- Para testes de negação de serviços, aplicar padrão: OWASP-DS-001, OWASPDS-002, OWASPDS-003, OWASP-DS- 004, OWASP-DS-005, OWASP-DS006, OWASP-DS-007 e OWASP-DS-008;
- Para testes de serviços web, aplicar padrão: OWASP-WS-001, OWASP-WS002, OWASP-WS-003, OWASP-WS-004, OWASP-WS-005, OWASP-WS006 e OWASP-WS-007.

Observa-se que o resultado de cada teste deverá vir acompanhado de relatórios contendo:

- Referência base (Whitepaper);
- Ameaças encontradas;
- Riscos levantados ao ambiente computacional;
- Contramedidas para mitigar as ameaças encontradas.

Relatório de teste de invasão,

Deverá ser elaborado e entregue a ANA após a fase de ataque, o relatório "RELATÓRIO TESTE DE INVASÃO" para cada teste que será realizado, contemplando no mínimo informações, tais como:

a) Objetivos, premissas e escopo do teste, datas e horas dos testes, metodologia de análise de vulnerabilidades, descrição das ações realizadas, metodologias, vulnerabilidades encontradas, categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades, apresentação das evidências apuradas, fontes de pesquisa, referências e ferramentas utilizadas, informações acessadas e demais evidências do sucesso da invasão.

b) Após a fase de ataque, deverão ser atendidas e apresentadas no Relatório, no mínimo, as seguintes informações detalhadas:

- Detalhes da infraestrutura descoberta, alvo dos testes de invasão; Equipamentos e recursos demandados para este teste;
- Tipos de ataque;
- Prazos (janelas de tempo para execução dos testes);
- Pontos de contato da contratada (responsáveis para tratamento de questões abordadas nos testes);
- Tipos de testes realizados pelos especialistas em segurança da informação;
- Confirmação ou refutação de a existência de vulnerabilidades;
- Documentação sobre o caminho utilizado para exploração, avaliação do impacto e prova da existência da vulnerabilidade;
- Obtenção de acesso e possível escalada de privilégios; Detalhamento da metodologia do ataque;
- Recomendações para sanar riscos e vulnerabilidades.

Será realizada reunião conduzida pela Contatada, onde será apresentado de forma detalhada todo o conteúdo do "RELATÓRIO TESTE DE INVASÃO", onde serão sanadas todas as dúvidas do corpo técnico da ANA.

Após a entrega do "RELATÓRIO DE TESTE DE INVASÃO", a ANA analisará o documento para aplicar as recomendações, remediar os riscos ou mesmo assumi-los.

Sobre as ferramentas a serem utilizadas,

Independente das fases supracitadas, todas as soluções e/ou ferramentas utilizadas para prestação do serviço deverão obrigatoriamente seguir os requisitos, a saber:

Deverá ser prestado por meio de solução provida através da nuvem do fabricante ou da CONTRATADA.

Grupo técnico de teste de invasão,

Para o serviço de teste de invasão, caberá à contratada, garantir que os profissionais envolvidos têm conhecimento e habilidade, para executar o processo de teste de invasão, com ao menos 1 (um) perfil de cada que segue descrito a seguir.

Perfis	Certificações	Descrição
Analista de Segurança I	CompTIA Security+	Diploma, devidamente registrado, de curso de nível superior de graduação na área de Tecnologia da Informação ou de graduação em qualquer curso superior, acrescido de certificado de curso de pós-graduação em área de Tecnologia da Informação de, no mínimo, 360 (trezentos e sessenta) horas, fornecido por instituição reconhecida pelo Ministério da Educação (MEC); Conhecimento avançado em segurança da informação, com experiência em análise de vulnerabilidade e testes de penetração de segurança da informação. Experiência comprovada de no mínimo 3 (três) anos em segurança da informação.

ANEXO II – MODELO DE EXECUÇÃO DOS SERVIÇOS

A execução do objeto contratado seguirá o modelo de execução descrito a seguir. Este modelo define as diretrizes e procedimentos que serão adotados durante a prestação dos serviços, visando garantir o cumprimento dos prazos, a qualidade das entregas e a satisfação das partes envolvidas, ressaltando que:

- Caso haja necessidade de ajustes ou modificações durante a execução dos serviços, os mesmos deverão ser discutidos e acordados em uma reunião específica entre o representante designado pela contratada e os gestores da CONTRATANTE. Essas alterações serão formalizadas e registradas em ata, a qual será elaborada pelo representante da contratada.
- A reunião para tratar dos ajustes contratuais terá como objetivo analisar e avaliar as necessidades apresentadas, considerando as demandas da CONTRATANTE e a viabilidade técnica e operacional da contratada. Serão discutidos os impactos financeiros, prazos de execução, recursos necessários e quaisquer outras questões relacionadas às alterações propostas.
- Ressalta-se que a elaboração da ata das reuniões ficará sob a responsabilidade do representante da contratada, garantindo que todas as discussões, decisões e encaminhamentos sejam devidamente registrados e documentados para posterior referência e validação.
- A adoção desse processo de ajustes contratuais, de forma formal e documentada, busca promover a transparência, a clareza e a conformidade com as exigências contratuais, além de facilitar a comunicação e a tomada de decisões entre as partes envolvidas.

Cabe ressaltar que quaisquer ajustes ou modificações realizados deverão estar em conformidade com as cláusulas contratuais e legislação aplicável, não alterar e não se contrapor ao Edital, e visar sempre o interesse mútuo das partes e o bom andamento do contrato.

Canais de comunicação,

Para abertura de solicitações a CONTRATADA deverá disponibilizar três tipos de canais de comunicação, a saber:

Item	Grupo de Tecnologia	Classificação
1	Linha de telefonia gratuita (0800) ou DDD local (61).	Tipo 1
2	E-mail com domínio registrado e de propriedade da CONTRATADA.	Tipo 2
3	Sistema de ITSM do inglês *Information Technology Service Management* (Gerenciamento de Serviços de TI).	Tipo 3

Independente do canal de comunicação utilizado pela ANA, as solicitações devem ser convergidas, atualizadas, resolvidas e concentradas em um único sistema de ITSM do inglês Information Technology Service Management (Gerenciamento de Serviços de TI). Ou seja, imaginando que a ANA realize a abertura de uma nova solicitação de serviço via linha telefônica gratuita, no segundo que segue a sua solicitação, a mesma deve constar no sistema de ITSM, assim também deve se proceder com a utilização do canal de comunicação do tipo 2: via e-mail.

Sobre o canal de comunicação do tipo 1: via linha telefonia gratuita (0800) ou DDD local (61), tais ligações obrigatoriamente devem ser atendidas e/ou recepcionadas por uma interface humana, não sendo permitido utilização de URA (Unidade de Resposta Audível), e/ou qualquer usufruto de atendimento eletrônico.

Para um eventual cenário de crise, ou seja, onde o negócio fim da ANA estar sendo fortemente afetado por um problema envolvendo a segurança da informação, a CONTRATADA deverá disponibilizar uma sala de videoconferência virtual de sua propriedade, onde a qualquer tempo poderá ser utilizada para reuniões emergenciais para tratamento de crises.

Tal sala deve estar disponível via internet e seu acesso deve obrigatoriamente ser criptografado, utilizando protocolo SSL do inglês Secure Socket Layer, com certificado digital emitido em nome da CONTRATADA. A CONTRATADA também deve garantir que os protocolos de comunicação, utilizados pela sala de videoconferência deve ser criptografado.

A sala virtual ainda deve ter capacidade para até 10 (dez) pessoas da ANA simultaneamente, e a fim de evitar eventuais perdas de tempo em momento de crise, a sala deve estar acessível a qualquer tempo, não sendo criada apenas no momento da crise.

Horário de atendimento,

Os SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA, devem obrigatoriamente serem executados, ofertados, e estarem acessíveis à ANA em regime de 24 (vinte quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, durante todo o período de vigência do contrato.

Modalidade de atendimento,

A modalidade principal de atendimento será do tipo remota, ou seja, a ser realizada através das dependências da CONTRATADA, obrigatoriamente obedecendo os critérios estabelecidos para execução do mesmo, no presente termo de referência.

Eventualmente a ANA poderá solicitar uma visita técnica, para que um atendimento qualquer possa ser realizado e/ou acompanhado, em suas dependências físicas.

Os atendimentos referentes ao objeto contratado denominado SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA é ilimitado durante o período de vigência do contrato, ou seja, não existe limite para quantidade de horas, e/ou quantidade de atendimentos realizados, com exceção do item SERVIÇOS CONTINUADOS DE SEGURANÇA da ANA.

Acessibilidade e confidencialidade,

Para garantir a qualidade e disponibilidade dos serviços remoto, deverá entre a ANA e o CSOC da CONTRATADA, haver dois tipos de conexões digitais de tipos distintos, sendo uma do tipo internet e outra do tipo MPLS do inglês Multi-Protocol Label Switching.

Ambos as conexões digitais devem ter velocidade de upload e download mínima de 50 (Cinquenta) Mbps, ser contratadas de operadoras e rotas distintas, e devem ser utilizadas única e exclusivamente para prestação do SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA da ANA.

Especificamente para o tipo de conexão digital internet, necessariamente precisará ter IP dedicado, e não serão aceitos contratos com links xDSL (executada a tecnologia HDSL).

Em qualquer que seja o tipo de conexão, será de responsabilidade e propriedade da CONTRATADA a contratação junto as devidas operadoras, bem como seus devidos custos durante todo período de vigência do contrato.

A fim de garantir a segurança do tráfego bidirecional entre a ANA e o CSOC da CONTRATADA, ambas as conexões (Internet e MPLS) devem ser criptografada. Ou seja, a CONTRATADA deverá estabelecer duas VPN`s do inglês Virtual private network, do tipo site to site.

Será de responsabilidade e propriedade da CONTRATADA os equipamentos e/ou soluções para estabelecer as VPN`s, exceto o firewall da ANA para estabelecimento dos links. Caberá a ANA apenas a disponibilidade de infraestrutura física no seu Data Center, infraestrutura física leia-se: energia elétrica, espaço no rack, climatização adequada, e sistemas de combate a incêndio. Tais equipamentos e/ou soluções devem possuir contratos de garantia junto ao seu respectivo fabricante, com suporte em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano.

A CONTRATADA deve assinar e entregar à ANA na data de reunião de início do contrato termo de confidencialidade e sigilo, conforme modelo contido no Anexo XX – Termo de Confidencialidade e Sigilo. Esse documento estabelece as condições para a prestação dos serviços acerca do sigilo das informações custodiadas, do acesso restrito das informações aos técnicos designados no projeto e da propriedade intelectual de todos os produtos e conhecimento advindos da execução.

Além disso, o termo de confidencialidade e sigilo deve ser reconhecido e assinado por todos os funcionários que venham executar serviços, diretamente ou indiretamente, no âmbito do contrato, sendo que a ANA pode solicitar, a qualquer momento, a comprovação dessa obrigação. O respectivo termo deve ser entregue antes do início das atividades.

Por outro lado, a CONTRATADA deve revogar todas as credenciais relacionadas a soluções de responsabilidade da CONTRATADA, empregadas na prestação de serviços a ANA, bem como solicitar a revogação destas à ANA, para soluções de responsabilidade da CONTRATADA, no mesmo dia do encerramento das atividades.

Tais exigências visam proteger a ANA contra o uso indevido de informações sob sua custódia por parte de profissional da CONTRATADA, assim como estão em conformidade com boas práticas de gestão e governança de TI.

CSOC - cyber security operations center,

Os SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA devem ser executados por meio de CSOC (Cyber Security Operation Center), não sendo necessário que seja próprio da contratada, porém deve obrigatoriamente posicionar-se no Brasil, diminuindo a chance de uma indisponibilidade afetar a prestação dos SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA.

O centro (CSOC) deve atender os seguintes requisitos mínimos, a saber:

- Utilizar sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas;
- Filmar toda a área, mantendo as imagens armazenadas pôr no mínimo 90 (noventa) dias;
- Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao CSOC;
- Possuir solução de monitoramento de disponibilidade e desempenho.
- Ser vigiado de forma ininterrupta por segurança física especializada em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- Funcionar em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e 365 (trezentos e sessenta e cinco) dias por ano;
- Possuir registro de entrada e saída de pessoas mantidos por pelo menos 90 dias.
- Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do contrato.
- Ser configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;
- Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;
- Não possuir campo físico visual externo das suas instalações, afim de garantir que as informações exibidas em monitores estejam inacessíveis a leituras e a capturas externas desautorizadas;
- Possuir ambiente dedicado único e exclusivamente para laboratório, onde seja possível reproduzir os incidentes e problemas da ANA, sem que haja impacto na operação do CSOC e/ou da própria ANA;

- Deverá possuir processos implementados que garantam a segurança das normas ABNT NBR ISO/IEC 27001. Tais processos deverão garantir controles rígidos e auditáveis de acesso físico e lógico as informações monitoramento;

O CSOC da CONTRATADA deverá possuir as características das certificações listadas na tabela abaixo. Tais características garante que a CONTRATADA segue os principais controles de segurança da informação, bem como também possui processos para tratamento de incidente e problemas bem estabelecidos, além de boa qualidade de atendimento e interface com o cliente.

item	Certificações
1	ABNT NBR ISO/IEC 27001
2	ABNT NBR ISO/IEC 20001

Mensuração,

O pagamento será feito mensalmente, levando-se em consideração o Nível Mínimo de Serviço (NMS) acordado em contrato, para o período de faturamento avaliado. O valor a ser pago será o valor unitário do item correspondente, alinhado com NMS acordado (vide item 9).

Logo de forma a viabilizar a análise da prestação dos serviços, a CONTRATADA deverá apresentar, através do seu portal de segurança descrito através do anexo III, informações acerca da aferição dos níveis de serviço contratados. Tais informações deverão estar agrupadas e obrigatoriamente deverão ter a disposição definida pela ANA.

A reunião mensal deverá ocorrer até o 5º (quinto) dia útil após o término do período de faturamento, que coincidirá com o mês legal, e a disponibilidade dos relatórios será condição necessária ao recebimento dos serviços pela ANA. O primeiro mês de faturamento será parcial, contado da data da emissão do termo de recebimento definitivo até o último dia do mês.

A respectiva nota fiscal/fatura, já deduzidos os abatimentos calculados, deverá ser emitida somente após o recebimento definitivo dos serviços e após a homologação das informações apresentadas pela CONTRATADA à ANA.

Caso não haja concordância, por parte da CONTRATADA, em relação aos abatimentos calculados, os mesmos serão convertidos em sanção, com aplicação de multa de mesmo valor, de forma a garantir o contraditório e a ampla defesa.

A qualquer tempo e a critério da ANA, a bases dos sistemas utilizados para cálculo das entregas e indicadores, podem ser solicitadas para auditorias e aferições.

E, finalmente, o pagamento dos SERVIÇOS TÉCNICOS ESPECIALIZADOS será feito após a ordem de serviço ser emitida e os serviços prestados de maneira satisfatória, conforme modelo de Termo de Recebimento de Serviços, respeitados os prazos definidos no item Serviços Técnicos Especializados. A nota fiscal/fatura relativa à prestação dos serviços, já considerado os abatimentos, deverá ser emitida somente após o recebimento dos serviços pela ANA.

Abrangência e escopo dos serviços,

Considerar-se-á, para efeitos desta contratação, todos os recursos necessários para sua efetiva prestação dos serviços.

O dimensionamento da equipe para execução adequada do serviço contratado é de responsabilidade exclusiva do Fornecedor de Serviço, devendo ser suficiente para o cumprimento integral dos níveis de serviço exigidos neste Termo de Referência.

Dependendo da complexidade, criticidade e do prazo do projeto os serviços poderão ser realizados nas instalações da CONTRATADA ou da ANA.

A CONTRATADA deverá ser capaz de atender os projetos de Serviços Continuados de Segurança Cibernética nas metodologias ITIL e NIST.

Todos os custos com licenças de simuladores, dispositivos físicos, hardware, software ou demais equipamentos devem estar contabilizados no valor do serviço, não sendo permitido o pagamento de valores adicionais ou extra.

Execução dos serviços,

A CONTRATADA deverá atender às seguintes condições gerais para início de prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente e ativação de serviços, sem ônus adicionais para a ANA:

- Serão de responsabilidade da CONTRATADA as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, excluindo-se a Solução de Segurança do Sistema ANA já ativa, em conformidade com o Projeto Executivo a ser elaborado e apresentado pela CONTRATADA para aprovação pela ANA;
- A CONTRATADA deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se pertinente, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;
- As visitas técnicas poderão ser realizadas nos dias úteis, das 08:30h às 17:30h, mediante agendamento prévio;
- Independentemente da alocação dos racks pela CONTRATADA, esta deverá efetuar a reorganização dos racks existentes, de forma a acomodar os seus equipamentos, quando necessário;
- A elaboração do Projeto Executivo estará a cargo da CONTRATADA e deverá conter as fases do projeto, os cronogramas de execução e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase, respeitando o prazo máximo total de 60 (sessenta) dias para a entrega de todos os serviços previstos, a contar da assinatura do contrato;

- Conter a descrição de topologia lógica e física da rede atual e topologia pretendida em cada etapa;
- Efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade da ANA;
- Projetar a engenharia de tráfego da Rede da ANA;
- Planejar a migração das configurações do parque atualmente em funcionamento;
- Para implantação dos serviços, indicar de forma detalhada as condições de rollback de cada mudança no ambiente do Sistema ANA;
- Estimar o consumo de unidades de rack em U's e de energia de cada ativo a ser instalado nas dependências da ANA.

Em relação a quaisquer equipamentos, softwares e demais componentes necessários à correta prestação dos serviços (e respectiva proposta de preços) deverão:

- Conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional do Sistema ANA, e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;
- Conter a última versão de software e firmware homologado pelo fabricante;
- Ter configuradas senhas de acesso para que a equipe de funcionários designados pela ANA efetue o acesso para a visualização das configurações e logs (acesso seguro e remoto);
- Ter configurada senha com direitos totais de administração e configuração a ser utilizada pela ANA em caso de emergência;
- Ser configurados para enviar logs para as soluções de concentração de logs disponibilizados no site da ANA.

Todos os recursos para implantação dos serviços providos pela CONTRATADA serão por ela providenciados, sem ônus para a ANA. Incluem-se, entre outros:

- Cabeamento de rede para interligação ao switch core da rede e demais ativos necessários ao funcionamento adequado da solução;
- Cabeamento de energia elétrica para alimentação dos equipamentos e respectivos adaptadores;
- Quaisquer materiais, cabos, parafusos, porcas, conectores elétricos, tomadas, adaptadores ou acessórios necessários ao cumprimento dos requisitos dos diversos serviços;

Para aprovação da instalação e configuração de qualquer item que enseje a emissão de termo de recebimento definitivo, a CONTRATADA deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;

As atividades quando realizadas no ambiente de produção poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 20h, ou em finais de semana e feriados), conforme disponibilidade da ANA;

A operação assistida deverá obedecer aos requisitos a seguir:

- Iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo;
- A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pela ANA que seja feita em data diferente; terá duração de 30 dias e será executada nas dependências da ANA, em horário comercial (8:30h às 17:30h);
- Caso seja necessária a consecução de atividades, pelo técnico responsável pela operação assistida, que possam afetar a disponibilidade de serviços de Rede da ANA, estas devem ocorrer após as 20:00h.

Caso a ANA encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;

Caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade nos sistemas da ANA, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação.

A CONTRATADA deverá implementar e documentar para todos os componentes da solução as configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (hardening), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de kernel, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários- padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.

Para o planejamento e o acompanhamento da instalação dos equipamentos e softwares necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do as- built, e para demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a CONTRATADA deverá alocar GERENTES DE PROJETOS que possuam qualificação Project Management Professional (PMP) e/ou, Prince2 Practitioner Certificate in Projetct Management, e/ou Professional Scrum Master I.

Solicitação Dos Serviços Técnicos,

- Os serviços serão solicitados via emissão de ordens de serviço (OS), mensais, registradas na ferramenta de acompanhamento da CONTRATANTE.
- A CONTRATANTE definirá o modelo da OS.

- A critério da CONTRATANTE o modelo de Ordem de Serviço poderá ser alterado para atender as necessidades do serviço, sem criar qualquer obrigação adicional à CONTRATADA, devendo, contudo, manter as informações mínimas necessárias para sua execução.
- Todas as OS deverão ser assinadas por ambas as partes.
- Havendo, por parte da CONTRATADA, alguma divergência na OS, desde que haja justificativa fundamentada, poderá a CONTRATANTE analisar e conduzir a solução das divergências e reapresentar a OS se for o caso.
- As OS poderão sofrer ajustes (decorrentes de situações supervenientes ocorridas na sua execução, que impliquem eventualmente na revisão de prazos, custos ou escopo), sempre formalizados por meio de Relatórios de Impacto (RI), assinados por ambas as partes, desde que não tenha sido dado o aceite definitivo nas respectivas entregas. A aceitação dos serviços é baseada na verificação dos entregáveis aferíveis preestabelecidos, conforme preconizado na Súmula TCU Nº 269 e no Acórdão Nº 916/2015 – Plenário – TCU. Este RI e os respectivos impactos nas OS deverão ser registrados na Ferramenta de Acompanhamento da CONTRATANTE.
- O pagamento das Ordens de Serviço será função não somente do escopo executado, mas também do alcance de níveis de serviço (INMS).
- A CONTRATADA deve indicar o preposto do contrato, que é o profissional que faz a comunicação formal entre CONTRATADA, equipe alocada na execução do contrato e a CONTRATANTE. O preposto deverá ser apresentado durante a reunião de kick off do contrato.
- As atividades de preposto da CONTRATADA não serão remuneradas diretamente pela CONTRATANTE.
- A CONTRATADA deve indicar o Gerente técnico do contrato, que é o perfil que facilita a comunicação entre a equipe alocada pela CONTRATADA para execução do objeto, o preposto do contrato e a equipe de gestão da CONTRATANTE. Este perfil deve ser desempenhado por um dos profissionais alocados na execução do objeto. O Gerente técnico do contrato deverá ser apresentado durante a reunião de kick off do contrato.
- A eventual suspensão ou cancelamento da OS pela CONTRATANTE implicará na remuneração proporcional de fases entregues e aceitas definitivamente até esse momento, nesta situação também é necessária a emissão e assinatura do respectivo relatório de impacto (RI).
- A execução das Ordens de Serviço pela Contratada ocorrerá de acordo com as condições, processos e atividades estabelecidos no Termo de Referência e anexos.
- A CONTRATANTE pode, contudo, a seu critério, na abertura da OS, estabelecer condições específicas de fornecimento respeitando os limites estabelecidos no Termo de Referência.

- A entrega dos artefatos e subprodutos da OS é realizada desde seu início até seu término, em consonância com as fases do processo e a produção dos produtos.
- A entrega em caráter provisório (aceite provisório) se dará por meio do registro eletrônico na ferramenta de acompanhamento da CONTRATANTE.
- A entrega em caráter definitivo (aceite definitivo) se dará por meio do registro eletrônico na ferramenta de acompanhamento da CONTRATANTE e seus respectivos artefatos (na forma definida pela CONTRATANTE) e da emissão e assinatura do Termo de Recebimento Definitivo (TRD) por ambas as partes.
- O modus operandi das reuniões relativas à metodologia sobre a execução do objeto serão definidas pela CONTRATANTE e repassadas formalmente à CONTRATADA, podendo sofrer ajustes durante a execução do objeto e vigência do contrato.
- A CONTRATANTE poderá, sempre que julgar necessário, com emissão do respectivo RI, promover o cancelamento da OS ou a alteração/atualização/supressão de escopo, alteração dos produtos a serem entregues e seus respectivos critérios de aceitação. Nessas situações, será feita avaliação de impacto estabelecendo, quando necessário, as novas condições de fornecimento.
- A CONTRATADA registrará as entregas dos produtos na Ferramenta de Acompanhamento da CONTRATANTE.
- A CONTRATADA entregará a documentações relativa à OS no sistema de controle da CONTRATANTE.
- O aceite definitivo dos serviços é emitido apenas após o atendimento das condições gerais e específicas dos serviços contratados, conforme estabelecido nesse Termo de Referência.
- A critério exclusivo da CONTRATANTE, uma OS poderá ser finalizada pela CONTRATADA com a entrega parcial dos serviços e/ou artefatos solicitados na OS.
- Relativo aos produtos entregues e para os quais foram emitidos TRD, a CONTRATADA deverá assegurar a GARANTIA dos mesmos contra defeitos e não conformidades, por um período de 12 (doze) meses contados a partir da data de assinatura do respectivo TRD. Esta garantia é válida mesmo após o final da vigência do contrato.
- A CONTRATANTE pode solicitar a substituição de qualquer dos profissionais alocados pela CONTRATADA na execução do objeto (inclusive preposto), bastando para isto a comunicação formal à CONTRATADA com antecedência mínima de 03 (três) dias.
- Considerando o disposto no art. 5º, V da IN SGD/ME nº 01/2019, todas as despesas com transporte, hospedagem e demais custos operacionais decorrentes do efetivo e adequado atendimento dos chamados e demais serviços envolvidos correrão por conta da Contratada.
- Após a assinatura do contrato e anterior ao início de suas atividades haverá uma reunião inicial entre a CONTRATANTE e CONTRATADA, denominada reunião de kickoff, nesta

reunião deverão estar presentes obrigatoriamente o preposto e o responsável técnico da CONTRATADA.

- Anterior ao término da atividades objeto do presente Edital, a CONTRATADA deverá providenciar juntamente com a CONTRATANTE e a empresa que vier a substitui-la, as atividades relativas à transição e repasse de conhecimento, de modo a garantir a continuidade das ações de suporte à infraestrutura.
- Ao término das atividades objeto do presente Edital, haverá uma reunião entre a CONTRATANTE e CONTRATADA, denominada reunião de encerramento.

Aceitação, critérios e métodos,

São esses os critérios básicos de aceitação dos serviços e métodos adotados para fins de pagamento:

- Conformidade com o nível mínimo de serviço ou SLA (Service Level Agreement): A contratada deve cumprir todas as condições estabelecidas no SLA, que define os níveis de serviço acordados entre as partes. Isso inclui o fornecimento das licenças dentro dos prazos estipulados, garantindo o acesso e a funcionalidade adequada dos softwares licenciados.
- Qualidade dos serviços: As licenças fornecidas devem estar livres de defeitos e serem totalmente funcionais, atendendo às especificações e requisitos definidos no edital e no contrato. Qualquer falha na qualidade das licenças entregues pode resultar em glosas no pagamento correspondente.
- Termo de Recebimento Provisório: Antes do pagamento das notas fiscais, será exigido o Termo de Recebimento Provisório, que é emitido pela contratante para atestar que as licenças foram entregues e estão disponíveis para uso. Esse termo pode ser emitido após a verificação preliminar da conformidade das licenças com as especificações técnicas estabelecidas.
- Termo de Recebimento Definitivo: O Termo de Recebimento Definitivo é emitido após a verificação completa e final das licenças, incluindo testes de funcionamento e conformidade com as especificações técnicas. Somente após a emissão desse termo, as notas fiscais serão consideradas para pagamento. Caso sejam identificadas não conformidades durante a verificação final, poderão ser aplicadas glosas correspondentes às licenças afetadas.
- Relatórios de Não Conformidades: A contratada deve fornecer relatórios detalhados sobre quaisquer não conformidades encontradas durante o processo de verificação das licenças. Esses relatórios devem descrever as falhas identificadas, suas causas e ações corretivas implementadas para resolver os problemas. A contratada deve ser responsável por corrigir as não conformidades dentro dos prazos estipulados.
- Cumprimento das obrigações contratuais: Além dos critérios específicos relacionados às licenças, a contratada também deve cumprir todas as obrigações estabelecidas no contrato, incluindo prazos, documentação, suporte técnico e quaisquer outras cláusulas contratuais pertinentes.

É importante ressaltar que eventuais glosas resultantes do não atendimento aos critérios acima devem ser comunicadas à contratada de forma clara e documentada, permitindo

a oportunidade de resposta e correção das não conformidades. A administração pública buscará sempre o diálogo e a resolução amigável dos problemas identificados, priorizando a qualidade e a conformidade dos serviços prestados.

Dos prazos de execução das ordens de serviço,

Os prazos para execução dos serviços são os definidos na OS.

Ambiente tecnológico da Ana (hardware e software),

Na elaboração de suas propostas, as licitantes devem levar em consideração que a ANA possui o seguinte parque tecnológico:

O Ambiente Tecnológico da ANA, composto de hardware e software, pode sofrer alterações antes da ocorrência da licitação dos serviços de segurança e depois da assinatura do contrato para a execução desses serviços. Sendo assim, sugerimos que as empresas agendem uma visita técnica para a verificação do ambiente.

Componente	Tecnologias Envolvidas	Quantidade	Ambiente Mais Crítico	Ambiente Menos Crítico
Usuários da TI com acesso privilegiado (admin segurança / rede / Root / DomainAdmin / Dbadmin / SysDBA, Vmadmin, Desenvolvedores, outros)	Não aplica	47 (Domain Admin)		
Servidores Windows: (físico e virtual)	Windows Server 2003 a 2022	106		
Servidores Linux/Unix: (físico e virtual)	CentOS versões 7 e 8, Red Hat Enterprise, Linux 7 e 8, Linux Fedora, Ubuntu, Oracle Linux, Free BSD, Debian Suse	94		
Estações de trabalho Windows:	Versões Windows 10	910		
Domain Controllers (AD ou LDAP?):	AD/LDAP	3 – AD	2	1
Switches, roteadores, appliance de segurança, storage, etc:	Switches	93 switches	83 switches	10 switches

	Storages (Pure Storage, NetApp e Hitachi(2))	4 storages	4 storages	
	Solução IPS Palo Alto	2 IPS	2 IPS	
	Firewall Palo Alto	2 Firewall	2 Firewall	
	FW Pfsense	107 aps	107 aps	
	AccessPoints			
Serviços em qual nuvem:	AWS e Oracle Exadata CC	Aws 2	AWS 1	AWS 1
		Oracle 2	Oracle 1	Oracle 1
Aplicações com credenciais hard-Coded:	ASP			
Banco de dados:	- Oracle	- 4 Ambientes Oracle	- 2 Amb. Oracle	- 3 Amb. Oracle
	- PostgreSQL	- 4 Instâncias PostgreSQL	- 2 Inst. PostgreSQL	- 2 Inst. PostgreSQL
	- MariaDB (MySQL)	- 13 Instâncias SQL Server	- 8 Inst. SQL Server	- 5 Inst. SQL Server
	- SQL Server			
	- MongoDB			
Total de CPU dos servidores de aplicação:	1.045			
Total de CPU dos servidores de BD:	- Oracle	- Oracle 8	- 4 Oracle	- 4 Oracle
	- PostgreSQL	- PostgreSQL - 12	- 8 PostgreSQL	- 4 PostgreSQL
	- SQL Server	- SQL Server - 36	- 30 SQL Server	- 6 SQL Server
Total de memória servidores aplicação:	2.6T			

Total de memória servidores de BD:	- Oracle	- Oracle – 2 TB	- Oracle – 1 TB	- Oracle – 1 TB
	- PostgreSQL	- PostgreSQL – 40 Gb	- PostgreSQL – 32 Gb	- PostgreSQL – 8 Gb
	- SQL Server	- SQL Server - 842Gb	- SQL Server – 632 Gb	- SQL Server – 210 Gb
Servidores docker:	Docker	3		
Cluster kubernetes (Openshift ou Kubernetes):	OKD 4.9	20 Nós		
Aplicações:	Java, Javascript, ASP, PHP, Python, Ruby on rails, Apex, Delphi, Jboss, Wildfly, Tomcat, IIS, Nginx, Apache, Phusion Passenger, Zope, OKD			
Solução de Balanceamento de Carga;	Nginx			
	HAProxy			
Solução de Mail Gateway;	Office 365			
Solução de Endpoint Security;	Defender Microsoft			

Solução de DNS (Open source ou proprietário) ;	MaraDns – Open Source			
Solução de SMTP (Open source ou proprietário) ;	Microsoft Exchenge			
Solução AD/DNS/DHCP;	Microsoft AD/DNS/DHCP			
Solução de 2º Fator de Autenticação	Microsoft AD			
Link de Internet;	1			
Access Point;	107 Huawei			

ANEXO III – NÍVEIS mínimos DE SERVIÇO (NMS/SLA)

A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS ou SLA) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

Os níveis mínimos de serviço contratados serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar os pagamentos previstos.

De modo a facilitar a compreensão dos Níveis Mínimos de Serviço (NMS) dos SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA, são apresentados, a seguir, exigências mínimas em termos de níveis de serviço que devem ser atendidas pela CONTRATADA na execução do contrato, a saber:

Disponibilidade mensal dos grupos de tecnologias,

Para os itens 2 a 7 dos SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA, a Meta de Disponibilidade Mensal (MDM) por grupo de tecnologia deve ser de, no mínimo 95% (noventa e cinco porcento).

Em cada período avaliado, o cálculo do Percentual de Disponibilidade Mensal (PDM) por item de serviço deve ser calculado com a seguinte fórmula:

$$\mathbf{PDM_k = [(TM - TI_k)/100] * 100}$$

- $\mathbf{PDM_k}$ = Percentual de Disponibilidade Mensal do k-ésimo item de serviço;
- **k** = k-ésimo item de serviço;
- **TM** = Tempo total mensal de operação, em minutos, no mês de faturamento;
- $\mathbf{TI_k}$ = Tempo total mensal de indisponibilidade do k-ésimo item de serviço, em minutos, no mês de faturamento.

Devem ser incluídos como Tempo de Indisponibilidade ($\mathbf{TI_k}$):

- Tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;
- Tempo decorrente entre o início da indisponibilidade do serviço e a sua total recuperação;

Não devem ser incluídos como Tempo de Indisponibilidade ($\mathbf{TI_k}$):

- Falta de energia no local de prestação dos serviços;
- Indisponibilidade da rede logicada ANA;
- Problemas derivados de ocorrências no ambiente da ANA, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;
- Ações necessárias para resolução de problemas que tenham sido autorizadas pela ANA;

- Indisponibilidade gerada pela operadora de telecomunicação responsável pelos links e equipamentos da Rede ANA;
- Indisponibilidade gerada pela necessidade de reparo ou troca dos equipamentos da solução de segurança da informação da rede ANA, listadas do tópico Ambiente Tecnológico da ANA do presente termo de referência;
- Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança da ANA;
- Indisponibilidade do ambiente virtualizado ANA, infraestrutura computacional em que parte dos softwares que compõem a solução deve ser instalada;
- Manutenções programadas pela ANA;
- Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pela ANA

Os chamados ou tickets abertos cujo prazo de resolução encerre somente no próximo período de faturamento somente terão calculados os fatores de abatimento a partir do período seguinte;

Entrega mensal dos serviços continuados de segurança cibernética,

Além da meta de disponibilidade mensal do parque de segurança da informação, deverão também ser apurados os níveis de serviço para os demais serviços que somados compõem o objeto SERVIÇOS CONTINUADOS DE SEGURANÇA CIBERNÉTICA.

A avaliação da qualidade dos serviços prestados ocorrerá através do acompanhamento e avaliação dos atendimentos aos chamados junto com a qualidade da prestação dos serviços continuados de segurança e a execução das ordens dos serviços técnicos evolutivos, seguindo os termos contratuais definidos no Termo de Referência.

Métricas e Convenções,

Na execução do objeto se aplicam as seguintes métricas e convenções:

- Horas expressas no formato “horas:minutos” indicam um relógio de 24 horas no fuso horário oficial Brasileiro (Brasília – GMT 03:00);
- Horas indicadas como “horas úteis” incluem as horas de 08:00 às 18:00;
- Dias indicados como “dias úteis” incluem “horas úteis”, de segunda a sexta-feira, exceto os feriados oficiais nacionais e locais;
- Reunião de Acompanhamento de Serviços: Reunião com a ANA Deverá ser emitida uma nota pela CONTRADATA referente aos serviços prestados no mês de referência;
- Relatório de Resultados de Monitoramento: Documento que contém informações técnicas detalhadas referentes ao monitoramento dos ativos de Segurança contratados;
- Armazenamento de Logs: Os logs referentes aos ativos monitorados, das soluções de Segurança Gerenciadas, serão armazenados;
- Triagem de incidentes de segurança: Triagem de incidentes de segurança para redução de falsos positivos realizando o escalonamento para a fila adequada;
- Incidentes de gravidade (Alta, Média ou Baixa): Classificação do nível de gravidade do incidente detectado/ocorrido;

- Análise de Vulnerabilidades dos Ativos de Segurança Contratados: é realizado scan e análise de vulnerabilidades em ativos de segurança contratados, visando manter um maior nível de segurança nos mesmos;
- Requisição de Mudança para aplicação de patches e hotfixes de segurança: Após serem lançados novos patches e hotfixes, a CONTRATADA, de acordo com o SLA acordado, iniciará o processo de construção da requisição de mudança para correções / atualizações nos ativos de segurança contratados;
- Atualização de assinaturas (vacinas, bases de vulnerabilidades, etc.) servidores/appliances e agentes de distribuição (caso de Endpoint Protection): Quando forem disponibilizadas novas atualizações de assinaturas será realizada a migração nos dispositivos de segurança contratados;
- Tratamento de Solicitações: Será realizado atendimento de chamados de solicitações da ANA ;
- SLA – Service Level Agreement: Níveis mínimos de prestação dos serviços requeridos pela ANA.

Níveis mínimos de serviços (MNS/SLA),

Informamos que, em conformidade com o edital, os seguintes níveis mínimos de serviço serão aplicados ao objeto do contrato:

Nível de Serviços para o Monitoramento de Segurança

ATIVIDADE	SLA DE ATENDIMENTO
Triagem de Incidentes de segurança	30 min
Resposta da Incidentes de gravidade alta	Início em 15 min
Resposta da Incidentes de gravidade média	Início em 30 min
Resposta da Incidentes de gravidade baixa	Início em 45 min

Nível de Serviços para o Gerenciamento de Segurança

ATIVIDADE	SLA DE ATENDIMENTO
Requisição de mudança para aplicação de patches e hotfixes de segurança	6 dias
Atualização de assinaturas (vacinas de vírus, bases de vulnerabilidades, etc.)	8 horas
Tratamento de Solicitações	1 hora

Um acordo de nível de serviço define os índices a serem atingidos para o cumprimento do

conjunto de compromissos acordados entre ANA e CONTRATADA. Tais índices serão medidos e aplicados aos serviços contratados pela ANA e prestados pela CONTRATADA;

Mensalmente os dados de Nível de Serviço deverão ser apresentados à ANA, incluindo informações sobre ações e necessidades para a correção de desvios, visando atingir, manter e melhorar os níveis desejados.

A abrangência e o nível de detalhamento dos demonstrativos serão definidos conforme as necessidades identificadas pela CONTRATADA, podendo sofrer alterações ao longo do tempo, as quais serão encaminhadas à ANA via os processos de Gerenciamento do Nível de Serviço e de Mudanças do mesmo.

Para a medição dos índices de nível de serviços, serão considerados os seguintes conceitos:

- Requisição: solicitação da ANA para intervenção preventiva ou corretiva no ambiente gerenciado e previsto no escopo desta proposta. Cada requisição será identificada unicamente por meio de um código e será classificada conforme seu nível de severidade no momento da sua comunicação a CONTRATADA;
- Incidente: É uma interrupção não planejada de um serviço de TI ou uma redução de qualidade de um serviço de TI;
- Problema: é a causa desconhecida de um ou mais incidentes ou os problemas são a causa de um ou mais incidentes;
- Severidade: nível de prioridade/emergência atribuído ou solicitado para a realização de um atendimento a uma requisição da ANA ou do ambiente, conforme critérios descritos a seguir. Solicitações de alteração do nível de severidade poderão ser submetidas à CONTRATADA e, quando julgadas pertinentes pela mesma, serão prontamente atendidas.
    - SEVERIDADE CRÍTICO: A Solução está totalmente parada ou inoperante;
    - SEVERIDADE ALTO: A Solução está ativa, mas com inoperância da maioria de suas funcionalidades, causando um impacto negativo no ambiente de produção;
    - SEVERIDADE MÉDIO: A Solução está operativa, mas suas funcionalidades são executadas com restrições;
    - SEVERIDADE BAIXO: A Solução está operativa e a falha não compromete suas funcionalidades ou questões não tratadas pela documentação;
    - SEVERIDADE AGENDADO: O atendimento está relacionado apenas a esclarecimentos de dúvidas ou necessidade de informações;

A cada chamado de suporte categorizado como Severidade Crítico ou Alto, o recurso humano designado para fornecer assistência deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante.

Referente aos chamados categorizados como Severidade Crítico ou Alto cabe ao fornecedor dar início, junto à ANA às providências que serão adotadas para a solução do chamado.

Para os chamados de suporte categorizado como Severidade Crítico ou Alto, o atendimento não

pode ser interrompido até o completo restabelecimento de todas as funções do sistema paralisado (indisponível), mesmo que para isso tenham que se estender por períodos noturnos e dias não úteis (sábados, domingos e feriados), de acordo com a disponibilidade da ANA.

Severidade	Descrição
Agendado	Esclarecimento de dúvidas ou similar.
Baixo	Sistemas operam sem impacto ao negócio.
Médio	Sistemas operam com degradação de desempenho.
Alto	Sistemas operam com paralisação parcial do ambiente.
Crítico	Sistemas inoperantes ou paralisação total do ambiente.

Tempo de Notificação: O tempo máximo para a NOTIFICAÇÃO da **ANA**, conforme a severidade do incidente o problema.

Tempo máximo para notificação de eventos: 10 minutos

Tempo de Atendimento: O tempo máximo para INÍCIO de um ATENDIMENTO a uma requisição, incidente ou problema.

Severidade	Descrição
Agendado	Esclarecimento de dúvidas ou similar – 8 hs.
Baixo	Sistemas operam sem impacto ao negócio – 4 hs.
Médio	Sistemas operam com degradação de desempenho – 40 min.
Alto	Sistemas operam com paralisação parcial do ambiente – 20 min.
Crítico	Sistemas inoperantes ou paralisação total do ambiente – 10 min.

Tempo de Solução: O tempo máximo para a SOLUÇÃO de um ATENDIMENTO a uma requisição, incidente ou problema. O tempo de solução poderá depender de fatores externos que deverão ser levados em conta durante a sua medição.

Severidade	Descrição
Baixo	Sistemas operam sem impacto ao negócio – 2 dias.
Médio	Sistemas operam com degradação de desempenho – 24 hs.
Alto	Sistemas operam com paralisação parcial do ambiente – 12 hs.
Crítico	Sistemas inoperantes ou paralisação total do ambiente – 6 hs.

Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas

cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.

Os chamados escalados para o fabricante e em tratamento por aquele não se encaixam nos prazos descritos.

Serão excluídos do cálculo, os tempos de paralisação, decorrentes dos seguintes eventos:

- Falta de energia no local de prestação dos serviços;
- Indisponibilidade da rede lógica da ANA;
- Problemas derivados de ocorrências no ambiente da ANA, onde comprovadamente a indisponibilidade não esteja sendo controlada pela CONTRATADA;
- Ações necessárias para resolução de problemas que tenham sido autorizadas pela ANA;
- Indisponibilidade gerada pela operadora de telecomunicação responsável pelos links e equipamentos da Rede ANA;
- Indisponibilidade gerada pela necessidade de reparo ou troca dos equipamentos da solução de segurança da informação da rede ANA, listadas do tópico AMBIENTE TECNOLÓGICO DA ANA (Hardware e Software) do presente termo de referência;
- Fatores externos a prestação de serviços, desde que justificado e acordado com o time de segurança da ANA;
- Indisponibilidade do ambiente virtualizado da ANA, infraestrutura computacional em que parte dos softwares que compõe a solução devem ser instalados;
- Manutenções programadas pela ANA;
- Manutenções programadas pela CONTRATADA, desde que previamente autorizadas pela ANA.

Em um atendimento onde seja necessária uma janela para execução dos serviços solicitados, os tempos entre a necessidade do atendimento e janela de execução deverão ser excluídos.

Entende-se que haverá uma fase inicial de transição e adequação dos processos de atendimento por parte da CONTRATADA. Sendo assim, os níveis de serviço (SLAs) não serão exigidos contratualmente durante os primeiros 60 (sessenta) dias de duração do contrato. Os índices deverão ser apurados e apresentados ao Inep, no entanto, a CONTRATADA não estará sujeita a penalidades pelo seu descumprimento durante este período.

ANEXO III – REQUISITOS DAS FERRAMENTAS USADAS NA EXECUÇÃO DO OBJETO

1. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE GESTÃO DE VULNERABILIDADES

Requisitos da ferramenta para ambientes crítico:

+++ Deve possibilitar, por meio da console, no mínimo 01 (um) método de escaneamento:

--------> Scan ativo;

--------> Scan com uso de agentes;

--------> Scan passivo;

+++ A solução deve possuir um sistema próprio de pontuação e priorização das vulnerabilidades diferentes do padrão CVSS;

+++ Deve possuir mecanismo de priorização dinâmico baseado em algoritmos de inteligência artificial;

+++ O Algoritmo de priorização deve considerar vulnerabilidades distintas para realizar o cálculo do score da vulnerabilidade;

+++ Toda vulnerabilidade que possuir um CVE associado deve receber uma nota dinâmica da solução de gestão de vulnerabilidades;

+++ A solução deve ser capaz de aplicar algoritmos de inteligência artificial (Machine learning) para analisar fontes de dados relacionadas a vulnerabilidades;

+++ O sistema de pontuação e priorização de vulnerabilidades deve avaliar, no mínimo, as seguintes características:

--------> CVSSv3 Impact Score;

--------> Idade da Vulnerabilidade;

--------> Se existe ameaça ou exploit que explore a vulnerabilidade;

--------> Número de produtos afetados pela vulnerabilidade;

--------> Intensidade baseada no Número e Frequência de ameaças que utilizaram a vulnerabilidade ao longo do tempo;

--------> Lista de todas as fontes (canais de mídia social, dark web etc.) em que ocorreram eventos de ameaças, relacionados a vulnerabilidade;

+++ A solução de gestão de vulnerabilidades deve suportar análise de vulnerabilidades de ambientes industriais (Tecnologias de Automação);

+++ Deve possuir uma API abrangente para automação de processos e integração com aplicações terceiras;

+++ Deve ser capaz de fazer a correlação em tempo real de ameaças ativas contra suas vulnerabilidades, incluindo feeds de inteligência de ameaças ao vivo;

+++ A solução deve permitir a instalação de agentes em estações de trabalho e servidores, para varredura diretamente no sistema operacional;

+++ A solução deve possuir conectores para a seguintes plataformas:

--------> Amazon Web Service (AWS);

--------> Microsoft Azure;

--------> Google Cloud Platform;

--------> Qualys Assets;

+++ A solução deve ser capaz de produzir relatórios nos seguintes formatos: PDF, CSV e HTML;

+++ A solução deve ser capaz de identificar novos hosts no ambiente, sem a necessidade de um scan;

+++ A solução deve possuir recurso de monitoria passiva do tráfego de rede para identificação de anomalias, novos dispositivos e desvios de padrões observados;

+++ A solução deve possibilitar, no mínimo 50 (cinquenta) scanners ativos;

+++ A solução deve possibilitar, no mínimo, 20 (vinte) sensores passivos de rede para realizar o monitoramento em tempo real do ambiente;

+++ Deve ser possível determinar em tempo real, quais portas estão abertas em determinado ativo;

+++ Deve ser capaz de guardar, no mínimo, os seguintes atributos de um ativo:

--------> BIOS UUID;

--------> MAC Address;

--------> Nome NetBIOS:

--------> FQDN;

+++ A solução deve ser capaz de realizar - em tempo real - a descoberta de novos ativos para, no mínimo:

--------> Bancos de dados;

--------> Hypervisors;

--------> Dispositivos móveis;

--------> Dispositivos de rede;

--------> Endpoints;

--------> Aplicações;

+++ Deve realizar - em tempo real - a identificação de informações sensíveis no tráfego de rede do ambiente;

+++ A solução deve ser capaz de identificar a comunicação de malwares na rede, de forma passiva;

+++ Deve ter a capacidade de guardar - em tempo real - informações de GET, POST e Download que trafeguem na rede;

+++ A solução deve ser capaz de - em tempo real - detectar logins e downloads de arquivos em um compartilhamento de rede sem a necessidade de um agente;

+++ Permitir identificar vulnerabilidades associadas aos servidores SQL no tráfego de rede - em tempo real - sem a necessidade de um agente;

+++ A solução deve realizar varreduras em uma variedade de sistemas operacionais, incluindo, no mínimo, Windows, Linux e Mac OS, bem como appliances virtuais;

+++ A solução deve suportar vários mecanismos de varredura distribuídos em diferentes localidades e regiões, e gerenciar todos por uma console central;

+++ A solução deve fornecer agentes instaláveis em sistemas operacionais distintos para monitoramento contínuo de configurações e vulnerabilidades;

+++ A solução deve incluir a capacidade de programar períodos de tempo e data onde varreduras não podem ser executadas, como, por exemplo, em determinados dias do mês ou determinados horários do dia;

+++ No caso em que uma atividade de varredura for interrompida por invadir o período não permitido, a mesma deve ser capaz de ser reiniciada de onde parou;

+++ A solução deve ser configurável para permitir a otimização das configurações de varredura;

+++ A solução deve permitir a entrada e o armazenamento seguro de credenciais do usuário, incluindo contas locais, de domínio (LDAP e Active Directory) e root para sistemas Linux;

+++ A solução deve fornecer a capacidade de escalar privilégios nos destinos, do acesso de usuário padrão até o acesso de sistema ou administrativo;

+++ A solução deve ser capaz de realizar pesquisas de dados confidenciais;

+++ A solução deve gerar um score que combine dados de vulnerabilidades com a criticidade dos ativos do ambiente computacional;

+++ O score deve ser gerado - automaticamente - por meio de algoritmos de inteligência artificial (Machine Learning), e deve calcular a probabilidade de exploração de uma determinada vulnerabilidade nos servidores;

+++ Deve ser capaz de calcular a criticidade dos ativos da organização;

+++ A solução deve ser capaz de realizar um benchmark no ambiente da ANA, comparando sua maturidade com outras organizações do mesmo setor;

+++ Deve fornecer uma lista com as principais recomendações para o ambiente com foco na redução da exposição cibernética da organização;

+++ A solução deve gerar uma pontuação para cada um dos ativos onde é levado em conta as vulnerabilidades presentes naquele ativo assim como a classificação do ativo na rede (peso do ativo).

+++ A solução deve gerar uma pontuação global referente a exposição cibernética da organização, baseada nas pontuações de cada um dos ativos.

+++ A solução deve oferecer uma capacidade de comparação (benchmarking) da pontuação referente a exposição cibernética com outros players da mesma indústria, assim como outras empresas do mercado.

+++ A solução deve permitir um acompanhamento histórico do nível de exposição da organização;

+++ Permitir realizar alterações na classificação dos ativos (atribuição de pesos diferentes) podendo sobrescrever a classificação atribuída automaticamente pela solução.

+++ A solução deve permitir a segregação lógica entre áreas distintas da empresa, a fim de obter a pontuação referente a exposição cibernética por área.

+++ Deve ser capaz de executar relatórios manuais e periódicos de acordo com a frequência estabelecida pelo administrador;

+++ A solução deve possibilitar a criação de relatórios baseado nos seguintes alvos: Todos os ativos e Alvos específicos;

+++ Deve suportar a criação de relatórios criptografados (protegidos por senha configurável);

+++ A solução deve suportar o envio automático de relatórios para destinatários específicos;

+++ Deve ser possível definir a frequência na geração dos relatórios para, no mínimo: Diário, Semanal, Mensal e Anual;

+++ Permitir especificar níveis de permissão nos relatórios para usuários e grupos específicos;

+++ A solução deve possuir relatórios pré-configurados com as seguintes informações:

--------> Hosts verificados sem credenciais;

--------> Top 100 Vulnerabilidades mais críticas;

--------> Top 10 Hosts infectados por Malwares;

--------> Hosts exploráveis por Malwares;

--------> Total de vulnerabilidades que podem ser exploradas pelo Metasploit;

--------> Vulnerabilidades críticas e exploráveis;

--------> Máquinas com vulnerabilidades que podem ser exploradas;

--------> Relatórios contendo scans credenciados que tiveram erro ou falha;

+++ A solução deve possuir dashboards customizáveis onde o administrador pode deletar, editar ou criar painéis de acordo com a necessidade;

+++ Deve possuir dashboard apresentando visão das vulnerabilidades discriminadas por sua criticidade e idade;

+++ A solução deve criptografar todas as informações em trânsito;

+++ Deve utilizar, no mínimo, chave AES-256 para criptografar os dados armazenados;

+++ A solução deve ser capaz de gerar uma chave randômica com no mínimo 256 bits para cada scanner conectado na plataforma de gerência;

+++ Todos os dados enviados para a plataforma de gerenciamento devem ser criptografados - no mínimo - com protocolo TLS 1.3, com tamanho de chave de 4096 bits;

+++ Dados indexados devem possuir - no mínimo - criptografia utilizando algoritmo AES-256;

+++ A plataforma deve ser capaz de gerar uma chave randômica de no mínimo 128 bits para qualquer "Job" gerado;

+++ A solução deve possuir no mínimo as seguintes certificações de privacidade e segurança:

--------> EU-U.S. Privacy Shield Framework.

+++ A solução deve possuir ferramentas e processos automatizados para monitorar: Uptime, Comportamentos anômalos e performance da plataforma;

+++ Deve possuir retenção na nuvem de - no mínimo - 12 meses dos resultados dos scans realizados no ambiente;

+++ A solução deve realizar varreduras de vulnerabilidades em aplicações Web, cobrindo, no mínimo, mas não se limitando, a base de ameaças apontadas pelo OWASP Top 10;

+++ A solução deve ser capaz de analisar, testar e reportar falhas de segurança em aplicações Web, como parte dos ativos a serem inspecionados;

+++ A solução deverá ser capaz de executar varreduras em sistemas web através de seus endereços IP ou FQDN (DNS);

+++ Deverá avaliar - no mínimo - os padrões de segurança OWASP Top 10;

+++ Para varreduras extensas e detalhadas, deve varrer e auditar - no mínimo - os seguintes elementos:

--------> Cookies, Headers, Formularios e Links;

--------> Nomes e valores de parâmetros da aplicação;

--------> Elementos JSON e XML;

--------> Elementos DOM;

+++ Deverá também permitir somente a execução da função crawler, que consiste na navegação para descoberta das URLs existentes na aplicação;

+++ Deve ser capaz de utilizar scripts customizados de crawl, com parâmetros definidos pelo usuário;

+++ Deve ser capaz de excluir determinadas URLs da varredura, através de expressões regulares;

+++ Deve ser capaz de excluir determinados tipos de arquivos através de suas extensões;

+++ Deve ser capaz de instituir - no mínimo - os seguintes limites:

--------> Número máximo de URLs para crawl e navegação;

--------> Número máximo de diretórios para varreduras;

--------> Número máximo de elementos DOM;

--------> Tamanho máximo de respostas;

--------> Tempo máximo para a varredura;

--------> Número máximo de conexões HTTP ao servidor hospedando a aplicação Web;

--------> Número máximo de requisições HTTP por segundo;

--------> Autenticação Básica (Digest);

--------> NTLM;

--------> Autenticação de Cookies;

--------> Autenticação através de Selenium;

+++ Deve ser capaz de importar scripts de autenticação Selenium previamente configurados pelo usuário;

+++ Deve ser capaz de customizar parâmetros Selenium como: delay de exibição da página, delay de execução de comandos e delay de comandos para recepção de novos comandos;

+++ A solução deve ser capaz de exibir os resultados das varreduras de forma temporal para acompanhamento de correções e introdução de novas vulnerabilidades;

+++ Os resultados devem ser apresentados agregados por vulnerabilidades ou por aplicações;

+++ Para cada vulnerabilidade encontrada, deve ser exibido detalhes e evidências;

+++ Cada vulnerabilidade encontrada deve conter também soluções propostas para mitigação ou remediação;

+++ A solução deve ser capaz de realizar varreduras nos seguintes componentes:

--------> Red Hat JBoss, AngularJS, Apache, Apache Tomcat;

--------> Backbone.js, ASP.NET, Bootstrap, Drupal, Joomla, jQuery, Lighttpd, Magento, Modernizr, Nginx, PHP, AJAX, Sitefinity, Telerik,ThinkPHP, Webmin, Nodejs, Javascript, Java e YUI

+++ O hardware necessário para instalação e configuração do ferramental será fornecido pela infraestrutura da ANA;

Requisitos da ferramenta para ambientes não crítico:

+++ Deve possuir personalização de relatórios classificados por vulnerabilidade ou host;

+++ Os relatórios devem ser exportados pelo menos em HTML, CSV ou PDF;

+++ Deve ser capaz de enviar notificações de resultados de varredura por e-mail;

+++ A solução deve prover a descoberta e varredura de ativos:

--------> Varreduras incluindo redes IPv4 / IPv6 / FQDN;

--------> Varreduras em busca de vulnerabilidades sem utilização de credenciais;

--------> Varreduras utilizando credenciais e verificação de patches;

--------> Varreduras de sistemas operacionais, dispositivos de rede, hypervisors, base dados, servidores web;

+++ Deve possuir trilha de auditoria;

+++ Suportar hypervisors pelo menos, Red Hat Enterprise Virtualization (RHEV), VMware, além de outros;

+++ Deve ser compatível com os sistemas Operacionais: Windows 7 SP1, 8.1 e 10, Windows Server 2003/2008 R2 ou superior, Linux Debian 9 e 10 Red Hat ES 6,7 e 8, no mínimo;

+++ A varredura por credenciais deve ser suportada nas seguintes bases de dados: Oracle, SQL Server, MySQL, PostgreSQL;

+++ Deve possuir varredura de conformidade personalizada para Windows e Unix,

+++ Possuir suporte a detecção de vírus, malwares botnets, processos conhecidos e desconhecidos;

+++ A solução deve auditar o agente do antivírus instalados, informando se está mal configurado e estão com regras desatualizadas;

+++ Auditoria de configuração baseada no mínimo em critérios do CIS, mas não limitada a outros entes como: CERT, COBIT/ITIL, DISASTIGs, FDCC, ISO, NIST, NSA, PCI;

+++ Possui suporte a configuração de políticas e templates;

+++ A solução deve conter pontuação de risco: ranking de vulnerabilidade baseado em CVSS, cinco níveis (crítico, alto, médio, baixo, informações), níveis de gravidade personalizáveis para reformulação de riscos;

+++ Possuir escaneamento de quantidade de IPs de destino/dispositivos alvo ilimitados;

+++ O Gerenciamento deverá ser realizado por interface web;

+++ A solução deve possuir agendamento de escaneamento possibilitando definir subnets ou IP's alvo específicos;

+++ A solução deve apresentar formas de resolução ou mitigação das vulnerabilidades, detalhando atualizações e configurações necessárias para eliminar ou, não sendo possível, para reduzir a exposição ao risco;

+++ Deve fornecer o acesso a templates (modelos de configuração pré-determinados) de escaneamento para identificação de vulnerabilidades específicas (por exemplo, o ransomware WannaCry e suas variantes);

+++ Identificadores CVE (Common Vulnerabilities and Exposures) associados as vulnerabilidades identificadas para geração de relatórios, gerenciamento de riscos e mitigação de ameaças;

+++ Identificação de vulnerabilidades de aplicação, tais como: Cross-SiteScripting, SQL Injection e outros;

+++ Manutenção do histórico de escaneamentos anteriores.

2. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE GESTÃO DE SEGURANÇA PARA INFRAESTRUTURA E SISTEMAS CRÍTICOS

Requisitos da ferramenta de gestão de dispositivos e ambientes:

+++ Características Gerais da solução:

--------> A solução deve apoiar, no mínimo, os requisitos (artigos 6, 42, 43, 46, 48 e 50) da Lei Geral de Proteção de Dados-LGPD, como: Determinar como os dados deverão ser tratados, mantidos e protegidos e a quem responsabilizar em caso de descumprimento; Proteger o acesso a dados pessoais sensíveis; Responsabilizar pessoal e responder a incidentes; Aplicar boas práticas de governança, através de regras que deverão respeitar os preceitos da lei, de maneira a mitigar os riscos inerentes ao tratamento de dados e implementar e demonstrar a efetividade das políticas de segurança relacionadas ao tratamento de dados.

--------> Apoiando os requisitos da LGPD a solução deverá proteger e monitorar acessos a dados pessoais sensíveis por meio da segurança de credenciais e acessos de alto privilégio em serviços críticos, detectando e respondendo rapidamente a incidentes de segurança, identificando e mitigando ações privilegiadas com comportamentos de alto risco, avaliando riscos e testando a efetividade dos processos de proteção de dados por meio de relatórios da solução com identificação e classificação do status de risco do ambiente privilegiado, demonstrando conformidade e prova de que os controles de segurança necessários estão nos lugares certos, provendo análise comportamental, auditoria e segurança dos acessos a sistemas por meio de todas credenciais administrativas de alto privilégio em dispositivos e sistemas-alvo diversos do ambiente.

--------> Um sistema-alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser protegidas e gerenciadas pela solução;

--------> Um usuário da solução é definido como qualquer pessoa que acesse um sistema-alvo mediante logon na solução e uso de credenciais por ela gerenciadas.

--------> Deve monitorar sessões, gravar, detectar, correlacionar e mitigar todos os comportamentos anormais de, pelo menos, 50 usuários simultâneos acessando todos sistemas-alvo do ambiente tecnológico, dentre eles servidores Linux/Unix, Windows, controladores de domínio Microsoft Active Directory, estações de trabalho Windows e demais ativos de rede e sistemas computacionais diversos.

--------> A solução deverá ser entregue com acesso remoto seguro (externo a rede corporativa) para os usuários simultâneos mencionados, sem a necessidade de instalação e uso de clientes e VPN nos dispositivos dos usuários remotos por todo período de assinatura contratado.

--------> A solução deverá ser entregue com acesso Single-sign-on e múltiplo fator de autenticação adaptativo para, no mínimo, os usuários internos e/ou remotos (externos a rede corporativa) mencionados, por todo período contratado, suportando, no mínimo:

--------> Usuário e senha dos diretórios suportados, aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para Biometria do tipo FaceID e através do leitor de digital, Smartphone push (Notificação para aprovar ou recusar uma autenticação), Geolocalização através de coodernadas GPS e banco de dados de IP, Suporte a tokens OATH OTP, autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel, Entrega de código via SMS e chamada de voz, perguntas de segurança, notificações por e-mail e telefone celular, tokens OTP (on-line, off-line, por e-mail, hardware).

--------> Autenticação auto-ajustada baseada no contexto de risco e segurança aprendidos pela solução, permitindo a criação de um perfil para cada usuário, aproveitando atributos históricos e situacionais específicos do mesmo, como localização, dispositivo, rede, horário e índice de risco de comportamento.

--------> Análise de solicitações de autenticação em relação a padrões históricos, atribuição de índice de risco a cada tentativa de logon, geração de alertas e criação de políticas de bloqueio a serem acionadas quando um comportamento anômalo é detectado e de acesso simplificado quando o usuário é entendido como legítimo.

--------> Permitir que os usuários adicionem e modifiquem fatores de autenticação diretamente em um portal com definição de período de desvio do múltiplo fator de autenticação.

--------> Prover relatórios e dashboards customizáveis com detalhamento de informações em tempo real sobre as atividades de autenticação, como falhas na autenticação secundária, tentativas bem-sucedidas de login e os fatores de autenticação mais usados.

--------> Entenda-se como sistemas-alvo os baseados, em no mínimo, as seguintes tecnologias: S.O.: Linux/Unix e Microsoft Windows; Hypervisors: VMWare e Microsoft Hyper-V; Contas de usuários de sistemas e de serviço; Credenciais do Microsoft COM+, IIS, Apache TomCat, RedHat Jboss; Objetos (usuários, grupos e computadores) do Microsoft Active Directory e LDAP; Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL; Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi, SAN (Storage Area Network) e NAS (Network Attached Storage); Contas de usuários e administradores de consoles de gerenciamento de servidores e estações de

trabalho; Contas de equipamentos dedicados à segurança, tais como Firewall, IPS, AntiSpam e filtros de conteúdo; Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas, etc; Credenciais de nuvem em VMWare ESXi, Azure, AWS, GCP, Office 365.

+++ Gestão de dados do ciclo de vida e compartilhamento das contas privilegiadas, monitoramento e gravação de sessões privilegiadas:

--------> A solução deve conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH", disponibilizados pelos sistemas-alvo do ambiente, sem que os usuários vejam qualquer senha e chave (vigentes no momento e providas para as aplicações e conexões remotas, devendo ser recuperadas de forma automática e transparente do repositório seguro de credenciais da solução), garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso a sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no S.O. do servidor de destino, possibilitando habilitar gravação da sessão, caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;

--------> A solução deve permitir Integração para gestão de acessos privilegiados em serviços de nuvem padrões de mercado, como Amazon Web Services (AWS), Google Cloud, IBM Cloud e Microsoft Azure, disponibilizando no mínimo as seguintes funcionalidades: Integração e gestão de acessos privilegiados em contas de serviços em nuvem; Integração com sessões de serviços de nuvem, incluindo início e finalização de sessão e Gravação e auditoria de acesso de sessões iniciadas em serviços de nuvem.

--------> Deve possuir as sessões administrativas acessadas e monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de comandos e vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os comandos e vídeos gerados possam ser indexados para pesquisa futura, permitindo o filtro de comandos e ações executadas ao longo da sessão gravada, possibilitando pesquisar ações específicas na sessão gravada;

--------> Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca automatizada das senhas e chaves SSH, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas e mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;

--------> Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados e propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas e descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;

--------> Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamento e garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;

--------> Deve proteger as senhas de credenciais administrativas locais de todas estações de trabalho Windows no repositório central seguro de credenciais, permitindo a aplicação de políticas granulares de rotações e trocas automáticas das senhas, trilha de auditoria dos acessos às mesmas, mitigando situações de roubo, perda e exploração de credenciais.

--------> Quando as estações de trabalho não puderem estar conectadas de forma permanente ao repositório central de credenciais, deve aplicar, de forma autônoma, políticas de rotação de credenciais locais até a sincronização das mesmas definidas no repositório central da solução.

--------> Possuir funcionalidade de "AD Bridge" para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD;

--------> Provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;

--------> Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características: Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável; Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos; Ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução; Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas; A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP;

--------> Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário; Suportar métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;

--------> Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout's, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas; logoff dos usuários; Alterações nas funções de delegação; Adições, deleções e alterações de senhas gerenciadas pela solução; Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas; Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;

--------> Deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como: Lista de sistemas gerenciados; Senhas armazenadas; Eventos de alteração de senha; Permissões de acesso web; Auditoria de contas, sistemas e usuários; Alerta em tempo real;

+++ Análise comportamental e mitigações de risco no ambiente crítico para Identidades Privilegiadas:

--------> A solução deverá realizar a identificação e o correlacionamento de todas as ações citadas abaixo, montando perfis de comportamento gerais (usuários, acessos, credenciais, máquinas, outros) do ambiente privilegiado e acessos aos sistemas-alvo por meio da solução.

--------> Deve combinar ações que caracterizam abusos, comportamentos anormais e fora dos padrões aprendidos/mapeados, aplicando ações mitigatórias automáticas como nova autenticação, suspensão e

encerramento de sessões e troca das credenciais privilegiadas, em caso de atividades suspeitas de alto risco, detectando, no mínimo:

Acessos a solução:

--------> Durante horários irregulares (quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental);

--------> Durante dias irregulares (quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental);

--------> Através de IP irregular e desconhecido (quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental); não gerenciados (quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução).

Acessos gerais:

--------> Excessivos a contas privilegiadas (quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental);

--------> Anômalos a várias máquinas (quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto);

--------> Realizados fora da solução (diretamente no sistema-alvo);

--------> Excessivos a uma máquina;

--------> Usuários incomuns logando de uma máquina de origem conhecida;

--------> Quando ocorrem indicações de atividade de um usuário inativo da solução;

--------> Atividades definidas como suspeitas detectadas em sessões privilegiadas (comandos e anomalias na solução).

Máquinas:

--------> Acessadas a partir de endereços IP incomuns;

--------> Acessadas durante horários irregulares, de acordo com seu padrão de utilização;

--------> Incomuns originando acessos.

Credenciais e Contas:

--------> Suspeita de roubo de credenciais, quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução;

--------> Alteração de senha suspeita, quando é identificada uma solicitação para alterar ou redefinir uma senha ignorando a solução;

--------> Credenciais expostas de contas de serviço que se conectam ao LDAP em texto não criptografado;

--------> Contas privilegiadas com configuração SPN (nome principal de serviço) vulneráveis a ataques de força bruta e de dicionário off-line, permitindo que um usuário interno malicioso recupere a senha de texto sem criptografia da contas;

--------> Contas de serviço conectadas por meio de logon interativo.

--------> Deve permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos, com a possibilidade de colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador,

--------> Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em comandos Linux, comandos, janelas e aplicações Windows, expressões regulares para comandos em geral e eventos configurados manualmente, permitindo a atribuição de nível de risco customizado;

Proteção contra tomada de controle do Active Directory:

--------> A solução deve monitorar todos os Controladores de Domínio Microsoft Active Directory e mitigar automaticamente situações como roubo de identidade, acesso não autorizado e ataques que visam a tomada de controle da rede via estrutura de diretórios, de acordo com as funções de monitoramento de atividades internas nos mesmos e tráfego de segmentos de rede que estes estejam instalados, para confirmação de integridade das solicitações e tickets Kerberos utilizados nos equipamentos e contas de usuário detectando, no mínimo:

--------> Atividades anômalas em tempo real, típicas de ataques ao protocolo de autenticação Kerberos, como roubo de credenciais, movimentação lateral e escalonamento de privilégios;

--------> A extração e uso de um Kerberos TGT (ticket de concessão de tickets) da memória LSASS (Subsistema de autoridade de segurança local) em um host para obter acesso a outros recursos da rede (Pass-the-ticket);

--------> A recuperação e exploração de hashes de senha armazenados no banco de dados do SAM (Security Accounts Manager) ou do Active Directory para representar um usuário legítimo (Pass-the-Hash);

--------> O uso do hash de uma conta de usuário para obter um tícket do Kerberos, que é usado para acessar outras contas e recursos de rede (Overpass-the-Hash);

--------> A modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede - PAC Forjado (Manipulação de Certificado de Atributo de Privilégio);

--------> Ataque ao Golden Ticket, quando busca-se a obtenção de acesso ao KDC (Kerberos Key Distribution Center) para geração de token principal de segurança que fornece acesso completo a um domínio inteiro;

--------> A recuperação maliciosa de credenciais do controlador de domínio (DCSync);

--------> Delegação não restrita, através da análise das contas de domínio, que recebem privilégios de delegação permissivos e, portanto, expõem o domínio a um alto risco;

--------> Manipulação de Certificado de Atributo de Privilégio - PAC Forjado, quando há a modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede;

+++ Arquitetura e Segurança da Solução

--------> Incorporar medidas de segurança como Certificação Common Criteria (CC) – ISO/IEC 15408 – como garantia de segurança do método utilizado no desenvolvimento do sistema de repositório seguro de credenciais e Criptografia dos módulos da solução, a fim de proteger a informação em trânsito entre

módulos da solução e aplicações web dos usuários finais e possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma, sendo compatível com: AES com chaves de 256 bits, FIPS 140-2 e Encriptação PKCS#11 ou superior;

--------> Deve utilizar banco de dados em alta disponibilidade, para armazenamento de credenciais, com as melhores práticas de segurança: mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software, garantia e suporte que o compatibilize com a solução;

--------> Suportar a implementação em parque computacional Windows Server 2012 R2, Windows Server 2016 e/ou Linux em ambiente físico ou virtualizado com infra-estrutura (servidores/software em ambiente virtualizado, S.O., camada de balanceamento/redirecionamento de tráfego, etc) provida pela CONTRATANTE para implantação e uso da solução em alta disponibilidade;

--------> A solução deverá possibilitar a sua instalação nos seguintes cenários: em diferentes provedores de nuvem, em diferentes regiões de um mesmo provedor de nuvem, entre provedores de nuvem e ambiente nas dependências da CONTRATANTE e em qualquer combinação entre os itens anteriormente descritos.

--------> A solução deverá fazer uso dos serviços nativos de gestão de chaves dos provedores de nuvem para garantir o máximo nível de proteção de suas chaves criptográficas, suportando ao menos os provedores AWS e Azure.

--------> A solução deverá possibilitar sua implantação de maneira automática, através da utilização de imagens ou pacotes de instalação disponibilizados pelos provedores de nuvem, suportando ao menos os provedores AWS e Azure.

--------> Os elementos críticos da solução, como Repositório Seguro de credenciais, Gateways de Gravação e Monitoração Comportamental deverão ser instalados em alta disponibilidade ativo-ativo em cada uma das localidades (site principal, site redundante adicional e nuvem), com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação e mecanismos para a recuperação de desastres compatível com soluções de backup e arquivamento disponíveis no mercado;

--------> Prover, no mínimo, dois ambientes adicionais apartados da solução em produção para testes e homologação, replicando as mesmas licenças e funcionalidades do ambiente de produção

3. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE MONITORAMENTO DE ATAQUES CIBERNÉTICO

Requisitos das ferramentas de apoio ao monitoramento:

+++ Permitir integração com qualquer sistema de correlação de eventos (SIEM) para recebimento de alertas e abertura automática de incidentes para tratamento via fluxo de trabalho. A plataforma contratada deverá suportar o recebimento de alertas em formato Syslog;

+++ Permitir o acesso a distintos painéis de controle, totalmente customizáveis sem a necessidade do uso de programação, através da utilização de perfis diferenciados;

+++ Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática;

+++ Permitir o recebimento de Alertas de Segurança;

+++ Permitir a criação de Investigações de Incidentes que não sejam necessariamente relacionados à Segurança da Informação;

+++ Possibilitar o registro de Análise Forense, tanto para rede quanto para host.

Requisitos da ferramenta de gestão de logs e operação de incidentes (SIEM):

+++ Deve possuir arquitetura de forma distribuída, possuindo no mínimo os seguintes módulos ou componentes: módulo de coleta de pacotes e logs e geração de metadados, módulo de indexação, agregação e enriquecimento dos metadados dos coletores, módulo de correlaciona mento avançado de alertas e tratamento de incidentes e módulo de gerencia centralizada de todos os outros módulos envolvidos;

+++ Permitir a correlação de eventos provenientes de logs e pacotes do tráfego de rede, devidamente estruturados em metadados;

+++ A solução deve ser capaz de processar, correlacionar e armazenar 5000 (cinco mil) eventos por segundo (EPS), de forma sustentada;

+++ Deverá ter capacidade e ser licenciada para processar no mínimo todos os eventos gerados pelos ativos de segurança do ambiente tecnológico listados anteriormente;

+++ Ser capaz de integrar em uma única console de visualização, dados e metadados de logs e pacotes do tráfego de rede;

+++ Permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;

+++ Possuir compatibilidade e integração nativa com pelo menos uma solução de forense comportamental de endpoints (EDR), com intuito de complementar a visibilidade entregue e capacidade de análise de atividade maliciosa;

+++ Prover uma console e visão altamente intuitiva para realizar investigações sobre os dados;

+++ Possuir a capacidade de navegação continua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;

+++ Prover uma interface extremamente intuitiva, permitindo que em até três cliques seja possível chegar a uma ação suspeita ou ataque, sem prévio conhecimento da mesma;

+++ Integrar-se nativamente com uma solução de análise forense de estações, sendo capaz de utilizar dados e indicadores de comprometimento gerados pela mesma;

+++ Permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;

+++ Deve possuir pelo menos 150 regras pré-definidas;

+++ A solução deve possuir a funcionalidade de UEBA (User and Entity Behavior Analytics).

+++ Deve permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por e-mail;

+++ O fabricante da solução deve possuir ampla experiência em malwares, assim como possuir seu próprio centro de pesquisa e desenvolvimento e inteligência às novas ameaças;

+++ Deve ter sua base de inteligência diariamente atualizada através de alimentadores (feeds) de informação, provenientes da base de conhecimento em ameaças da própria empresa e de terceiros;

+++ Deve permitir o desenvolvimento e customização de interpretadores (parsers) utilizando linguagens XML e LUA, através de ferramenta gráfica do mesmo fabricante;

+++ Deve ser capaz de detectar em tempo real, ameaças alimentadas pelas seguintes bases de inteligência:

--------> relatórios de ameaças e segurança;

--------> relatórios de botnets e centros de Comando e Controle;

--------> identificação de exploit kits;

--------> indicadores de ataques "zero-day";

--------> indicadores de comprometimento, suspeitas e avisos Informativos;

--------> inteligência de tendências;

--------> proxies anônimos;

--------> classificação de sites;

--------> endereços de rede TOR.

+++ Deve possuir integração nativa com módulo de análise de malware de mesmo fabricante;

+++ O módulo de análise de malware deve permitir o uso de regras YARA;

+++ Deve possuir integração nativa com soluções de gestão de centro de operações de segurança (Security Operations Center - SOC);

+++ Deve permitir a criação de perfis de visualização do metadados derivados dos dados capturados;

+++ Deve possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;

+++ Deve permitir a visualização e análise dos dados capturados em formato gráfico de linha do tempo, construindo os gráficos com base no número de sessões, bytes ou pacotes;

+++ Deve permitir a captura de dados de forma distribuída e toda a análise centralizada;

+++ Deve possuir controle de acesso baseado em papéis e perfis de usuários;

+++ Deve permitir gerar relatórios em formatos HTML, PDF e CSV;

+++ Deve possuir um módulo para construção de relatórios customizados pelo usuário, com funcionalidade do tipo arrastar-e- colar para definição dos campos e elementos deles;

+++ Possuir a capacidade de integração com outras soluções de segurança, por meio de envio de logs/eventos via protocolos SYSLOG e SNMP;

+++ Permitir integração nativa com módulo opcional para detecção e análise de comportamento de malware do tipo "0- day" em endpoints (EDR), de forma aprimorar as investigações da solução;

+++ Permitir a definição e customização de alertas, relatórios e gráficos;

+++ Possuir integração com serviço de diretório (Active Directory) e Pluggable Authentication Module (PAM);

+++ Disponibilizar uma API ou SDK permitindo a integração e customização com a solução;

+++ Suportar a comunicação criptografada entre os componentes envolvidos;

+++ Fazer uso de protocolo proprietário entre os componentes, para garantir máximo desempenho;

+++ Deve ser projetada para possuir escalabilidade infinita;

+++ Possuir um módulo de monitoração de desempenho e saúde dos equipamentos envolvidos;

+++ Suportar o gerenciamento dos componentes através de uma interface de gerência central;

+++ Possuir métricas de saúde dos equipamentos como: utilização de CPU, temperatura da CPU, utilização de memória, disco rígido, status do serviço, status das conexões;

+++ O hardware para implementação da solução será fornecido pela infraestrutura da ANA, contudo todo e qualquer software, inclusive do hipervisor caso a solução seja virtual, deverá ser fornecido e licenciado pela CONTRATADA.

+++ Possuir relatórios de conformidade e regulamentações pré-definidos (out-of-the-box) como BASEL II, FERPA, FFIEC, FISMA, GLBA, HIPPA, ISO27002, NERC-CIP, NISPOM, PCI e SOX;

+++ Utilizar sistema operacional baseado em Linux;

+++ Deverá segregar a visualização de relatórios apenas para usuários com a devida permissão;

+++ Possuir a criação de relatórios utilizando qualquer informação armazenada no sistema;

+++ Suportar a integração nativa com sistemas de GRC (Governance, Risk e Compliance), possibilitando a integração de dashboards entre as soluções e provendo contexto de governança a um incidente gerado pela solução proposta;

+++ Possuir a funcionalidade para resolução de endereços IP, como localização da cidade, pais e organização das conexões;

+++ Possuir a capacidade de exportar e importar arquivos no formato packet capture (pcap);

+++ Permitir a visualização das sessões nos seguintes formatos: metadado, texto, hexadecimal, pacotes, reconstrução Web (HTTP), reconstrução e-mail (SMTP) e arquivos (binários);

+++ Suportar a análise de dados na camada de aplicação (modelo OSI) a partir de entidades como usuários, e-mail, endereço, arquivos e ações;

+++ Suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;

+++ A solução deve suportar a decriptação de tráfego SSL, por meio do uso de appliances físicos dedicados a este propósito;

+++ Suportar a geração de hash (MD5 e SHA1) para verificação de integridade dos arquivos extraídos a partir do tráfego de rede capturado;

+++ Deve possuir a capacidade de extração de metadados do tráfego de dados capturado, com reconhecimento nativo de no mínimo os seguintes protocolos e aplicações: FTP, SCP, HTTP, HTTPS, IMAP, IRC, MAIL (RFC822), NETBIOS, POP3, RDP, SIP, SMB, SMIME, SMTP, SNMP, SSH, TELNET, TNS, DNS, TORRENT.

+++ Possuir a capacidade de criação de interpretadores (parsers) para protocolos e aplicações proprietárias e/ou não conhecidas;

+++ Possuir a capacidade de identificação de protocolo pelo conteúdo das sessões, independente da porta utilizada de comunicação;

+++ Permitir isolar sessões de tráfegos, com identificação de conteúdo (payload) de origem e destino, para os protocolos ICMP, TCP e UDP;

+++ Permitir a extração dos arquivos presentes no tráfego de rede capturado no formato compactado .zip;

+++ Alertar em tempo real sobre tráfego coincidente com assinaturas pré-definidas e permitir a visualização da sessão em que a assinatura ocorreu, assim como a exportação da sessão para o formato .pcap;

+++ Possuir ferramenta para administração centralizada dos módulos de captura do tráfego de rede, permitindo a replicação de parâmetros de configuração entre os dispositivos a partir de uma única fonte;

+++ Deve permitir a criação customizada de interpretadores (parsers) através de linguagem XML para identificação de protocolos de rede específicos;

+++ Ser capaz de analisar tráfego IPv4 e IPv6;

+++ Permitir a customização de um interpretador de busca, cuja função é analisar todas as sessões de rede em busca de palavras chaves ou sentenças;

+++ Funcionar somente em modo passivo sem adicionar latência à rede durante a monitoração passiva;

+++ Armazenar todos os pacotes de forma segura;

+++ Permitir nativamente, a análise automatizada e ampla de malwares e suas atividades de rede;

+++ Permitir a captura e análise de características suspeitas em arquivos de conteúdo executável na rede em tempo real; A solução deve possuir um mecanismo de pontuação de risco no momento da análise de malwares;

+++ Possuir painel (dashboard) configurável que permita a rápida visualização do status da segurança e acesso granular a sessão reconstruída equivalente ao tráfego que gerou o alerta;

+++ Possuir a capacidade de exibir visualmente os objetos trafegados pela rede sem a necessidade de manipular os dados diretamente na console ou banco de dados;

+++ Permitir que a partir de uma informação existente em um relatório, se verifique o tráfego de rede que a gerou através de recurso de “drill-down”;

+++ Ser capaz de identificar a troca de extensão de arquivos (arquivo .exe enviado como .jpg);

+++ Possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;

+++ Permitir o processamento de eventos/logs, apenas com a adição de componentes para tal finalidade, mantendo a taxonomia dos metadados;

+++ Ser capaz coletar e armazenar todos os logs de ativos de rede e dispositivos que são recebidos em sua interface de rede, gravando-os em formato original para posterior uso em fins forenses;

+++ Ser capaz de coletar os logs dos ativos de rede e dispositivos de forma não intrusiva, sem a instalação de agentes;

+++ Suportar a criação de interpretadores (parsers) para os logs não suportados nativamente através de linguagem XML e LUA;

+++ Suportar a criação de interpretadores (parsers) customizados para no mínimo 20 sistemas proprietários das proponentes;

+++ Suportar de forma nativa os logs de pelo menos 300 dispositivos diferentes de diversos fabricantes;

+++ Possuir a capacidade de geração de alertas sobre qualquer dado ou comportamento desejado e permitir o envio deste alerta a plataformas externas como SIEM ou SYSLOG;

+++ Possuir capacidade de coletar logs de sistemas operacionais Windows, Linux, Unix e FreeBSD;

+++ Ser capaz de coletar logs de firewalls, antivírus, IDSs, proxies, servidores DNS, load balancers e demais dispositivos de segurança;

+++ Ser capaz de coletar logs e eventos de quaisquer dispositivos e aplicações IP que suportem nativamente os protocolos: SYSLOG, SYSLOG-NG, SNMP, Microsoft Windows Event Logging API, Microsoft Windows Remote Management, CheckPoint LEA, arquivos de logs recebido via FTP, arquivos de logs formatados por delimitadores, ODBC, CISCO e CISCO Security Device Event Exchange (SDEE);

+++ Utilizar formatos de logs/eventos através de formatos nativos de cada fabricante do dispositivo, sem utilizar um tipo de formato comum definido pelo proponente da solução;

+++ Deve exigir a adição de agentes ou software nos dispositivos monitorados, exceto caso o dispositivo a ser monitorado não disponibilize nenhum meio nativo de envio de logs citado no item anterior;

+++ Deve coletar e armazenar logs/eventos dos dispositivos sem realizar normalização no momento da coleta;

+++ Deve fazer uso de sistema de bancos de dados relacional por questão de desempenho, normalização e DBAs requeridos por esses sistemas;

+++ Permitir que os logs/eventos dos dispositivos da CONTRATANTE sejam enriquecidos com informações de classificação de risco;

+++ Permitir o correlacionamento de logs/eventos próximo ao tempo real;

+++ Possuir um painel de controle (Dashboard), onde através de simples “drill-down” possa ver o log/evento coletado; A solução deve fornecer painel de controle (Dashboard) que constantemente mostre o status do ambiente de correlação de eventos; A solução deve ser capaz de notificar o administrador caso algum dispositivo monitorado pare de enviar eventos;

+++ Permitir que o administrador possa filtrar logs/eventos ao gerar relatórios;

+++ Oferecer uma plataforma unificada, acessível via browser WEB para realizar investigações, gestão de incidentes, gestão de alertas, gestão de relatórios, administração dos componentes e gestão de inteligência externa;

+++ Permitir que os relatórios sejam executados em periodicidade diária, semanal, mensal ou em ocasiões específicas de forma automática;

+++ Possuir a capacidade de análise avançada de eventos em tempo real através de regras de correlacionamento e eventos complexos em dados correlacionados através da linguagem EPL (Event Processing Language), com mecanismo de versão igual superior à 5.3;

+++ Suportar nativamente a coleta de NetFlow, sendo capaz de capturar, analisar e correlacionar de forma contínua até 25000 fluxos por segundo na versão 5 e 15000 fluxos por segundo na versão 9;

+++ Deve detectar de forma nativa ataques do tipo NetFlow Synflood na coleta de Netflows;

+++ Ter a habilidade de receber logs/eventos oriundos de um relay desyslogs;

+++ Suportar o recebimento de eventos no formato Common Event Format (CEF);

+++ Possuir serviço de monitoração de estado de recebimento e/ou processamento de logs/eventos;

+++ Possuir procedimento de Backup & Restore para um sistema de armazenamento de longo prazo, implementando o conceito de arquivador.

+++ Suportar de forma nativa e automática o armazenamento em camadas, com as seguintes funcionalidades: HOT (dados presentes em sistemas como DACs e SANs), WARM (dados presentes em sistemas como NAS para pesquisa, execução de relatórios, exportação de dados) e COLD (dados presentes em sistemas de armazenamento off-line para possível restauração em WARM);

+++ Suportar nos sistemas de armazenamento de longo prazo, pelo menos 3 algoritmos de compressão: gzip, bzip2 e lzma;

+++ Permitir a agregação em grupos de instâncias dos vários sistemas de armazenamento de longo prazo;

+++ Permitir a exportação de logs/eventos armazenados nos formatos texto, XML, JSON, CSV;

+++ Possuir um módulo específico para tratar dados arquivados e/ou recuperados;

+++ Ser baseada em plataforma WEB, com acesso via browser padrão de mercado, sem a necessidade de instalação de aplicações cliente nas estações dos analistas responsáveis pela resposta aos incidentes;

+++ Permitir a criação e acompanhamento de Incidentes de Segurança, de forma manual ou automática, com no mínimo as seguintes características:

--------> Sumário do incidente, incluindo título, sumário e detalhes. Também deverá incluir o status do incidente, incluindo data de criação, de modificação, de fechamento, tempo em que o chamado está aberto, número de alertas agregados, prioridade e analistas envolvidos;

--------> Classificação inicial da ameaça, incluindo categoria, origem (interna/externa), possibilidade de modificação manual da prioridade e justificativa, além de informações específicas para subsidiar o relatório de incidentes e possibilidade de inclusão de documentação adicional através da anexação de arquivos;

--------> Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos etc.;

--------> Permitir agregar vários alertas em um único incidente. Esta agregação de alertas deverá permitir a visualização rápida de, no mínimo, os seguintes campos: horário do alerta, nome, prioridade e aspectos comportamentais;

--------> Definição das tarefas a serem executadas. A plataforma deverá conter uma biblioteca de procedimentos de resposta já existente;

--------> Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise; Permitir inserir análise forense de host e rede como um complemento da análise do incidente;

--------> Permitir registrar os resultados de um Incidente incluindo sua confirmação, categoria de ataque, identificação de técnicas utilizadas, detalhes sobre o alvo dos ataques e eficácia dos controles de detecção, prevenção e investigação;

--------> Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2);

--------> Permitir detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux; A solução deve possuir tecnologia de análise comportamental (UBA), baseado em técnicas de "machine learning" e analises estatísticas para a monitoração de segurança, gerando índices de riscos para eventos e entidades mapeadas;

+++ Exibir a data e hora do último login no rodapé da interface, de forma garantir que a credencial não esteja sendo compartilhada;

+++ Permitir o processamento de informações estruturadas de ameaças STIXTM ("Structured Threat Information eXpression");

+++ Possuir um ambiente de construção de regras que ofereça um mecanismo de testes (debug), visando à redução de erros de lógica e sintaxe;

+++ Permitir o ajuste de sessões concorrentes na interface de gerência;

+++ Permitir a customização de perfis de visualização de metadados de acordo com o objetivo da investigação (ex.: Analise Web, Analise e-mail, Analise de Arquivos, etc.);

+++ Possuir um menu de contexto na interface de investigações, de forma visualizar instantaneamente se endereços foram encontrados em Alertas, Incidentes ou Listas.

Requisitos da ferramenta de gestão de dispositivos de rede (NDR):

+++ A solução deve permitir análise comportamental da rede e seus componentes, dispositivos e usuários na detecção de anomalia(s), através de tecnologia baseada em Inteligência Artificial e Machine Learning.

+++ A solução deve realizar as inspeções, processamento, análise e detecção de anormalidades, sem a necessidade do envio de dados para fora da rede ou envio de logs (característica de SIEM) ou utilizando inteligência externa.

+++ Solução deve realizar a inspeção de todo trafego das redes do CONTRATANTE, de forma off-line, não dependendo da instalação de agentes nos dispositivos ou de envio de dados (syslog)

+++ Solução deve realizar a inspeção de todo trafego das redes da CONTRATANTE, também a nível de camada de aplicação (Layer 7), de forma off-line, não dependendo da instalação de agentes em computadores

+++ A coleta e análise do comportamento do tráfego deverão ser realizadas obrigatoriamente por equipamento (hardware) dedicado a esta função instalados nas dependências da CONTRATANTE.

+++ A responsabilidade de integração e suporte dos componentes de software e hardware da solução deve ser unificada sob um mesmo fornecedor, ainda que a solução tenha componentes de diferentes fabricantes.

+++ A solução deve ser inteiramente funcional, não sendo aceita solução parcial e/ou solução com necessidade de aquisição de componentes adicionais para o correto funcionamento da mesma. Para caso de componentes adicionais os mesmos (licenciamento) devem estar comtemplados na proposta comercial.

+++ Todos os componentes de software, hardware da solução deve estar em suas últimas versões estáveis.

+++ O hardware permite expansão de armazenamento sem a necessidade de substituição de equipamento ou reconfiguração de software,

+++ A solução deverá armazenar os registros dos eventos de anomalias no mínimo por 30 dias a fim de prover qualquer consulta.

+++ A solução deverá suportar análise de no mínimo 2000 ativos

+++ A solução deve realizar as inspeções por meio de espelhamento de portas através de interface Ethernet de 1Gbps e ou fibra ótica (10baseSR) de 10Gbps com no mínimo duas portas.

+++ A solução de deve permitir Threat Hunting, análise comportamental da rede e seus componentes, detecção de anomalia(s) o e visibilidade de rede.

+++ Deve utilizar no mínimo os seguintes métodos de inteligência artificial para criação de perfis de uso e identificação de desvios comportamentais na rede:

--------> Machine learning não supervisionado

--------> Machine learning supervisionado

--------> Deep Learning

--------> Redes Neurais

+++ A solução não deve depender de pré-configurações baseadas na rede da organização para que identifique associações entre múltiplos elementos da rede para que consiga identificar anomalias de comportamento.

+++ A solução deve ser capaz de aprender o comportamento da rede e de seus componentes (dispositivos e usuários) de forma autônoma e contínua se adaptando a variações de comportamento destes durante o tempo.

+++ A solução deve possuir mecanismos de DPI (Deep Packet Inspection).

+++ Solução deve realizar a inspeção do tráfego de forma off-line através de tráfego espelhado nos switches, ou seja, não dependendo de qualquer alteração de roteamento e fluxo de dados da rede.

+++ A ferramenta deve realizar o aprendizado do ambiente de rede e inspeção do tráfego de forma off-line através de tráfego espelhado de porta nos switches, ou seja, não dependendo de qualquer escaneamento ativo, alteração de roteamento e fluxo de dados da rede.

+++ A solução deve inspecionar e analisar os dados brutos da rede através de espelhamento de porta (SPAN/Port MIrror) ou através do uso de TAP – Terminal Access Point.

+++ A ferramenta deve suportar a ingestão de dados através de mecanismos de tunelamento de tráfego na camada 2 (enlace) do modelo OSI como VXLAN e ERSPAN.

+++ A ferramenta deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra ataques cibernéticos.

+++ A ferramenta deve permitir a inspeção de plataformas como:

--------> Amazon AWS

--------> Microsoft Azure

--------> Google G-Suite

--------> Office 365

--------> SalesForce

--------> Dropbox enterprise

--------> Componentes virtuais (máquinas virtuais)

--------> Endpoint para Sistemas Operacionais.

--------> Docker, Kubernetes e AWS Fargate.

--------> Box

--------> Slack

--------> Zoom

+++ A solução deve identificar de forma autônoma, os dispositivos conectados na rede no mínimo com as seguintes informações.

--------> Classificação do tipo de dispositivo (desktop, servidor, Impressora, camera, iot, etc);

--------> IP do dispositivo;

--------> Mac Address;

--------> Nome DNS do dispositivo;

--------> Primeira vez que o dispositivo/IP foi visto na rede;

--------> Última vez que o dispositivo foi visto na rede;

--------> Associação com usuários (login Active Directory) quando cabível."

+++ A ferramenta deve criar métricas, de forma autônoma, de raridade de Ips, Domínios DNS, Dispositivos, etc. baseado na frequência que estes são acessados através da rede.

+++ A ferramenta deve criar métricas, de forma autônoma, de anormalidades comparando a ação atual de um dispositivo, usuário, IP, domínio, etc. contra as ações de mesmo escopo realizadas no passado.

+++ A métrica de anormalidade deve apresentar o percentual de desvio do comportamento atual de um dispositivo comparado com o comportamento passado aprendido.

+++ A ferramenta deve ser comprovadamente baseada em análise de comportamento permitindo a detecção de, no mínimo, as seguintes anomalias:

+++ A solução deverá informar sobre conexões a destinos raros na internet, não frequentemente visitados por dispositivos da rede interna e/ou usuários.

+++ Possui informações de Whois e Geolocalização para os endereços IP e URL classificadas como ameaças.

+++ Dispositivo realizando conexões para destinos raros na internet não frequentemente visitados com por dispositivos da rede interna.

+++ Dispositivo se comunicando com um servidor externo usando um certificado auto assinado.

+++ Dispositivo se comunicando com um servidor usando um certificado expirado.

+++ Dispositivo se comunicando com um dispositivo externo usando um certificado inválido.

+++ Detectar dispositivo com conexões para um IP externo raro de maneira regular. (Beaconing)

+++ Detectar grande número de solicitações para servidores Webs, os quais estão retornando códigos de erro HTTP.

+++ Detectar atividade de penetração ou escaneamento de portas na rede.

+++ Detectar dispositivos internos realizando movimentação lateral.

+++ Detectar vários dispositivos internos começaram a desviar de suas atividades normais e escanearam a rede interna.

+++ Detectar dispositivo fazendo requisições de DNS repetidas recebendo respostas com registro TXT. (Tunelamento via DNS)

+++ Detectar dispositivo se comunicando externamente via DNS de maneira consistente com o tunelamento de DNS.

+++ Detectar dispositivo fazendo conexões criptografadas para um domínio relacionado a DNS Dinâmico

+++ Detectar dispositivo fazendo alto volume de requisições de DNS repetidas.

+++ Detectar dispositivo fazendo uma série de conexões utilizando Hostnames raros que parecem não ter uma resolução de DNS legítima.

+++ Detectar o servidor DNS interno agindo como um resolvedor de DNS aberto (OpenDns).

+++ Detectar dispositivo se comunicando com o serviço de anonimização da rede TOR.

+++ Detectar dispositivo se comunicando com a rede Tor por meio de um Web Service intermediário.

+++ Detectar atividade anormal de PowerShell e o Windown Romote Mamagement, seguido por uma conexão a um destino externo raro seguido de download de arquivo suspeito.

+++ Detectar dispositivo executando comandos PsExec ou Telnet em uma máquina remota.

+++ Detectar dispositivos transferindo volume de dados para fora da rede (IP público) e/ou internamente.

+++ Detectar dispositivos trocando um volume de dados anormal com outro dispositivo na rede interna.

+++ Detectar dispositivo se conectando repetidamente a destinos externos que não possuem nomes legíveis para humanos.

+++ Detectar dispositivo detectado conectando-se a hostnames identificados como trojans financeiros.

+++ Detectar dispositivo fazendo conexões com hostnames raros associados a uma botnet.

+++ Detectar dispositivo solicitando um domínio conhecido por hospedar malwares.

+++ Detectar dispositivo gravando arquivos com nomes suspeitos, relacionado a ransomware, em Servidores de arquivos da rede SMB.

+++ Detectar dispositivo transferindo um volume de moderado a grande de dados para fora da rede durante um período de 24 horas ou mais por meio de um grande volume de conexões.

+++ Detectar dispositivo fazendo download dados de um sistema interno e fazendo upload de volumes de dados semelhantes para destino externo.

+++ Detectar dispositivos se comunicando com domínios suspeitos na internet e, ao mesmo tempo, realizando comportamentos incomuns de transferência de arquivos na rede interna.

+++ Detectar dispositivo acessando uma grande quantidade de compartilhamentos SMB que não foram acessados anteriormente pelo mesmo dispositivo.

+++ Detectar dispositivo não conseguiu estabelecer uma sessão SMB2 seguida de uma configuração bem-sucedida da sessão SMB1 usando credenciais administrativas.

+++ Detectar dispositivo lendo e gravando volumes de dados semelhantes para compartilhamentos de arquivos remotos.

+++ Detectar dispositivo acessando arquivos que possuem de senhas não criptografadas.

+++ Detectar dispositivo enviando um grande volume de dados para um IP externo que raramente é utilizado por qualquer dispositivo na rede interna.

+++ Detectar dispositivo fazendo conexões web externas sem usar um proxy web.

+++ Dispositivo sendo bloqueado repetidamente por um proxy web durante um período de várias horas.

+++ Dispositivo solicitando informações de configuração de proxy (WPAD) para um IP externo.

+++ Detectar dispositivo fazendo conexões HTTP suspeitas, de forma repetitiva, diretamente para um endereço IP sem utilizar um Hostname.

+++ Detectar dispositivos causando repetidos picos de conexões HTTP ou SSL na rede interna ou para a internet.

+++ Detectar dispositivos fazendo download de arquivo executável (exe e/ou msi) vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

+++ Detectar dispositivos fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

+++ Detectar dispositivo fazendo requisições HTTP suspeitas repetidamente em portas não padrão.

+++ Detectar dispositivo informando no cabeçalho User-Agent que possui um sistema operacional o qual é diferente do SO que realmente está utilizando.

+++ Detectar dispositivo fazendo download de um arquivo que não corresponde ao seu 'File Type' de uma fonte externa que a rede normalmente não acessa.

+++ Detectar dispositivo usando uma plataforma externa de armazenamento de arquivos de terceiros, exemplo: GoogleDrive, DropBox, Wetransfer, OneDrive etc.

+++ Detectar dispositivo fazendo download de arquivo comprimido vindo de uma fonte a qual não é comumente acessada por dispositivos da rede interna.

+++ Detectar dispositivo fazendo download de um arquivo suspeito e em seguida fez uma conexão para um destino externo com o qual a rede normalmente não se comunica.

+++ Detectar dispositivo enviando dados para o Pastebin, Zerobin.net, ghostbin.com, rentry.co, controlc.com, hastebin.com.

+++ Detectar dispositivos usando um sistema terceiro de mensageria (Whatsapp, telegram, Hangout ou similares).

+++ Detectar dispositivo acessando rede social (Facebook ou similares).

+++ Detectar dispositivo se comunicando com um destino raro na internet usando portas normalmente usadas apenas na rede interna.

+++ Detectar dispositivo fazendo conexões peer-to-peer BitTorrent.

+++ Detectar dispositivos fazendo conexões SQL para IPs externos a rede.

+++ Detectar dispositivo que recebeu um número anormalmente grande de conexões de entrada de IP externos raros.

+++ Detectar dispositivo enviando uma quantidade anormal alta de dados para destinos fora da rede.

+++ Detectar dispositivo trocando um volume de dados anormal com outro dispositivo na rede interna.

+++ Detectar dispositivo enviando uma quantidade anormalmente alta de dados externamente para um local para o qual a rede não enviou dados anteriormente.

+++ Detectar dispositivo explorado vulnerabilidade Heartbleed na rede interna.

+++ Detectar dispositivo se conectando a um DNS SinkHole conhecido.

+++ Detectar dispositivo realizando grandes volumes de pequenas conexões SSH e/ou RDP.

+++ Detectar dispositivo iniciando um grande número de conexões RDP e/ou SSH e conexões não realizadas anteriormente.

+++ Detectar dispositivo recebendo um grande número de conexões RDP ou SSH de entrada de IPs externos raros.

+++ Alteração de bloco CIDR de uma subrede.

+++ Alteração no comportamento de tráfego DHCP.

+++ Detectar novo servidores de DNS e DHCP na rede.

+++ Detectar servidores de proxy web na rede.

+++ Detectar a adição ou remoção de domínios DNS na rede

+++ Detectar perdas de pacotes e retransmissões superior a um percentual parametrizável na ferramenta ou anormal.

+++ Detectar credenciais de alto privilégio sendo utilizada para acessar servidores (podendo ser parametrizadas ou visualizada pelo AD).

+++ Detectar uma credencial efetuando login de uma origem incomum.

+++ Detectar credenciais usadas em múltiplos dispositivos internos.

+++ Possuir funcionalidade integrada para reconstrução completa de arquivos, a partir dos PCAPs capturados, inclusive de arquivos anexos a e-mails, trafegados na web ou compartilhados entre usuários;

+++ Realizar inspeção em pacotes https (https inspection).

+++ Permitir recebimento de logs externos para a realização da análise, tais como Microsoft Active Directory, Checkpoint e McAffe.

+++ Possuir interface gráfica de gerenciamento, independente de plataforma, preferencialmente em Web via protocolo HTTPS, uso de criptografia TLS 1.2, funcionando nos navegadores Google Chrome, Microsoft New Edge e Firefox,

+++ A solução deve se integrar com serviço OpenLDAP e/ou AD a fim de possibilitar a autenticação na interface, autorização de usuários e para consultas com objetivos de enriquecer os dados inspecionados.

+++ A solução deve permitir a utilização de segundo fator de autenticação nativa para logins na interface web.

+++ A interface deve permitir a procura e navegação a qualquer dispositivo, usuário, Ips, portas, tipos de ataques etc. que tenham sido inspecionados em qualquer horário/data armazenada pela solução.

+++ Possuir alertas de detecção de anomalias contendo no mínimo os seguintes dados:

--------> Data e horário.

--------> Dispositivo e/ou usuários que originou a ação.

--------> Descrição técnica do evento.

--------> Gráfico apresentando a quantidade de eventos similares e evolução do nível de risco.

--------> Dados técnicos resumidos das ações que causaram a anomalia e subsequente alerta."

+++ Permitir que os alertas de anomalias sejam enviadas por e-mail e/ou sistema de mensageria (WhatsApp, Telegram, SMS etc.)

+++ Permitir a visibilidade dos logins dos usuários aos dispositivos da rede (Desktops e notebooks)

+++ Deve permitir o recebimento de logs de sistemas externos utilizando padrões de mercado, como CEF, LEEF, JSON e Syslog.

+++ Deve permitir a integração nativa com plataforma de gerenciamento de chamados como HPSM, Atlassian, JIRA e ServiceNow.

+++ Deve permitir a integração com plataformas de Threat Inteligence utilizando os protocolos STIX/TAXII.

+++ A plataforma deve possuir OPEN API para suportar integração com sistemas terceiros.

+++ Deve possuir ferramenta para a criação e customização de relatório e envio.

+++ Possuir relatório gerencial indicando a quantidade total de dispositivos, quantidade total de sub redes e throghput (máximo e média).

+++ Deve indicar a quantidade total de dispositivos, quantidade total de sub redes e banda média processada.

+++ Possuir sumário das violações por fase do ataque.

+++ Possuir sumário dos dispositivos com maior nível de brechas não usuais.

+++ Possuir sumario dos top dispositivos que mais violaram comportamentos anômalos.

+++ Mostrar as violações mais frequentes a principais itens de compliance como: uso de USB no dispositivo, google drive, tráfego RDP saindo da rede, acesso a servidor SQL através da internet, dentre outros.

+++ Possuir sumário dos dispositivos que mais violaram os itens de compliance gerando risco a organização.

+++ Deve permitir que o relatório seja exportado para documento padrão .PDF e/ou .csv.

+++ Deve possuir mecanismo para busca de dados diretamente na base de dados da ferramenta.

+++ Possuir sumário das tops violações e/ou comportamentos anômalos

4. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE RESPOSTA A INCIDENTES DE SEGURANÇA

A mesmas do Item 3. Assim sendo necessário que esteja em execução demanda do serviço apoiado pelo item 3 para a prestação deste tipo de serviço.

5. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE PROTEÇÃO DE ENDPOINTS E SERVIDORES DE REDE

Requisitos da ferramenta em termos gerais:

+++ A solução deverá ser entregue na modalidade on-premises (local) ou como um serviço (em nuvem);

+++ Possuir console Web para gerenciamento e administração da ferramenta;

+++ A solução deverá ser toda de um único fabricante;

+++ A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações, Controle de dispositivos e EDR (Endpoint Detection and Response) em um único agente.

Requisitos da ferramenta para administração:

+++ Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

+++ Deve possibilitar instalação "silenciosa", podendo utilizar de scripts, ou soluções para deploy e upgrade de software, sem a interação do usuário final;

+++ Deve permitir o bloqueio por nome de arquivo;

+++ Deve permitir o travamento de pastas e diretórios;

+++ Deve permitir o travamento de compartilhamentos;

+++ Deve permitir o rastreamento e bloqueio de infecções;

+++ Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

+++ Quando on-premises, deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

+++ Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

+++ Deve permitir a desinstalação através da console de gerenciamento da solução;

+++ Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

+++ Quando on-premises, deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

+++ Deve permitir a deleção dos arquivos quarentenados;

+++ Deve permitir remoção automática de clientes inativos por determinado período de tempo;

+++ Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;

+++ Quando on-premises, identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada. Em caso de soluções em nuvem, será aceita utilização de ferramenta do próprio fabricante para varredura local;

+++ Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

+++ Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

+++ Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

+++ Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory, tipo ou IP;

+++ Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

+++ Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

+++ Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

+++ Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

+++ Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção;

+++ Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

+++ Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

+++ Deve permitir a criação de usuários locais de administração da console de anti-malware;

+++ Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

+++ Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

+++ Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

+++ Deve permitir a gerência de domínios separados para usuários previamente definidos;

+++ Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

+++ Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

Requisitos da ferramenta para atualização:

+++ Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

+++ Deve permitir atualização incremental da lista de definições de vírus;

+++ Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

+++ Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

+++ Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

+++ Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

+++ O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

Requisitos da ferramenta para proteção avançada para servidores Windows/Linux:

Características gerais,

+++ A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

--------> Windows Server 2000;

--------> Windows Server 2003 SP1 e 2003 R2 SP2;

--------> Windows Server 2008 e 2008 R2;

--------> Windows Server 2012 e 2012 R2;

--------> Windows Server 2016;

--------> Windows Server 2019;

--------> Windows Server 2022;

--------> Red Hat Enterprise 5, 6, 7 e 8;

--------> CentOS 5, 6, 7 e 8;

--------> AIX 6.1, 7.1 e 7.2;

--------> Oracle Linux 5, 6, 7 e 8;

--------> SUSE Linux Enterprise Server 10, 11, 12 e 15;

--------> Ubuntu 10, 12, 14, 16, 18 e 20;

--------> Debian 6, 7, 8, 9 e 10;

--------> Rocky Linux 8;

--------> AlmaLinux 8;

--------> Cloud Linux 5, 6, 7 e 8;

--------> Solaris 10 1/13 Sparc;

--------> Solaris 10 1/13 (x86/x64);

--------> Solaris 11.2/ 11.3 Sparc;

--------> Solaris 11.2/ 11.3 (x86/x64);

--------> Solaris 11.4 (x86, x64 ou SPARC)

--------> Amazon Linux e Amazon Linux 2 (x64).

+++ A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;

--------> A console de gerenciamento deverá ser em nuvem ou on-premises, permitindo o gerenciamento das políticas de segurança através da Internet;

--------> A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;

--------> A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;

--------> Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

--------> A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

--------> A console de administração deverá permitir o envio de notificações via SMTP;

--------> Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

--------> A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;

--------> A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

--------> A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

--------> A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;

--------> A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

--------> A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

--------> A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;

--------> Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

--------> A solução de segurança ter a capacidade de identificar ataques entre conteineres;

--------> Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

--------> Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar políticas de segurança;

--------> A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

--------> Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

--------> A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

--------> Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

--------> Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

--------> Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

--------> Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

--------> Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

--------> Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

--------> Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

--------> A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

--------> Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

--------> A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

--------> A solução deverá mostrar quais máquinas estão usando determinada política;

--------> Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

--------> Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

--------> A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

--------> Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

--------> O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

--------> A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

--------> A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

--------> A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

--------> A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArcSight de modo a permitir enviar os seus logs para essas soluções;

--------> A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

--------> Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

--------> Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

--------> As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

--------> Após a atualização deve ser informado o que foi modificado ou adicionado;

--------> Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

--------> A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

--------> A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

--------> Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

--------> No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

--------> Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

--------> Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

--------> Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

--------> O fabricante deverá participar do programa "Microsoft Application Protection Program" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

--------> A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

--------> O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

--------> A solução deve possuir API documentada para integração na esteira de automação;

--------> A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

--------> Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

--------> A solução deve permitir desabilitar os módulos individualmente;

--------> Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.

Requisitos das funcionalidades de antimalware:

--------> A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

--------> A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

--------> A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

--------> Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

--------> A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

--------> Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

--------> A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

--------> A solução deverá oferecer escanear processos em memória em busca de Malware;

--------> O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

--------> O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;

--------> Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

--------> A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

--------> Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

--------> A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

--------> Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

--------> Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

--------> Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

--------> A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

--------> Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

--------> Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

Requisitos das funcionalidades de proteção contra URLs maliciosas:

--------> Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

--------> A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

--------> A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;

--------> Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

--------> Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

--------> Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

--------> A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

--------> A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

Requisitos das funcionalidades de firewall:

--------> Operar como firewall de host, através da instalação de agente nos servidores protegidos;

--------> Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

--------> Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

--------> Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

--------> A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;

--------> Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

--------> Precisa ter a capacidade de definição de regras para contextos específicos;

--------> Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;

--------> Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

--------> Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

--------> O firewall deverá ser stateful bidirecional;

--------> O firewall deverá permitir liberar ou apenas logar eventos;

--------> O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

--------> As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

--------> A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

--------> As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

--------> Deverá realizar pseudo stateful em tráfego UDP;

--------> Deverá logar a atividade stateful;

--------> Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

--------> Deverá permitir limitar o número de meias conexões vindas de um computador;

--------> Deverá prevenir ack storm;

--------> Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

--------> Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período configurado pelo administrador;

--------> Deverá permitir criar lista de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede;

--------> Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

Requisitos das funcionalidades de vulnerabilidade de so e aplicações:

--------> Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

--------> Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

--------> A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;

--------> Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

--------> Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS,

SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

--------> Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

--------> Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

--------> Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

--------> Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

--------> Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

--------> Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

--------> Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

--------> Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

--------> Deverá ser capaz de inspecionar tráfego criptografado de entrada;

--------> Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

--------> As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

--------> Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

--------> Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

--------> Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

--------> Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

--------> As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

--------> As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

--------> As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;

--------> As regras de IPS poderão ter sua capacidade de LOG desabilitado;

--------> As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

--------> As regras devem ser atualizadas automaticamente pelo fabricante;

--------> Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

Requisitos das funcionalidades de monitoramento da integridade:

--------> A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

--------> Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

--------> Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

--------> Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

--------> Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

--------> Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

--------> Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

--------> O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

--------> Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real- time para ambiente Linux;

--------> Deverá logar e colocar em relatório todas as modificações que ocorram;

--------> As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

--------> Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

--------> Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

--------> Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

Requisitos das funcionalidades de inspeção de LOGs:

--------> A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;

--------> Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

--------> Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;

--------> Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

--------> Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

--------> Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;

--------> Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;

--------> Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;

--------> Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;

--------> Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

--------> As regras poderão ser modificadas por severidade de ocorrência de eventos;

--------> As regras devem se atualizar automaticamente pelo fabricante;

--------> Permitir modificação pelo administrador em regras para adequação ao ambiente.

Requisitos da funcionalidade de controle de aplicação:

--------> A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

--------> O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;

--------> O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

--------> A console deverá exibir eventos de no mínimo 30 dias;

--------> A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;

--------> A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

Requisitos da funcionalidade para detecção e resposta:

--------> A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

--------> A solução deve possuir módulo de investigação, detecção integrados;

--------> Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

--------> A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

--------> Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

--------> O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

--------> Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

--------> A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

--------> A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;

--------> A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

--------> Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

--------> Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

--------> Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

--------> Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;

--------> Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

--------> Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

--------> A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

--------> Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

Requisitos da ferramenta para proteção antimalware Windows estações de trabalho e notebooks:

--------> Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

--------> Windows 8.1 (x86/x64);

--------> Windows 10 (x86/x64);

--------> Windows 11 (x64).

--------> Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

--------> Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

--------> Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

--------> Processos em execução em memória principal (RAM);

--------> Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

--------> Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

--------> Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

--------> Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;

--------> Deve possuir detecção heurística de vírus desconhecidos;

--------> Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

--------> Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

--------> Em tempo real de arquivos acessados pelo usuário;

--------> Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

--------> Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

--------> Automáticos do sistema com as seguintes opções:

--------> Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

--------> Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

--------> Frequência: horária, diária, semanal e mensal;

--------> Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

--------> Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

--------> Em caso de arquivos suspeitos, a solução deve ter a capacidade de enviar o artefato para um ambiente de sandbox do próprio fabricante para identificar ameaças desconhecidas;

--------> O módulo de análise de artefatos desconhecidos (sandbox) deve estar integrada à solução de antimalware, sem necessidade de plugins adicionais;

--------> O módulo de sandbox deve permitir a análise de arquivos submetidos diretamente dos agentes;

--------> Em caso de ameaças desconhecidas detectadas pela sandbox, a solução deve ter a capacidade de adicionar os objetos suspeitos (hash de arquivo, IP, domínio e URL) numa lista de bloqueio automaticamente;

--------> Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

--------> Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

--------> Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

--------> Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

--------> Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

--------> Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos

--------> Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

--------> Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

--------> Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

--------> Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

--------> Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

--------> Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

--------> Deve bloquear processos comuns associados a ransomware;

--------> Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios

--------> Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

--------> Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

Requisitos da funcionalidade para controle de dispositivos:

--------> As configurações da funcionalidade de controle de dispositivos devem ser aplicada por usuário;

--------> Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

--------> Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

--------> Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

--------> Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

--------> Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

--------> Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;

--------> Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

--------> Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

--------> Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

Requisitos da funcionalidade para proteção anti-malware estações de trabalho Mac os X:

--------> O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:

--------> macOS 12 (Monterey);

--------> macOS 11 (Big Sur)

--------> macOS 10.15 (Catalina);

--------> macOS 10.14 (Mojave);

--------> macOS 10.13 (High Sierra);

--------> Suporte ao Apple Remote Desktop para instalação remota da solução;

--------> Gerenciamento integrado à console de gerência central da solução

--------> Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

--------> Permitir a verificação das ameaças da maneira manual e agendada;

--------> Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

--------> Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

--------> Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

--------> Deve possuir no mecanismo de autoproteção as seguintes proteções:

--------> Proteção e verificação dos arquivos de assinatura;

--------> Proteção dos processos do agente de segurança;

--------> Proteção das chaves de registro do agente de segurança;

--------> Proteção do diretório de instalação do agente de segurança.

Requisitos da funcionalidade para proteção para smartphones e tablets:

---------> O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

--------> IOS e Android;

--------> As funcionalidades estarão disponíveis de acordo com cada plataforma

--------> Deve permitir o provisionamento de configurações de:

--------> Wi-fi, Exchange Activesync, vpn, proxy http global e certificados;

--------> Deve possuir proteção de anti-malware para Android;

--------> Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

--------> Possuir capacidade de detecção de spam proveniente de SMS;

--------> Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número bloqueados para recebimento de chamadas;

--------> Possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de número permitidos para efetuação de chamadas;

--------> Permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

--------> Permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

--------> Permitir o bloqueio de aplicativos de acordo com sua faixa etária indicativa;

--------> Possuir controle da política de segurança de senhas, com critérios mínimos de: Padrão de senha; Uso obrigatório de senha; Tamanho mínimo; Tempo de expiração; Bloqueio automático da tela; Bloqueio por tentativas inválidas.

--------> Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis:

--------> Bluetooth;

--------> Câmera;

--------> Cartões de memória;

--------> Wlan/wifi;

--------> GPS;

--------> Microsoft Activesync;

--------> MMS/SMS;

--------> Alto-falante;

--------> Armazenamento USB;

--------> 3G;

--------> Modo de desenvolvedor;

--------> Ancoragem (tethering).

Requisitos da funcionalidade criptografia de disco:

--------> Possuir a capacidade de realizar a criptografia nos seguintes sistemas operacionais:

--------> Windows 8.1 (x86/x64) ;

--------> Windows 10 (x86/x64);

--------> Windows 11 (x64).

--------> Possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), permitindo criptografia para: Disco completo (FDE – full disk encryption); Pastas e arquivos; Mídias removíveis; Anexos de e-mails e Automática de disco;

--------> Possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

--------> Possuir a capacidade de exceções para criptografia automática;

--------> Possuir compatibilidade de autenticação por múltiplos fatores;

--------> Permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

--------> Possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

--------> Possuir mecanismos para wipe (limpeza) remoto;

--------> Possuir mecanismo para desativar temporariamente a autenticação depré-inicialização (boot);

--------> Possuir mecanismo que permita desfazer a criptografia do disco no evento em que se torne corrompido, impedindo a inicialização da estação/notebook;

--------> O ambiente de autenticação pré-inicialização deve permitir a conexão a redes sem fio (wireless);

--------> Permitir, em nível de política, a indicação de pastas a serem criptografadas;

--------> Possibilitar que cada política tenha uma chave de criptografia única;

--------> Permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

--------> Possibilitar a desativação de dispositivos de gravação de mídias óticas e de dispositivos de armazenamento USB;

--------> Possibilitar apagar todos os dados do dispositivo na ocorrência de um número personalizável de tentativas inválidas de autenticação.

Requisitos da funcionalidade para proteção Host IPS e Host firewall:

--------> Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:

--------> Windows 8.1 (x86/x64);

--------> Windows 10 (x86/x64);

--------> Windows 11 (x64).

--------> Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

--------> As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

--------> Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

--------> Deve permitir ativar e desativar o produto sem a necessidade de remoção;

--------> Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;

--------> Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;

--------> O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

--------> O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

--------> O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra ameaças conhecidas ou desconhecidas;

--------> O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

--------> Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

--------> Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

--------> A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

Requisitos da funcionalidade para controle de aplicações:

--------> Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

--------> Windows 8.1 (x86/x64);

--------> Windows 10 (x64);

--------> Windows 11 (x64).

--------> As regras de controle de aplicação devem permitir as seguintes ações:

--------> Permissão de execução;

--------> Bloqueio de execução;

--------> Bloqueio de novas instalações.

--------> A regra de liberação para o controle de aplicação deverá pemitir que o programa liberado efetue ou não a execução de outros processos,

--------> As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

--------> As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

--------> Assinatura SHA-1 e SHA-256 do executável;

--------> Atributos do certificado utilizado para assinatura digital do executável;

--------> Caminho lógico do executável;

+++ Base de assinaturas de certticados digitais válidos e seguros.

--------> As regras de controle de aplicação devem possuir categorias pré-determininadas de aplicações;

--------> As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

--------> O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;

--------> Deve permitir a busca por aplicações ou fabricante destas;

--------> Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

Requisitos da funcionalidade para detecção e resposta:

--------> A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

--------> O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

--------> A solução deve possuir módulo de investigação e detecção integrados;

--------> Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

--------> Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

--------> Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

--------> Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

--------> Fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

--------> Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

--------> Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;

--------> Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;

--------> Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

--------> Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

--------> Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

--------> A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

--------> Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

--------> O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

--------> Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

--------> A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

--------> A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

--------> Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;

--------> Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

--------> Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

--------> Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

--------> Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

--------> Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

--------> Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

--------> Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

--------> Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

--------> Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

--------> Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

--------> A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

--------> Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

--------> Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

--------> Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;

--------> Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

--------> Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

--------> Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

--------> Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

--------> Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

--------> Restaurar a conectividade da estação de trabalho com a rede;

--------> Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

--------> Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

Requisito da ferramenta para proteção contra vazamento de informações (DLP):

--------> Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:Windows Server 2012 (32/64-bit) ou superior, Windows 7 SP1 (x86/x64), Windows 8 e 8.1 (x86/x64), Windows 10 (x86/x64) e superior.

--------> Deve possuir, nativamente, templates para atender as seguintes regulamentações: PCI/DSS, HIPA, Glba, SB-1386, US PII.

--------> Deve ser capaz de detectar informações, em documentos nos formatos:

--------> Microsoft Office (doc, docx, xls, xlsx, ppt, pptx)

--------> OpenOffice;

--------> rtf, wordpad, text; xml, html;

--------> Gráficos: visio, postscript, pdf, tiff,

--------> Comprimidos: win zip, rar, tar, jar, arj, 7z, rpm, cpio, gzip, bzip2,

--------> unix/linux zip, lzh;

--------> Códigos: C/C++, Java, Verilog, Autocad, .js, .vbs e demais arquivos de Script;

--------> Deve ser capaz de detectar informações, com base em:

--------> Dados estruturados, dados pessoais, endereços de e-mail, CPF, entre outros;

--------> Palavras ou frases configuráveis;

--------> Expressões regulares;

--------> Extensão dos arquivos.

--------> Deve ser capaz de detectar em arquivos compactados;

--------> Deve permitir a criação de modelos personalizados para identificação de informações;

--------> Deve permitir a criação de políticas personalizadas;

--------> Deve permitir a criação de políticas baseadas em múltiplos modelos;

--------> Deve permitir mais de uma ação para cada política, como:

--------> Apenas registrar o evento da violação;

--------> Bloquear a transmissão;

--------> Gerar alertar para o usuário;

--------> Gerar alertar na central de gerenciamento;

--------> Capturar informação para uma possível investigação da violação.

--------> Deve permitir criar regras distintas com base se a estação está fora ou dentro do ambiente físico da ANA;

--------> Deve ser capaz de identificar e bloquear informações nos meios de transmissão:

--------> Cliente de e-mail;

--------> Protocolos HTTP, HTTPS, FTP;

--------> Mídias removíveis;

--------> Discos óticos CD/DVD;

--------> Gravação CD/DVD;

--------> Aplicações de mensagens instantâneas;

--------> Tecla de print screen;

--------> Aplicações P2P;

--------> Área de transferência do Windows;

--------> Webmail;

--------> Armazenamento na nuvem (cloud);

--------> Impressoras;

--------> Scanners;

--------> Compartilhamentos de arquivos;

--------> Activesync;

--------> Criptografia PGP;

--------> Deve permitir a criação de exceções nas restrições dos meios de transmissão.

6. FERRAMENTA(S) DE APOIO A GESTÃO DE MENSAGERIA PROATIVA

Requisitos da ferramenta para gestão de mensageria proativa:

+++ A solução deve permitir a identificação e proteção contra ameaças no Microsoft Office 365 (Exchange Online, Sharepoint Online, Onedrive for Business e Microsoft Teams) e GSuite;

+++ Identificar e bloquear arquivos maliciosos carregados para o Google Drive, Onedrive, Sharepoint e Microsoft Teams. Por exemplo, se um usuário tentar carregar um determinado arquivo malicioso ou proibido em uma das plataformas citadas, a solução deve fazer o bloqueio;

+++ Bloquear upload de arquivos por tipo definido em política para as soluções supracitadas;

+++ Identificar e bloquear URLs maliciosas em arquivos e URLs, incluindo URLs dentro de anexos;

+++ Realizar escaneamentos de ameaças em tempo-real nos serviços integrados, identificando componentes maliciosos;

+++ Permitir realizar escaneamento retroativo de ameaças (sob demanda), isto é, em busca de ameaças já armazenadas nas caixas de email dos usuários ou em diretórios do Google Drive, Onedrive e Sharepoint;

+++ O nivel de sensibilidade das URLs maliciosas deve ser configurável através de políticas;

+++ Deve possuir capacidade de cadastro dos usuários importantes para focar a análise de ataques de Comprometimento de Email (BEC);

+++ Deve permitir que os administradores configurem a periodicidade das notificações para, no mínimo, URLs maliciosas identificadas, SPAMs maliciosos, Phishing, Ransomware, arquivos analisados na sandbox e identificados como baixo, médio e alto risco;

+++ Identificar tentativas de Comprometimento de Email baseado em uma análise dos estilos de escrita de cada usuário cadastrado como importante;

+++ A solução deve permitir a visualização das estatísticas no dashboard por serviço integrado (Gmail, Google Drive, Exchange Online, Teams, Onedrive, Sharepoint) e alterar o período dos logs para, no mínimo, 24 horas, 7 dias e 30 dias;

+++ Deve permitir a exibição da tendência para cada um dos tipos de serviço integrado em relação ao mesmo período anterior. Por exemplo, exibir aumento ou redução das ameaças no Exchange Online nos últimos 30 dias, comparando com os 30 dias anteriores;

+++ Deve ter a capacidade de analisar arquivos e URLs em sandbox para identificação de ameaças desconhecidas (sem assinatura);

+++ Deve utilizar mecanismos de proteção que contemplem, pelo menos, malwares conhecidos por assinatura, malwares desconhecidos por Machine Learning, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URLs;

+++ A solução deve permitir compartilhamento de informações através de SIEM via API ou através da gerência centralizada;

+++ A solução deve prover relatórios que contemplem, pelo menos, riscos de segurança (ameaças), ransomware, arquivos analisados em sandbox, auditoria e sobre a API;

+++ Os relatórios devem ser exportáveis para, pelo menos, PDF;

+++ Os relatórios devem ser enviados por email, mediante configuração do administrador;

+++ A verificação Anti-malware deverá permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.

+++ Realizar integração nuvem-a-nuvem, através de API da Microsoft e Google;

+++ As ações configuráveis nas políticas do serviço de email devem contemplar, no mínimo, etiquetar a mensagem (inserir tag), quarentenar, deletar, ignorar e mover para lixeira;

+++ Os demais serviços devem possuir ações pré-definidas e configuráveis para eliminar, quarentenar e ignorar os arquivos identificados;

+++ Deve empregar o uso de análise em ambiente virtual (sandbox) do próprio fabricante para detecção de malwares avançados, com objetivo de diminuir seu risco de violação;

+++ As políticas deverão ser aplicáveis por usuário ou grupo sincronizado da estrutura de serviço online (Microsoft ou Google);

+++ Possuir um dashboard com as principais ameaças detectadas, a exemplo dos tipos Ransomware, Phishing, Comprometimento de E-mail.

+++ A solução deverá ser capaz de implementar políticas com base no filtro de conteúdo das mensagens;

+++ A solução deverá ter a capacidade de compartilhar objetos suspeitos identificados através da análise em sandbox com a gerência centralizada do fabricante;

+++ Cada política de serviço deve ser configurável para apenas monitorar ou tomar ação de proteção;

+++ As notificações enviadas para o administrador e para os usuários devem ser customizáveis, permitindo tradução, inclusão ou exclusão de campos;

+++ Deverá permitir a configuração dos níveis de detecção para SPAM;

+++ Deverá permitir o administrador criar exceções para permitir ou bloquear determinados endereços de email e URLs manualmente;

+++ A solução deve possuir capacidade de ignorar emails já enviados para a lixeira do serviço de email;

+++ Deve permitir ao administrador bloquear mensagens de graymail por tipo (mensagens de marketing, notificações de foruns e redes sociais, etc);

+++ Os logs devem ser interativos, permitindo ao administrador montar consultas baseadas nos parametros como serviço detectado, tipo/categoria da ameaça, usuários afetados, política acionada, nome da ameaça, dentre outros;

+++ Os resultados das consultas de logs deverão ter opção de salvar como um relatório exportável;

+++ A solução deve permitir que o administrador realize buscas pontuais nos logs, a partir de parametros previamente definidos;

+++ Deve possuir áreas de quarentena distintas para cada um dos serviços integrados, permitindo a restauração, download ou exclusão de arquivos/emails quarentenados pela política;

+++ Deve permitir a criação de exceções para detecções por Machine Learning e por Sandbox;

+++ A solução deve ter a capacidade de integração com serviços de autenticação para logon único (single sign-on) com, pelo menos, Okta, ADFS e Azure AD.

+++ Deve possuir capacidade de configuração de contas de administração com permissões granulares por administrador, permitindo visualização ou controle total dos itens de menu;

+++ Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação;

+++ Deve suportar a integração com serviço de gerenciamento de incidentes do próprio fabricante através da plataforma de investigação.

+++ O recurso de detecção e resposta para e-mails deverá ser integrado à solução da Microsoft Office 365 sem a necessidade de alterar configurações dos serviços de e-mail, ou configurações dos usuários;

+++ Possuir modelos pré-definidos pelo fabricante de atividades suspeitas e/ou maliciosas para identificação e categorização de ameaças no ambiente;

+++ A solução deve ser capaz de associar diferentes modelos de ameaças e associá-los a um único incidente/evento;

+++ Deve ter capacidade de apresentar informações relacionadas ao MITRE para cada um dos eventos detectados no ambiente, caso possuam;

+++ Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

+++ Em caso de ameaça avançada por email, a solução deve permitir tomar diferentes ações de resposta no ambiente, contemplando, no mínimo:

+++ Permitir adicionar o remetente (sender) de um e-mail na lista de bloqueio, impedindo o mesmo de enviar novos e-mails os usuários internos;

+++ Mover o e-mail selecionado para a área de quarentena de um específico usuário ou todos os usuários que contenham este e-mail em suas caixas;

+++ Deletar o e-mail selecionado das caixas selecionadas.

7. FERRAMENTA(S) DE APOIO A SERVIÇO DE INTELIGÊNCIA APLICADA A SEGURANÇA

+++ Deverá identificar, reconhecer, coletar, analisar, processar, organizar e apresentar informações disponíveis e acessíveis, de forma automatizada e personalizada, em conversas, mídias e redes sociais, demais páginas da internet de superfície, profunda e oculta, fóruns, redes de compartilhamento de textos e códigos-fonte, aplicativos de mensageria, lojas de aplicativos, feeds RSS, páginas de comércio eletrônico, bem como monitorar outros serviços de descoberta e monitoração e quaisquer outras fontes de informação disponíveis e acessíveis;

+++ Coletar diariamente informações de pelo menos 44 fontes relevantes de inteligência sobre ameaças disponíveis pelo mundo, de categorias como phishing, código, propriedade intelectual, chaves/senhas, botnets, internet profunda (deep web), spam, aplicativos falsos e documentos confidenciais;

+++ Correlacionar as informações coletadas, utilizando plataforma de big data para processamento visando normalizar informações, gerando listas acionáveis de inteligência contra ameaças;

+++ Monitorar ameaças emergentes e avaliar a aplicabilidade especificamente no ambiente da ANA em questão, propondo proativamente a realização de contramedidas com o objetivo de prevenir a exploração de alguma brecha de segurança;

+++ Deverá permitir o gerenciamento, configuração e utilização centralizada de todos os recursos disponibilizados;

+++ Deverá possuir painel de visualização de fácil utilização e configuração, permitindo a seleção da(s) funcionalidade(s) que será(ão) utilizada(s);

+++ Deverá possuir modelos de filtro de informações pré-configurados, personalizados de acordo com comportamentos conhecidos dos usuários na utilização das diferentes fontes de informação monitoradas;

+++ Deverá ser possível, de forma simples e rápida, a alteração dos critérios de busca de informações de acordo com as necessidades da ANA;

+++ Deverá fornecer análise de dados coletados, fornecendo um painel de visualização que contemple, no mínimo:

+++ Visualização de perfis relacionados a palavras-chaves;

+++ Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;

+++ Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas;

+++ Apresentação dos dados filtrados em painéis com as principais fontes identificadas na busca.

+++ Possibilitar a exportação das informações identificadas nos formatos CSV, JSON, bem como a geração de relatórios em PDF;

+++ Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte;

+++ A integração deve ser realizada por meio de API Rest;

+++ Deverá identificar a emissão de certificados para domínios monitorados e de nomes similares a termos ligados à ANA;

+++ Deverá identificar a criação de domínios monitorados e de nomes similares a termos pré-definidos e configuráveis;

+++ Realizar o monitoramento de marcas, por palavras-chave definidas, na internet;

+++ A solução deverá ser capaz de analisar imagens para identificar abuso de marca, a partir de modelos fornecidos pela ANA;

+++ As ocorrências devem possuir um campo de descrição em que os analistas possam contextualizar as informações associadas;

+++ O serviço deverá realizar a detecção de domínios registrados que possam oferecer, no mínimo:

+++ Riscos de serem utilizados de forma maliciosa, variações comuns de nome, permutações de caracteres e outros (typosquatting, nomes de domínios similares);

+++ Descoberta de páginas de phishing ativas utilizando o nome, a marca e a identidade visual e seu conglomerado;

+++ Capacidade de detecção de páginas de phishing por quaisquer meios disponíveis;

+++ Validar domínios suspeitos em repositórios de phishing.

+++ Deverá fornecer coleta de informações para realização de pesquisas em redes sociais e aplicativos, para, no mínimo: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, IRC, Pastebin, Scribd, ReclameAQUI, Apple Store, 4Shared, Google Play, Vimeo e Github;

+++ Deverá, previamente à contratação, possuir métodos de coleta de redes sociais, páginas, portais e fóruns na internet superficial, profunda e oculta ("clear web", "deep web" e "dark web");

+++ Informar anomalias nos registros de nomes dos domínios monitorados ("whois", registros DNS, etc.);

+++ Monitorar as BINs de cartões de crédito da ANA, mediante lista que será enviada pós contratação;

+++ Realizar a análise de áudio de no mínimo 1 plataforma de mensagens, caso identifique correspondência com os critérios pesquisados, fazer a transcrição de áudio;

+++ Na transcrição dos áudios analisados nos vídeos, deverá ser possível destacar informações relevantes de acordo com os ativos digitais definidos pela ANA;

+++ O áudio (completo), bem como seus metadados, onde foi encontrado algum resultado, deve ser capturado, identificado e disponibilizado para análise;

+++ Realizar análise de conteúdo de imagens (OCR);

+++ Identificar, disponibilizar e possibilitar a análise de trechos anteriores e posteriores dos textos capturados, sendo possível identificar a origem e o desdobramento do(s) assunto(s) pesquisado(s), de acordo com as necessidades da ANA;

+++ Atuar de forma efetiva, no mínimo, com os aplicativos WhatsApp, Telegram, Discord e IRC;

+++ Possuir foco no Brasil com fontes relevantes relacionadas a grupos de fraudadores do sistema financeiro brasileiro;

+++ Permitir a inclusão e o monitoramento de novos grupos dos aplicativos de mensageria;

+++ Extrair, no mínimo, os seguintes metadados de cada mensagem: autor, aplicativo de origem e data e hora, com precisão de segundos, dos momentos de envio e coleta;

+++ Atuar de forma efetiva, no mínimo, com Twitter, Instagram, Youtube e Facebook;

+++ Monitorar, no mínimo, a rede de compartilhamento de textos Pastebin e a plataforma de compartilhamento de códigos Github e Bitbucket;

+++ A CONTRATADA deverá manter total sigilo e confidencialidade dos serviços prestados à ANA no que se refere a não divulgação, por qualquer forma, de toda ou parte das informações ou documentos a ele relativos, e aos quais venha a ter acesso, em decorrência da prestação dos serviços executados;

+++ Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de sites maliciosos, sites que contenham phishing ou sites/domínios que disparem phishing que utilizem o nome, a marca ou a imagem, mesmo que similar (com intuito de confundir), os clientes da CONTRATADA;

+++ Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de perfis falsos de funcionários (Executivos) e da própria empresa em redes sociais;

+++ Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis que violem os direitos de uso da ANA ou que permitam burlar os meios de proteção desses direitos;

+++ Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer tipos de informação disponíveis e acessíveis quando for identificada a tentativa de ataque a reputação da instituição ou ainda a tentativa de captura de credenciais da ANA;

+++ Possibilitar a realização do serviço de TAKEDOWN para retirada do ar de quaisquer informações em redes sociais (Facebook, Twittter, Linkedin, Instagram, YouTube etc. que tenham relação com a ANA e não seja autorizado por essa instituição;

+++ Possibilitar a realização do serviço de TAKEDOWN para retirar das principais lojas de aplicativos para mobile (Google Play Store, Apple Store, etc.) os aplicativos falsos e maliciosos distribuídos fora das lojas oficiais comumente conhecidas;

+++ Possibilitar a realização do serviço de TAKEDOWN para retirar conteúdo com documentos, informações confidenciais, informações de cartões de crédito, divulgações relacionadas a produtos e sistemas da ANA, divulgações relacionadas a clientes e empregados da ANA, além do monitoramento de sites de compartilhamento de arquivos e informações, sites de compartilhamento de textos (Pastebin, Ghostbin, entre outros) presentes na internet superficial;

+++ A plataforma disponibilizada pela CONTRATADA deve oferecer conexão segura através do protocolo HTTPS;

+++ A plataforma deve permitir realizar a abertura de chamados a partir de um evento;

+++ A CONTRATADA deve possuir mecanismos próprios que realizem a monitoração das principais Redes Sociais (Facebook, Twitter, Linkedin, Instagram, YouTube, etc.) e lojas de aplicativos para Smartphones (Google Play Store e Apple Store);

+++ A CONTRATADA deve prover serviço de monitoramento de domínios nacionais e internacionais, incluindo TLDs e gTLDs, que verifique a utilização do uso indevido da marca da ANA no nome do domínio ou na URL cadastrada, contendo o domínio/URL cadastrado, a empresa que administra o registro do domínio, e os dados proprietário do domínio;

+++ A CONTRATADA deverá acatar novas palavras-chave, listas de palavras, desde que estejam no contexto da mesma área de negócio da ANA sempre que demandados pela ANA para elaboração dos parâmetros de busca a serem executados;

+++ A CONTRATADA deverá emitir um alerta, atualizado conforme andamento, para acompanhamento do processo de TAKEDOWN de cada ocorrência;

+++ A CONTRATADA deverá disponibilizar um painel para consulta e análise de ocorrências (em andamento e finalizadas) do serviço de TAKEDOWN. Deve permitir consultas por intervalo de tempo, tipos de ocorrências e demais critérios relevantes na análise das ocorrências;

8. FERRAMENTA(S) DE APOIO PARA SERVIÇO DE CONSCIENTIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

Requisitos da ferramenta para funcionalidade de solução educacional contra-ataque de pishing:

+++ A solução deve possuir sua própria estrutura de envio de e-mails (Servidores SMTP), não onerado os recursos do CONTRATANTE para o envio dos e-mails de simulação;

+++ A solução deve possuir suporte a inserção de usuários em lote através de arquivo CSV ou similar, permitindo ainda a separação dos usuários em grupos;

+++ A solução educacional contra-ataque de Phishing deve ser capaz de criar templates educacionais exclusivos para o CONTRATANTE, em português com a logo marca do CONTRATANTE;

+++ A solução educacional contra-ataque de Phishing deve possibilitar na visão do usuário atacado a inserção de dados, no entanto, sejam eles quais forem os dados não devem ser armazenados de nenhuma forma, em nenhuma área de armazenamento, sejam internas a solução quanto externa;

+++ A solução educacional contra-ataque de Phishing deve ser capaz de, durante a criação do e-mail template customizado para o CONTRATANTE, conter no mínimo as parametrizações abaixo:

--------> Seleção de usuário e de grupo de usuários que farão parte da simulação;

--------> Seleção de agendamento com data e horário para início e fim de cada campanha de conscientização, especifica por grupo a ser atingido;

--------> Definição de assunto do e-mail de simulação do ataque Phishing;

--------> Definição do nome do remetente que enviará o e-mail de simulação do ataque Phishing; Definição do endereço (usuário e domínio) do e-mail de simulação do ataque Phishing.

+++ A solução deve possibilitar o uso de variáveis de ambiente, que permitam incluir individualmente no corpo do e-mail conteúdos dinâmicos, para no mínimo:

--------> Nome do usuário;

--------> Sobrenome;

--------> Endereço de e-mail;

+++ A solução educacional contra-ataque de Phishing deve ser capaz de criar relatórios executivos e mostrar de forma gráfica no console do produto no mínimo:

--------> Verificação de quantas simulações foram enviadas para o CONTRATANTE;

--------> Verificação de quantos usuários acessaram o e-mail de simulação de ataque Phishing;

--------> Verificação de quantos usuários abriram o arquivo anexo do e-mail de simulação de ataque Phishing;

--------> Verificação de quantos usuários inseriram os dados solicitados no e-mail de simulação de ataque Phishing; Verificação de quantos usuários reportaram para a área de TI a existência de um ataque Phishing;

--------> Verificação de quantos usuários executaram os módulos de conscientização educacional Anti-Phishing;

+++ A solução educacional contra-ataque de Phishing deve ser capaz de construir uma mensagem de conscientização, informando que usuário foi pego em uma simulação de ataque Phishing, a qual deve ser mostrada no momento que seja caracterizado como se o usuário estivesse realmente sofrido um ataque;

+++ A solução educacional contra-ataque de Phishing deve ser capaz de indicar a necessidade de o usuário participar de uma campanha para conscientização, a partir da mensagem de conscientização

(item anterior) na qual deverá existir um link direcionando para a campanha indicada para o usuário e grupos de usuários;

+++ A solução educacional contra-ataque de Phishing deve ser capaz de apresentar de forma gráfica o progresso na conscientização dos usuários, executando gráficos comparativos entre campanhas já realizadas pela ferramenta, onde poderá ser observado o declínio e a ascensão na maturidade e conscientização do CONTRATANTE.

9. FERRAMENTA(S) DE APOIO PARA SERVIÇOS DE TESTES DE INVASÃO (Pentest)

As ferramentas de apoio serão aquelas que habilitem a execução dos serviços de pentest de uso da contratada, desde que gere os produtos requeridos.
