ANEXO III
REQUISITOS FUNCIONAIS NOC / SOC

1. ESPECIFICAÇÕES TÉCNICAS - NOC (Network Operations Center)

1.1. Compreende os serviços prestados pela CONTRATADA de disponibilização de ambiente de monitoração da infraestrutura de TI e exibição de métricas interativas.
1.2. Promover a customização do ambiente de monitoração infraestrutura de TI e exibição de métricas interativas para que possa se adequar à identidade visual da CONTRATANTE como logotipo, cores, etc.
1.3. Definir e criar os usuários administradores e usuários padrão (operação).
1.4. Executar ajustes de desempenho do ambiente (tuning) de infraestrutura da SOLUÇÃO.
1.5. Definir métricas e indicadores que serão utilizados para o monitoramento do desempenho e disponibilidade do ambiente de monitoração da infraestrutura de TI e exibição de métricas interativas e suas integrações.
1.6. Integrar os alarmes definidos junto ao console do ambiente de monitoração da infraestrutura de TI e exibição de métricas interativas.
1.7. Implantar rotinas de expurgo com housekeeping.
1.8. Os serviços demandados deverão incluir, mas não se limitando, as seguintes atividades:
1.9. Construção e customização de novos templates do ambiente de monitoração da infraestrutura de TI e exibição de métricas interativas.
1.10. Automatização de tarefas, orquestrando e hierarquizando os serviços, envolvendo dados da infraestrutura de TI, através de scripts escritos em linguagem de programação Python, Ansible e uso da API da infraestrutura de TI.
1.11. A Criação da arvore de serviços deve ser estruturada através de automações para subsequente cálculo de SLA.
1.12. Na apuração do SLA deve ser possível identificar a origem das indisponibilidades para notificação.
1.13. Suporte a desenvolvimento de scripts para coleta de dados e construção de monitoramento externo no da infraestrutura de TI.
1.14. Evolução do dashboards customizados das métricas interativas.
1.15. Provisionamento de ambiente de monitoração da infraestrutura de TI e exibição de métricasinterativas e outras ferramentas em nuvem pública.
1.16. Integrações entre da infraestrutura de TI e exibição de métricas interativas e outras ferramentasutilizando a API da aplicação e API's Rest de outras aplicações, ou ainda agentes próprios.
1.17. Automatização de processos e orquestração de instalações e configurações utilizando a ferramenta Ansible ou compatível.

2. Especificação Técnica Serviços Gerenciados de Segurança da Informação – SOC

2.1. Deverá prestar Serviços Gerenciados de Segurança da Informação, incluindo Serviços de Administração, Operação e Atendimento a Requisições, Gestão e Respostas de Incidentes N1, Monitoramento e Visibilidade de ataques Cibernéticos, Atividade de inteligência de ameaças (Threat hunting):
2.1. Serviços Gerenciados de Segurança da Informação é um conjunto de serviços pela qual a empresa a ser contratada presta serviços de segurança, incluindo a administração e operação das ferramentas de segurança do ambiente e de outras ferramentas a serem disponibilizadas pela CONTRATADA.
2.3. As ferramentas devem ser sustentadas em Nuvem de maneira a causar impacto mínimo no ambiente monitorado, salve engano a instalação de agentes de coleta, integrações por API ou repasse de syslogs, para que possam coletar as informações e processá-las em servidores em nuvem, que por sua vez deve estar hospedada em nuvem nacional respeitando assim as normalizações vigentes.

2.4. Os itens de 1 a 6, descritos na tabela 01 a seguir envolvem:

Descrição detalhada do Objeto		
Item	**Descrição**	**Periodicidade/ Frequência**
1	Serviço de administração, operação e manutenção e atendimento a requisições, para sustentar e operar todas as soluções e produtos de segurança da CONTRATANTE, bem como, a realização permanente de ações proativas (gap analysis) voltadas para a segurança do parque computacional do CONTRATANTE com o objetivo de mantê-lo estável, seguro, disponível e íntegro durante 24horas e sete dias por semana.	Rotineiro
2	Serviço de gestão de incidentes de segurança (Blue Team), para analisar, remediar, conter e documentar os eventos de segurança da informação que foram transformados em um incidente de segurança da informação, obedecendo os principais frameworks de gestão de incidentes de segurança da informação e boas práticas de mercado.	Rotineiro
3	Serviço de monitoramento e visibilidade de ataques cibernéticos tem como objetivo o monitoramento continuo 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 que possam gerar eventos de segurança da informação, aos quais devem ser analisados, podendo estes serem transformados em um incidente de segurança da informação, conforme definido em processo de gestão de incidentes.	Rotineiro
4	Serviço de Inteligência de ameaças pró-ativa com o objetivo de descobrir, mitigar e tratar ameaças potencialmente danosas para o ambiente do CONTRATANTE de maneira antecipada através de descoberta própria.	Roteineiro

2.5. As soluções acima descritas devem obrigatoriamente conter as seguintes tecnologias:
2.6. SIEM (Security Information and Event Management).
2.7. Deve-se trata-se de uma solução de segurança cibernética que integra a coleta, análise e correlação de informações e eventos de segurança de diversos dispositivos e sistemas em uma única plataforma centralizada. O objetivo principal de um SIEM é fornecer visibilidade abrangente das atividades dede segurança em uma rede, permitindo a detecção e resposta eficazes a ameaças em tempo real. A solução deve incluir agentes instalados em dispositivos e sistemas de rede para coletar registros de eventos em tempo real ou ainda ser capaz de importar LOGs de interesse através de APIs ou ainda instrumentos analogos a um syslog. Esses registros devem ser transmitidos para um repositório centralizado em Nuvem, onde serão armazenados e normalizados para permitir a análise e correlação eficientes. O SIEM deve ser totalmente customizável e de código aberto.
2.8. SOAR (Security Orchestration, Automation, and Response) Trata-se de uma plataforma que permite a automação e orquestração de tarefas de segurança cibernética estando intimamente relacionado a um SIEM, pois complementa e estende as funcionalidades deste último. O SOAR deve ser projetado para agir sobre eventos levantados pelo SIEM de forma automatizada, coordenando as atividades de resposta a incidentes. Ele fornece recursos avançados de automação e fluxo de trabalho para ajudar as equipes de segurança a lidar com incidentes de forma mais rápida, eficiente e consistente.
2.9. Inteligência de Ameaças (Threat Intell) Refere-se ao processo de coleta, análise e disseminação de informações relevantes sobre ameaças cibernéticas. O objetivo principal é fornecer insights valiosospara auxiliar na proteção e defesa de sistemas, redes e dados contra ataques maliciosos. A ameaça de inteligência deve obrigatoriamente envolver a coleta de dados de várias fontes, como feeds de dados públicos, compartilhamento de informações entre organizações, análise de malware, fóruns especializados, comunidades de segurança e outras fontes especializadas. Esses dados devem ser analisados e contextualizados para identificar tendências,

padrões e comportamentos de ameaças, bem como para entender as motivações e táticas dos adversários cibernéticos.

2.10. Deve ainda agregar e normalizar dados de várias fontes, permitindo a análise e correlação eficiente de informações de ameaças. Elas podem fornecer alertas e indicadores de comprometimento (IOCs) relevantes para ajudar as equipes de segurança a identificar e responder a ameaças.

2.11. Servidor Honeypot Descreve-se como um servidor HoneyPot um sistema projetado para simular vulnerabilidades e atrair potenciais atacantes, com o objetivo de monitorar e estudar suas técnicas, táticas e intenções, onde, deve-se criar um ambiente falso e a configuração de serviços e serviços de rede com vulnerabilidades conhecidas. Esses serviços podem ser sistemas operacionais, aplicativos, serviços de rede, entre outros, que são propositadamente deixados desatualizados ou com configurações inseguras. Para que quando um atacante interagir com o servidor HoneyPot, ele acreditar estar atacando um sistema real. O servidor HoneyPot obrigatoriamente deve, registrar e monitorar todas as atividades realizadas pelo atacante, capturando informações sobre seus métodos de ataque, técnicas utilizadas, ferramentas empregadas e outras informações relevantes ao âmbito da segurança cibernética suficientes para proteger o ambiente monitorado.

- Cloud

- Portal de gerenciamento disponibilizado via web (SaaS);
- Área de auditoria para acompanhar acessos e alterações dos Administradores;
- Plugin para Auto-download e auto-updating do cliente instalado;

- On-premise

- Ter a possibilidade de ter toda a infraestrutura de gerenciamento e provisionamento dos serviços sendo executadas em infraestrutura local caso seja necessário;

- Enterprise Browser

- O browser corporativo deverá ser parte da solução de ZTNA como produto único sendo gerenciado na mesma console sendo uma funcionalidade de um produto único;
- A solução deve fornecer um navegador corporativo, Chromium-based, proprietário para garantir a segurança do acesso;
- Deve fornecer gestão sobre o cache local da navegação;
- Deverá fornecer console de controle centralizado;
- Deverá possuir mecanismo para controle, aprovação e bloqueio de extensões instaladas no navegador;
- Deverá restringir o acesso a download de arquivos de acordo com políticas de segurança definidas;
- Deverá restringir o acesso aos mecanismos de copiar e colar definidos de acordo com as políticas de segurança definidas;
- Deverá incluir marca d'água customizável informando o usuário, ip e outras informações que identifiquem o usuário que está acessando;
- Deverá fornecer mecanismos anti-keylogging para proteger contra ameaças de roubo de senhas;
- Deverá fornecer mecanismo que evite a captura de tela de acordo compolíticas de segurança definidas pelo administrador;
- Fornecer acesso adaptativo para interface mobile quando aplicações forem acessadas via celular;
- App mobile deverá suportar IOS e Android;
- SSO integrado.

- Private Access Agent

- Fornecer agente para acesso as aplicações sem a necessidade de utilizar um IP público para as aplicações;

- Endpoint Analisys (EPA)

- Verificar se determinado processo está em execução antes de liberação de acesso;
- Verificar determinados valores em chave de registro (REGEDIT) como condição para acesso;
- Verificar versões de Sistema Operacional como condicionante para liberação dos acessos as aplicações;
- Verificação de MAC Address como condicionante para o acesso;
- Verificação de certificado no dispositivo para validação do acesso;
- Verificação de encriptação de HD como condicionante ao acesso;
- Criar área de quarentena para clientes que falharam na varredura do endpoint para acesso limitado as aplicações que permitam que o usuário esteja compliance com a política criada;

- Analytics Security

- Permitir inserir pontuação de risco dinâmica baseado em estado de ameaça do dispositivo;
- Criar políticas de bloqueio de acesso baseado em pontuação de risco;
- Incluir dispositivos em área de observação para acompanhar comportamento;
- Criar políticas baseada na geo-localização do dispositivo;
- Permitir a criação de relatórios customizáveis com dados coletados;
- Toda a infraestrutura, manutenção e atualização dos serviços deverão ser ofertados na modalidade SaaS para a gerenciamento do ambiente.
- Oferecer mecanismos baseados em Machine Learning para auto-remediação e identificação de ameaças e risco.