



RFP – Request for Proposal

Página 1 de
58

Contratação RFP OSS/BSS

Edição
Versão 3.0

Data:
15/07/26

RFP

Diretoria de Operações
Redes Privativas do Governo

Requisitos OSS/BSS
Rede Privativa do Governo

	RFP – Request for Proposal	Página 2 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

1.	Descrição do Projeto da Rede Privativa de Governo	4
2.	Ecosistema da Telebras	6
3.	Requisitos das Ferramentas/Soluções de OSS/BSS.....	8
3.1.	Lote – SOAR / SIEM / NMS_Observabilidade / PAM / TACACS+ / NAC / SYSLOG.....	9
4.	Condições Gerais.....	50
5.	Serviços Previstos.....	55



RFP – Request for Proposal

Página 3 de 58

Contratação RFP OSS/BSS

Edição
Versão 3.0

Data:
15/07/26

TERMOS E ABREVIações:

TERMO	DEFINIÇÃO NO CONTEXTO DA RFP OSS/BSS
OSS	Operations Support Systems
BSS	Business Support Systems
SOAR	Security Orchestration, Automation and Response
SIEM	Security Information and Event Management
PAM	Privileged Access Management
IAM	Identity and Access Management
TACACS+	Terminal Access Controller Access-Control System Plus
NAC	Network Access Control
SYSLOG	System Logging Protocol
CMDB	Configuration Management Database
NMS	Network Management System
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
WAF	Web Application Firewall
DAM	Database Activity Monitoring / Observabilidade de Dados
ITSM	IT Service Management
AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
SNMP	Simple Network Management Protocol
DHCP	Dynamic Host Configuration Protocol
LDAP	Lightweight Directory Access Protocol
SAML	Security Assertion Markup Language
SSO	Single Sign-On
RBAC	Role-Based Access Control
MFA	Multi-Factor Authentication
TLS	Transport Layer Security
IPSec	Internet Protocol Security
SSH	Secure Shell
RDP	Remote Desktop Protocol
SFTP	Secure File Transfer Protocol
SMB	Server Message Block
VNC	Virtual Network Computing
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
DNS	Domain Name System
ICMP	Internet Control Message Protocol
CVE	Common Vulnerabilities and Exposures
OWASP	Open Worldwide Application Security Project
XSS	Cross-Site Scripting
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
CLI	Command Line Interface
GUI	Graphical User Interface
MSSP	Managed Security Service Provider
ROI	Return on Investment
SOC	Security Operations Center
AD	Active Directory
MTA	Mail Transfer Agent
OUI	Organizationally Unique Identifier
ONVIF	Open Network Video Interface Forum
NetFlow	Protocolo de monitoramento de fluxos de rede
EAP-PEAP	Protected Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol – Transport Layer Security
RADIUS	Remote Authentication Dial-In User Service
CSV	Comma-Separated Values
JSON	JavaScript Object Notation
HTML	HyperText Markup Language
JS	JavaScript

	RFP – Request for Proposal	Página 4 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

1. Descrição do Projeto da Rede Privativa de Governo

- a) Esse capítulo tem o objetivo de contextualizar a **PROPONENTE** sobre a Rede Privativa de Governo, Fixa e Móvel, a qual será integrada à gerência da rede existente da Telebras, no que tange ao escopo de OSS/BSS, necessitando de ferramentas/soluções de gerenciamento de rede e sistemas, escopo dessa RFP.
- b) A Rede Fixa Privativa terá atendimento de até 6.500 pontos nas Capitais em dupla abordagem, com capacidade de atendimento conforme a necessidade de banda do usuário (1Gbps, 10Gbps e 100Gbps) não se limitando a estas bandas, utilizando interfaces ETHERNET, GPON e XGS-PON. A rede fixa será implementada em todas as 26 capitais do Brasil e o Distrito Federal, utilizando o backbone da TELEBRAS bem como a sua estrutura de fibra óptica já lançada nas capitais, sendo esta nova rede um complemento da rede existente.

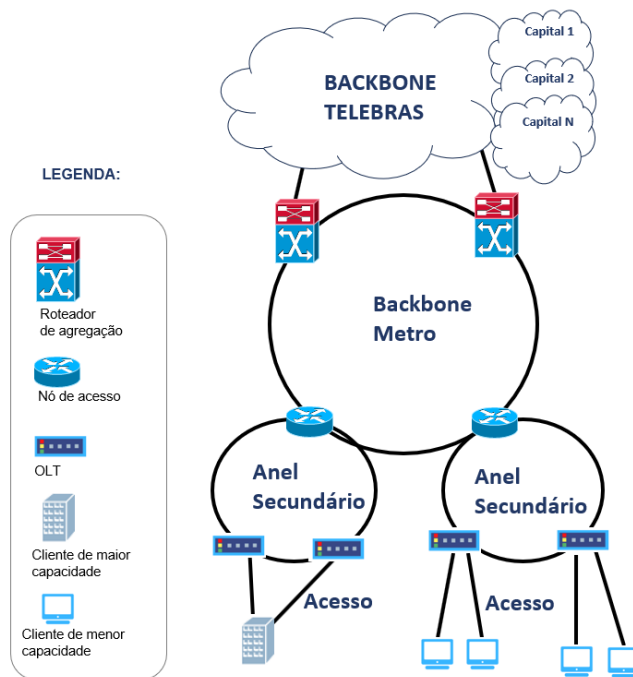


Figura 1 - Arquitetura da Rede Fixa

- c) A rede de transporte será formada por roteadores e switches interconectados em anéis redundantes de fibra óptica, a fim de prover a comunicação entre a rede fixa de acesso e o backbone de dados da TELEBRAS.



- d) A rede SD-WAN será formada utilizando elementos da rede de transmissão implementada pela EAF e/ou rede de transmissão existentes de outras operadoras, como redes móveis (4G/5G), satélite, rede fixa etc. Tais elementos serão gerenciados por um elemento orquestrador de hierarquia superior instalado em um datacenter centralizado visando prover o uso mais eficiente dos recursos disponíveis da rede.

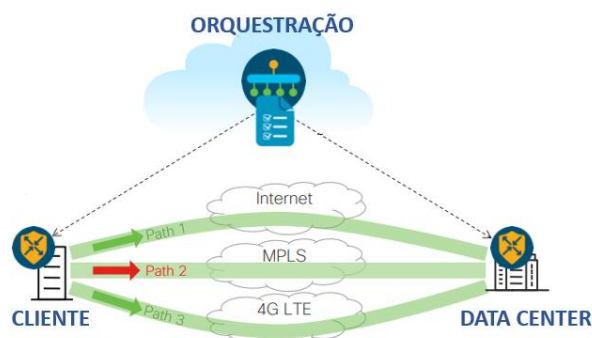


Figura 2 - Arquitetura da Rede SD-WAN exemplificando a utilização dos up-links

- e) **Atendimento de pontos fora das capitais** – além dos pontos nas capitais, que fazem parte da Rede Privativa, serão instalados encriptadores em pontos dentro e/ou fora das capitais, visando ampliar a proteção na rede dos clientes. Nesses pontos fora das capitais, o encriptador será inserido na rede do cliente e deve funcionar de forma agnóstica ao tipo de rede. Abaixo a topologia para o atendimento fora das capitais:

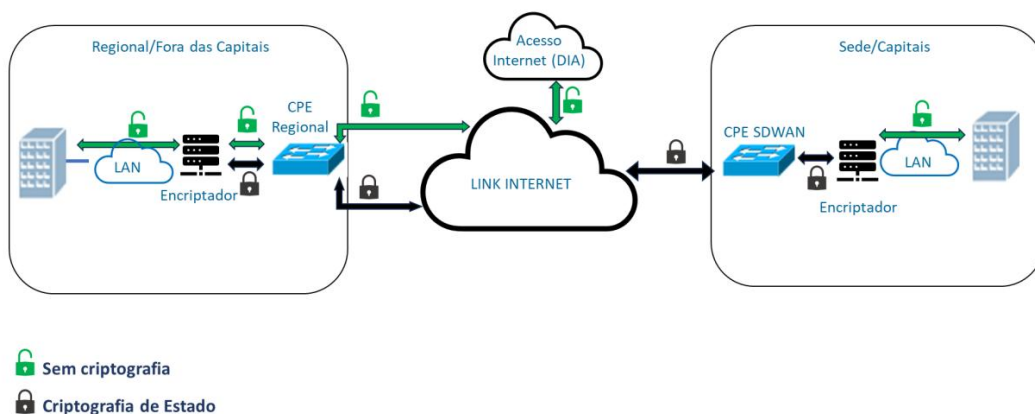


Figura 3 – Topologia para atendimento com encriptadores fora das capitais

- f) Equipamentos implantados no ecossistema Telebras, da **Rede Fixa Privativa do Governo Federal**:
- f.1. Nutanix NX-8155A-G9 NCI
 - f.2. Firewall FortiGate Modelo FG-1001F
 - f.3. Nutanix NX-8155-G9 NUS
 - f.4. Taishan 2280
 - f.5. **Roteador**: Huawei NetEngine 8000 M8 / 8000 F8 / ATN 910-D
 - f.6. **Switch**: CloudEngine S6730-H / S5731
 - f.7. **OLT**: SmartAX MA5800-x2 / MA5800-x7 / MA5800-x15
 - f.8. **SDWAN** : FortiGate FG-1001F / FG-401F / FG-101F / FG-40F

	RFP – Request for Proposal	Página 6 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- g) A **rede móvel de comunicação crítica do Governo Federal** consiste na implantação de um CORE 4G/LTE e de uma plataforma de comunicação crítica (**MCX**), para uso das forças de segurança e defesa do Distrito Federal, com capacidade para atender até 150 mil usuários móveis, onde 31,5 mil são usuários de MCX de missão crítica;
- h) Topologia ilustrativa prevista para **Rede Móvel Privativa do Governo Federal**, com o MCX:

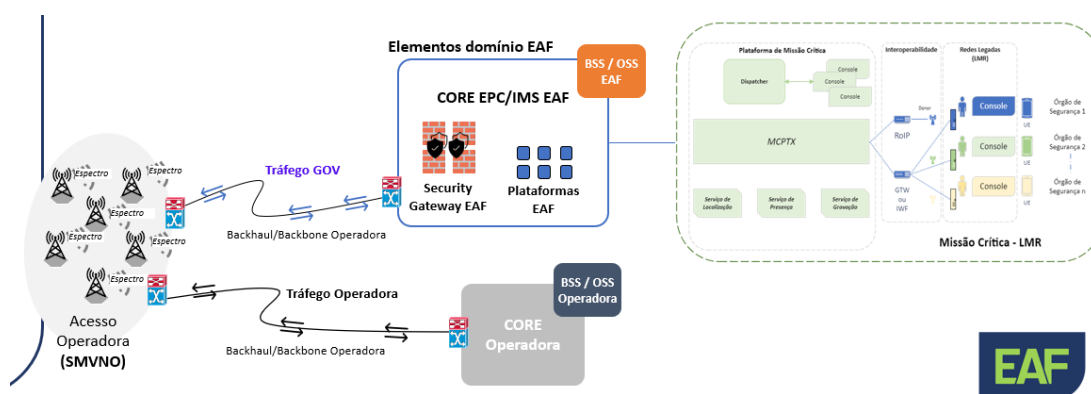


Figura 4 – Topologia prevista da Rede Móvel Privativa do Governo Federal

- i) Equipamentos implantados **até o momento** no ecossistema Telebras, da Rede Móvel Privativa do Governo Federal:
- i.1. **Servidores** : DELL PowerEdge R760 / R360
 - i.2. **Switch** : Extreme Networks 8520 / 5520-48T / Juniper EX4100
 - i.3. **Firewall** : Palo Alto PA-1410 / Juniper SRX345 / FortiGate 101E /
 - i.4. **VMware**: vSphere FND 8.0
- j) Para ambas as redes, Fixa e Móvel, estão sendo usados os datacenters, operados pela Telebras: o principal tier 4 no COPE-P (Distrito Federal) e o redundante geográfico tier 3 no COPE-S (Rio de Janeiro);

2. Ecossistema da Telebras

- a) Esse capítulo tem o objetivo de disponibilizar à PROPONENTE informações sobre o ecossistema existente da Telebras, devendo ser consideradas pela PROPONENTE na sua resposta a essa RFP de OSS/BSS.
- b) A PROPONENTE deverá informar se as suas ferramentas/soluções de OSS/BSS ofertadas, estarão atendendo o ecossistema da Telebras, indicando no seu escopo de fornecimento, a necessidade ou não de:
 - b.1. fornecimento de novas ferramentas/soluções de OSS/BSS;
 - b.2. serviços de integração;
 - b.3. substituição;
 - b.4. atualização de uma ou mais ferramentas/soluções de OSS/BSS da Telebras.

	RFP – Request for Proposal	Página 7 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

c) Composição da infraestrutura atual da Telebras:

c.1. **Rede:**

- a. CISCO N5K-C5548UP, N7K-C7010
- b. SAN: Dell EMC Connectrix B-Series DS-6620B,
- c. ACESSO: Switches Dell - N2048P

c.2. **Segurança:**

- a. Checkpoint NGEN, Arbor Anti-DDoS, CA-PAM, TACACS+ (CISCO PRIME), Fortinet SDWAN/NGFW/Manager/Analyzer/Authenticator

c.3. **Backup/Storage:**

- a. PureStorage FlashArray, EMC VMax, Veeam, Exagrid EX84 e EX52

c.4. **Servidores/Computação:**

- a. Dell R640, Dell R940, Dell R610, Dell R570, CISCO UCS-B200-M3

c.5. **Virtualização:**

- a. VMWare vSphere ESX

c.6. **Ferramentas de OSS/BSS:**

- a. BSS: SAP, SAP-CRM, Portal de Clientes.
- b. OSS: CPQD OSS (OM, ITSM, GP), Netbox, Zabbix, Grafana, GLPI.
- c. Segurança: CA-PAM, TACACS+, MS AD (ENTRA ID)

	RFP – Request for Proposal	Página 8 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

3. Requisitos das Ferramentas/Soluções de OSS/BSS

a) Os requisitos das ferramentas/soluções da presente RFP estão divididos em um lote específico de atendimento, devendo a PROPONENTE apresentar proposta completa de fornecimento de ferramentas e/ou soluções de OSS/BSS para todos os itens do lote;

b) O escopo principal dessa RFP é composto pelas ferramentas/soluções de OSS/BSS, descritas abaixo:

SOAR / SIEM / NMS_Observabilidade / PAM / TACACS+ / NAC / SYSLOG

c) Todas as soluções ofertadas deverão ser no modelo de **licenciamento on-premise**;

d) Arquitetura prevista para atendimento ao escopo de ferramentas/soluções de OSS/BSS, conforme figura 5 abaixo, meramente ilustrativa:

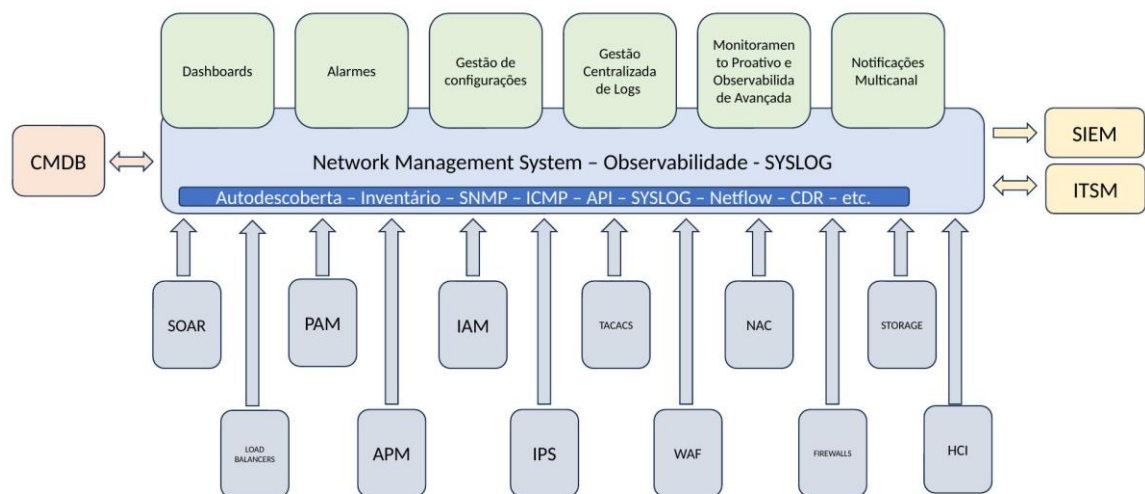


Figura 5: Arquitetura com **Front-end Único** (Observabilidade)

	RFP – Request for Proposal	Página 9 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- e) Arquitetura de Referência e Alta Disponibilidade – as plataformas centrais (gerência, orquestração, correlação, coleta, logs e portais) deverão ser implantadas nos dois data centers:
- e.1. **COPE-P** (primário, Brasília) e **COPE-S** (secundário, Rio de Janeiro) – deverá ser implementada uma arquitetura em alta disponibilidade geográfica entre os dois data centers, em modelo ativo/ativo ou ativo/passivo, com failover automático e mínimo impacto ao acesso dos usuários;
 - e.2. A alta disponibilidade deverá ser implementada entre os Data Centers COPE-P e COPE-S para os componentes centrais e de gerência de cada ferramenta/solução de OSS/BSS, tais como console, coletores, correlação, orquestração e servidores de política/AAA, contemplando, quando aplicável, replicação e sincronização de configurações e sessões entre as instâncias localizadas nos dois Data Centers. Não é requerida redundância ou alta disponibilidade adicional entre componentes dentro de um mesmo Data Center, salvo quando expressamente estabelecido requisito específico no item correspondente da solução. Os elementos controlados ou monitorados (endpoints) não são objeto de alta disponibilidade, mas sim os serviços que os gerenciam;
 - e.3. Para as plataformas com atuação em linha ou enforcement local (por exemplo, IPS e NAC), o enforcement na localidade deverá continuar operante mesmo em caso de perda temporária de comunicação com o núcleo central;
 - e.4. A cadeia de coleta (SYSLOG/agente de dados) deve operar com failover automático entre os coletores integrados à licença da solução, com uma fila persistente (armazenar e encaminhar) para o caso de indisponibilidade temporária do destino por no máximo 4 horas;
 - e.5. O tráfego de gerência entre componentes distribuídos e o núcleo central deverá ser autenticado e criptografado (TLS ou IPSec), em segmento lógico isolado do tráfego de dados;
 - e.6. A solução deverá permitir atualização centralizada de produtos e conteúdos (assinaturas, versões), inclusive para componentes sem acesso direto à internet (on-premises/air-gapped);
 - e.7. A comprovação de alta disponibilidade e failover integrará a etapa de aceitação de cada ferramenta/solução de OSS/BSS.
- f) Especificamente, esse documento abrange:
- f.1. Descrição dos requisitos relativos ao escopo desta RFP;
 - f.2. Os equipamentos e softwares para fornecimento de ferramentas/soluções de OSS/BSS, funções de suporte, interfaces e arquitetura.
 - f.3. Serviços de suporte à solução, incluindo garantia, manutenção e suporte até L3.
 - f.4. Requisitos de suporte operacional, operação assistida, incluindo peças de reposição, logística, suporte a serviços gerenciados e transferência de competências.
 - f.5. Desenvolvimento de documentação operacional para práticas melhores recomendadas, incluindo processos, troubleshooting e runbooks detalhados.

3.1. Lote – SOAR / SIEM / NMS_Observabilidade / PAM / TACACS+ / NAC / SYSLOG

	RFP – Request for Proposal	Página 10 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- a.1. A Proponente deverá ofertar na sua proposta técnico comercial, o atendimento para todas as ferramentas/soluções pertencentes ao lote de Segurança e Automação;
 - a.2. A Proponente deverá descrever a configuração mínima de capacidade e dimensionamento, para atendimento ao ecossistema atual da Telebras e a rede privativa de governo;
 - a.3. A Proponente deverá descrever detalhadamente os steps de crescimento seguintes à configuração mínima, descrita no item anterior, contemplando o ecossistema existente e a rede privativa de governo;
 - a.4. As soluções de SOAR, SIEM, PAM e NAC deverão ser do fabricante Fortinet. As demais soluções deverão possuir integração nativa, plena e comprovada com o ecossistema Fortinet, garantindo interoperabilidade, gestão integrada e adequada comunicação entre os componentes, considerando que a presente contratação constitui uma ampliação do ambiente atual de Cibersegurança da Rede Fixa Privativa do Governo Federal;
 - a.5. As soluções disponibilizadas exclusivamente em software poderão ser implementadas no atual ambiente de gerenciamento e virtualização Nutanix, desde que comprovadamente compatíveis com a infraestrutura existente, atendam integralmente aos requisitos técnicos e de segurança estabelecidos e não ocasionem impactos, indisponibilidade ou degradação no desempenho e na operação da Rede Fixa Privativa do Governo Federal.
- i. **SOAR (Security Orchestration, Automation and Response):** Plataforma de cibersegurança, que integra diferentes ferramentas de segurança, automatiza tarefas repetitivas e reduz o tempo de resposta da equipe de operações, com informações consistentes a incidentes e ameaças;
- a. **Requisitos de Gerenciamento**
 1. Alertas e incidentes devem ser tratados separadamente, cada um em seu próprio módulo na interface do usuário;
 2. Atributos de cada módulo (Campos), como nome, gravidade, do módulo Alerta, deve ser personalizável para que os usuários possam adicioná-los ou removê-los, além disso os usuários devem poder criar, modificar e excluir seus próprios atributos personalizados em qualquer módulo do sistema;
 3. A solução deve permitir que cada registro seja correlacionado e vinculado a qualquer outro registro no sistema, incluindo tipos personalizados de registros que os próprios usuários definam;
 4. A solução deve fornecer a capacidade de agregar registros semelhantes com base em valores de campo semelhantes;
 5. A solução deve ter um mecanismo de previsão baseado em aprendizado de máquina, que prevê valores de campos com base em dados históricos. O escopo da previsão de aprendizado de máquina deve abranger todos os módulos do produto, incluindo os built-in (como alertas, incidentes indicadores) e personalizados;
 6. A solução deve incluir um recurso de detecção de e-mail de phishing baseado em IA;
 7. O sistema deve fornecer uma funcionalidade de pesquisa global que permita ao analista pesquisar palavras-chave em todo o sistema e em todos os módulos;
 8. A interface Web para o usuário deve oferecer a possibilidade de vincular vários registros a um ticket ou criar novos registros juntos e vinculá-los ao ticket atual. Os registros podem ser, mas não limitados a: Artefatos, Tarefas, Sala de Guerra, Usuários, Campanhas, Buscas, Ativos, Alertas, Anexos, E-mails e Incidentes;



9. Os tickets devem ter um atributo de prioridade que possa ser usado para classificá-los enquanto os exibe na interface do usuário da Web;
10. O escalonamento de tickets deve ser possível manualmente por meio da interface Web ou automaticamente por meio de um fluxo de trabalho de automação, que pode aplicar qualquer lógica como condição anterior ao escalonamento do ticket;
11. Deve incluir um gerenciamento de crises da sala de guerra para permitir a colaboração entre equipes durante as crises. A sala de guerra deve poder ser criada manualmente ou escalando um ticket T1 ou T2;
12. Tickets, artefatos, anexos e módulos customizados devem dar aos analistas um meio de comunicar por texto (comentários) cada mensagem deixada por um analista, ou um workflow de automação deve permanecer como atributo do registro onde foi criado. Além disso, os comentários devem suportar as funcionalidades abaixo:
 - a. Os comentários podem ser texto simples ou rich text
 - b. Um comentário pode ser usado para executar ações
 - c. Comentários são compatíveis com tags genéricas
 - d. Os comentários suportam anexos de arquivos
 - e. Comentários são compatíveis com **RBAC** (Role-Based Access Control – Controle de Acesso Baseado em Funções)
13. O sistema deve permitir que o analista execute a Análise de Causa Raiz com uma média de correlação gráfica;
14. A correlação gráfica deve estar disponível para diferentes tipos de registro, como ativos, vulnerabilidades, alertas e incidentes;
15. A solução deve se integrar ao framework MITRE ATTACK fornecendo enriquecimento tático, análise de ameaças, investigação de incidentes e sugestões de remediação;
16. O sistema deve permitir que o analista realize a Análise Pós-Incidente (PIA – relacionada ao tratamento de incidentes);
17. O sistema deve suportar tíquetes de mapeamento para fases da cadeia de morte cibernética;
18. A solução deve ter um recurso de gerenciamento de filas personalizável que ofereça suporte a atribuições automatizadas de alertas/incidentes/tarefas para vários grupos de usuários;
19. A solução deve oferecer suporte a um sistema de rastreamento conforme o Acordo de Nível de Serviço, configurável dentro da estrutura de gerenciamento de caso para que o tempo de conclusão de vários marcos possa ser identificado e relatado;
20. O gerenciamento de casos deve oferecer suporte a anexos de arquivo;
21. A solução deve ser capaz de extrair artefatos (IP, URL, Domínio) de mais de 1550 tipos de arquivos, incluindo MS Office e PDFs.
22. Os artefatos extraídos devem estar vinculados ao registro do arquivo de onde foram extraídos;
23. A solução deve ser capaz de extrair metadados de arquivos (autor, timestamp) juntamente com uma visualização de conteúdo como texto ou HTML de mais de 1550 tipos de arquivos, incluindo MS Office e PDFs;
24. A solução deve permitir que o analista edite campos diretamente na WebUI se o RBAC estiver configurado para permitir tal ação, respeitando as permissões de acesso e mantendo os registros de auditoria das alterações realizadas;
25. As notificações devem ser flexíveis e usar vários canais, como interface do usuário, e-mail e várias integrações com serviços de conferência, como MS Teams e Slacks;
26. Filas de emissão de bilhetes, gerenciamento de turnos e entrega devem ser um recurso integrado. A solução deve fornecer um sistema de filas onde os analistas são designados com base em sua disponibilidade (turno);



27. Deve permitir que os usuários definam condições para controlar a visibilidade dos objetos na interface do usuário. Isso não está relacionado à filtragem de registros, mas às condições de exibição para objetos de páginas específicas, como guias;
28. Solução deve criar uma linha do tempo automática para alertas e incidentes e salas de guerra (no mínimo), de forma a permitir visualizar os eventos relacionados em uma linha de tempo;
29. Para um alerta, incidente, indicador, o sistema deve mostrar correlações. Para um alerta, deve-se apresentar indicadores, informações do Mitre, características do alerta, conteúdo do alerta, anexos (se possuir), SLA do alerta, possibilidade de escalar para Incidente, dentre outros;
30. Solução deve permitir a construção de WarRooms (salas de guerra) para gestão de casos críticos de ataques cibernéticos. A sala de guerra deve permitir atribuir tarefas aos seus integrantes, monitorar alertas e fatos ligados ao ataque, monitorar SLA e linha do tempo de ações da sala de guerra, permitir colaboração por intermédio de Zoom, slack, Teams ou outros métodos populares;
31. Solução deve permitir reduzir a quantidade de falsos positivos, permitindo maior eficiência operacional ao SOC;

b. Requisitos de **Workflows de Automação** do SOAR

1. O número de playbooks fornecidos pelo fornecedor, incluindo casos de uso, amostras e outros relacionados a conectores, deve ser superior a 4.500 (quatro mil quinhentos);
2. Os playbooks devem ser agrupados em pastas com a capacidade de exportar ou importar a pasta inteira de playbooks diretamente da WebUI;
3. Os playbooks devem ter propriedades que permitam que determinados playbooks sejam executados antes de outros na fila com base em sua importância;
4. Os playbooks devem ter acionadores condicionais, portanto, os playbooks não serão acionados a menos que condições específicas sejam atendidas;
5. Os operadores abaixo devem ser suportados:
 - a. Igual
 - b. Não igual
 - c. Menor que/Menos que ou igual
 - d. Maior que/menor que ou igual
 - e. Está na lista
 - f. Não está na lista
 - g. É nulo
6. Os playbooks devem ser compatíveis com os seguintes acionadores:
 - a. Manual: o analista pode executar um playbook manualmente a partir da WebUI;
 - b. No registro Criar/Atualizar/Excluir: quando um registro (Alerta, indicador, incidente) é criado ou modificado;
 - c. Via API: quando o SOAR recebe uma solicitação HTTP com parâmetros específicos, ele executa um playbook específico;
 - d. Referenciado: um playbook deve poder ser executado por outro playbook fornecendo seus parâmetros necessários;
7. O sistema deve fornecer uma interface gráfica do usuário para o designer de playbook, onde os usuários podem usar o mouse para arrastar e soltar componentes no designer. Além disso, o designer do playbook deve conter um painel assistente para buscar todas as variáveis disponíveis e um painel utilitário para ajudar o analista a manipular os dados dentro do playbook;



8. O designer do playbook deve permitir que o analista reverta e refaça ações, portanto, se uma etapa for criada, por exemplo, uma reversão excluiria a ação e um "refazer" a traria de volta;
9. A solução deve permitir que o usuário execute o playbook de dentro do playbook designer e teste sua execução com registros do ambiente ou o último registro com o qual o playbook foi executado;
10. Os analistas devem ter a capacidade de exportar e importar playbooks individualmente, incluindo várias versões do playbook;
11. A solução deve suportar a criação, modificação e exclusão de variáveis globais acessíveis por todos os playbooks. As variáveis globais devem ser editáveis por meio de playbooks ou por meio da WebUI;
12. O sistema deve fornecer um histórico visual de execução do playbook que identifica a saída, entrada e configuração de cada etapa;
13. O nível de log dos playbooks deve ser configurável globalmente (todo o sistema) e localmente para cada playbook;
14. As ferramentas de depuração devem estar disponíveis, prontas para uso no designer do playbook. O depurador deve ser capaz de usar dados da execução anterior do playbook ou dados fornecidos pelo analista;
15. O **RBAC** deve abranger playbooks e fluxos de trabalho de automação;
16. A solução deve fornecer mensagens de erro detalhadas quando a execução de um playbook falhar e permitir a reinicialização do playbook a partir da etapa em que o o mesmo falhou;
17. As etapas de decisão dentro dos playbooks devem ser flexíveis o suficiente para acomodar condições complexas, incluindo aquelas com aritmética, comparação e operadores lógicos, como listados abaixo:
 - a. Igual (Compara dois objetos para igualdade)
 - b. Não igual (Compara dois objetos para desigualdade)
 - c. Maior que (verdadeiro se o lado esquerdo for maior que o lado direito)
 - d. GT/igual (verdadeiro) se o lado esquerdo for maior ou igual ao lado direito)
 - e. Menos do que (verdadeiro se o lado esquerdo for mais baixo que o lado direito)
 - f. Menor ou igual (verdadeiro se o lado esquerdo for menor ou igual ao lado direito)
 - g. "E" (Retorna verdadeiro se os operandos esquerdo e direito forem verdadeiros)
 - h. "Ou" (Retorna verdadeiro se o operando esquerdo ou direito for verdadeiro)
 - i. Não (negar uma declaração)
 - j. Adição (Adiciona dois objetos juntos)
 - k. Subtração (Subtraia o segundo número do primeiro)
 - l. Divisão (Divida dois números)
 - m. Módulo (Calcular o resto de uma divisão inteira)
 - n. Multiplicação (Multiplique o operando esquerdo pelo direito)
 - o. potência (Elevar o operando esquerdo à potência do operando direito)
18. Condições como:
 - a. $(\text{Variável1} + \text{variável2}) / 2 > \text{variável3}$
 - b. $((\text{Variável1} + \text{variável2}) / 2 > \text{variável3})$ ou $(\text{Variável4} / \text{variável5}) < 2$
19. Deve ser possível utilizar os operadores condicionais sem usar qualquer linguagem de programação explícita;
20. Em relação aos operadores condicionais, a etapa de tomada de decisão deve ter uma opção para definir uma próxima etapa padrão caso, todas as condições falhem;
21. Os playbooks devem ser chamados de outros playbooks;
22. Os analistas devem ser capazes de usar a linguagem de programação Python com pelo menos formatação automática e destaque de sintaxe diretamente em um playbook, caso desejem.



23. O administrador da solução SOAR deve ser capaz de limitar os módulos que podem ser usados nos scripts python;
24. A solução deve oferecer suporte ao gerenciamento de conflitos de registros e permitir que os usuários selecionem quais campos podem ser substituídos;
25. A solução deve fornecer um editor de Rich text em sua WebUI para permitir que os analistas editem texto formatado com tabelas, imagens e vídeos;
26. As etapas do playbook devem ser configuráveis para interromper a execução do playbook se ocorrer um erro no nível da etapa ou passar a mensagem de erro para a próxima etapa e continuar;
27. O gerenciamento de playbooks deve permitir que os analistas editem playbooks em massa, com a capacidade de executar as funções abaixo:
 - a. Alterar status (Playbook Ativo ou Desativado)
 - b. Clone o(s) playbook(s) selecionado(s)
 - c. Mover o(s) playbook(s) selecionado(s) para um grupo diferente
 - d. Alterar o nível de registro para o(s) playbook(s) selecionado(s)
 - e. Exportar o(s) playbook(s) selecionado(s)
28. Qualquer playbook dentro da solução proposta deve ser escalonável para ser executado em um intervalo específico, com a capacidade de impedir sua execução se uma instância anterior ainda estiver em execução;
29. Dentro do designer de playbook, os analistas devem ser capazes de:
 - a. Clonar uma etapa
 - b. Copiar/Colar uma etapa ou um grupo de etapas no mesmo playbook ou em um diferente
 - c. Alinhar as etapas em um diagrama vertical ou horizontal
 - d. Selecionar uma etapa ou um grupo de etapas e excluí-los
30. Os playbooks devem ser capazes de obter dados e aprovações por e-mails com a capacidade de realizar uma ação específica se ocorrer um tempo limite;
31. Solução deve permitir o versionamento de Playbooks;
32. Solução deve permitir trocar as prioridades de playbooks;
33. Solução deve permitir pesquisar histórico de playbooks executados, assim como obter KPIs de quantidade de playbooks executados, número de ações executadas;
34. Solução deve suportar a construção automática de playbooks por inteligência artificial. Por exemplo, analista cibernético pede para IA criar playbook que faça enriquecimento de um IP, levando em consideração fontes X, Y e Z e, então, a IA gera o playbook, que pode depois ser modificado pelo analista;
35. Solução deve ser capaz de sugerir playbooks para serem executados para remediar ameaças detectadas em alertas e incidentes, usando inteligência artificial;
36. Solução deve permitir a execução de simulações de ataques, a fim de monitorar a forma como o time do SOC responde a incidentes;
37. A solução deve permitir instalar cenários de simulação diversos, além de poder executá-lo inúmeras vezes;
38. Solução deve fazer a triagem automática de alertas, seguindo com o enriquecimento de indicadores extraídos, além de potencialmente mudar a severidade dos alertas em decorrência da gravidade detectada a partir de seu conteúdo (tudo de forma automática);
39. Solução deve permitir diminuir o MTTR (Mean Time to Response) através de playbooks pré-configurados para resposta;
40. Os playbooks podem ser ativados por sistemas externos a solução através de API segura;
41. Solução deve ter suporte a playbooks que solicitam aprovação em certo passo/etapa para continuar com os próximos passos;



42. Solução deve permitir Playbooks que referenciam outros playbooks (playbooks aninhados).

c. Requisitos de **Licenciamento** do SOAR

1. O licenciamento deve ser baseado no appliance e no número de usuários e não no número de playbooks ou em qualquer outra métrica operacional;
2. A licença deve suportar usuários simultâneos, independentemente de quantos usuários sejam criados no sistema;
3. A solução deve suportar licenciamento quando implantada em redes air-gapped (isolamento físico);
4. A solução deve ter uma licença de teste que possua limitações, mas não a tempo, deve ser gratuita, podendo ser utilizada para fins de desenvolvimento;
5. O Playbook Editor deve permitir que os usuários criem vários grupos recolhíveis de etapas e notas para melhorar a legibilidade;
6. Os playbooks devem oferecer suporte a uma etapa de espera configurável com uma quantidade de tempo definida ou uma condição que, se atendida ou um tempo limite configurável atingido, o playbook encerrará a espera e prosseguirá para a próxima etapa;
7. A solução deve fornecer um portal de conteúdo público e de dentro de sua interface de usuário da Web para baixar e consumir componentes do produto, tais como:
 - a. Painéis
 - b. Relatórios
 - c. Playbooks
 - d. Widgets personalizados
 - e. Integrações (conectores)
 - f. Módulos e extensões do produto
8. A solução deve permitir integrações com sistemas de terceiros, como por exemplo, soluções de **SIEM**, serviços de inteligência de ameaças e firewalls, em atendimento ao ecossistema da Telebras e a rede privativa de governo;
9. O sistema deve ter um mecanismo de atualização de conteúdo in-life independente das atualizações de firmware da solução. As integrações com sistemas de terceiros devem ter suas próprias atualizações, utilizáveis em qualquer versão suportada do firmware da solução;
10. A interface do usuário da Web deve incluir assistentes para auxiliar os usuários na criação de conteúdo, seja esse conteúdo uma integração, uma extensão de produto ou um widget personalizado;
11. Cada integração deve ser documentada online;
12. O sistema deve fornecer um assistente de entrada de dados amigável para configurar os dados de sistemas de terceiros.

d. Requisitos de **Integração/Conteúdo**

1. O sistema deve fornecer um painel de integridade que indica se todas as integrações com os sistemas de terceiros estão íntegras;
2. As ações dos conectores devem estar sujeitas ao RBAC, portanto, apenas perfis definidos podem usar ações definidas;
3. O sistema deve permitir que o analista execute qualquer ação do conector por meio do **SOAR** WebUI sem usar fluxos de trabalho de automação (playbooks);
4. A solução deve fornecer um assistente para auxiliar os usuários na criação de suas integrações personalizadas, ao mesmo tempo em que todas as integrações existentes devem ser editáveis via WebUI sem precisar usar um IDE externo;



5. A solução deve permitir a instalação local de novas integrações;
6. Solução deve permitir ao analista ter múltiplas configurações para um mesmo conector. Por exemplo, para o conector do Firewall do vendor 1 é possível ter múltiplas configurações, pois para cada Firewall pode-se ter credenciais/API diferentes de acesso (informações utilizadas pelos playbooks);
7. Cada conector deve vir acompanhado de uma documentação, que explique casos de uso e detalhes da instalação dos conectores;
8. A solução deve permitir ao analista construir seus conectores (caso a solução ainda não disponibilize conectores que o analista deseje);
9. A solução já deve trazer conectores prontos para uso, no mínimo, para os seguintes tipos de appliances/soluções: Network and Firewall Products, Ticket Management, Log management and SIEM, Vulnerability Management, Endpoint Security, Threat Intelligence Feeds, DevOps, Cloud providers, Sandboxing, Email e Email Security, soluções de Incident Investigation, soluções de Big Data Analytics, Web Security, Threat Detection, Identity Management, Soluções de bancos de dados;
10. A solução deve se integrar com os SIEM líderes de mercado: IBM Qradar, Splunk FortiSIEM, ArcSight (ou nome mais novo), LogRhythm, RSA Netwitness, Rapid7;
11. A solução deve poder importar Processos de Fluxos de Trabalho (workflows) de soluções padrão de mercado, tipo Flowable, Camunda e Signavio (no mínimo);
12. A solução deve poder enviar mensagens de Syslog para elementos externos com informações sobre saúde, playbooks, execução de sistemas internos;

e. Requisitos de **Inteligência de Ameaças** (Threat Intelligence)

1. O fabricante da solução deve fornecer seu próprio serviço de inteligência de ameaças, operando nativamente com o SOAR proposto;
2. A solução deve ter um módulo de gerenciamento de inteligência de ameaças que inclua um painel de informações de ameaças com estatísticas sobre: Feeds ativos, observáveis de alta confiança, fontes de feed;
3. Integração com várias dezenas de fontes CTI;
4. Os feeds de ameaças devem mostrar seus dados correlacionados com outros indicadores, a estrutura MITRE (organização norte-americana sem fins lucrativos, que gerencia centros de pesquisa e desenvolvimento financiados pelo governo dos EUA), e as solicitações de inteligência de prioridade. Além disso, cada indicador deve ter um widget gráfico de correlação que indica graficamente todos os relacionamentos;
5. O gerenciamento de caso deve permitir que os analistas levantem a solicitação de requisito de Inteligência de prioridade para indicadores desconhecidos. As tarefas devem ser criadas para rastrear a solicitação. A solução deve fornecer uma estrutura que permita que os analistas respondam com um relatório abrangente de ameaças para o PIR levantado;
6. A solução deve atuar como serviço de Inteligência de Ameaças para sistemas de terceiros, onde coleções ou indicadores específicos podem ser buscados do SOAR por SIEMs, EDRs e NGFWs via TAXII e CSV sobre HTTP;
7. Deve ser possível importar e exportar indicadores em massa diretamente da WebUI;
8. A solução deve ser flexível o suficiente para permitir a reputação de indicadores de computação com base em dados de várias fontes de Threat Intelligence;
9. Solução deve permitir a partir de um alerta ou indicador, abrir um PIR (Priority Intelligence Requirement) para o time de Threat Intelligence;

	RFP – Request for Proposal	Página 17 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

10. Solução deve permitir a criação de datasets a partir do conjunto de IOCs monitorados. Por exemplo, filtrar e exportar dataset relacionado com Comando e Controle e Botnets;

f. Requisitos de **Deployment & Architecture**

1. A solução deve permitir backup e restauração da configuração e dos dados do sistema;
2. A solução deve ter a capacidade de criar módulos (subsistemas) de produtos personalizados a partir da GUI da web, permitindo gerenciar um novo tipo de registro, como: Alertas, Incidentes e indicadores;
3. O sistema deve ser escalável e resiliente, permitindo o agrupamento de vários nós (mais de 2) em uma configuração Ativa/Ativa;
4. A solução deve ter um proxy reverso para que os componentes remotos se comuniquem com os centrais para evitar ter que publicar os componentes centrais diretamente na WAN. O proxy reverso deve suportar alta disponibilidade;
5. A solução deve oferecer uma arquitetura multilocatário escalável e geograficamente distribuída com; nós remotos no local, execução remota de playbook, gerenciamento centralizado de MSSP;
6. A solução deve permitir a execução de ações de remediação e coleta de dados na rede segmentada por meio de um agente SOAR implantado no segmento de rede remoto, os agentes devem suportar atualizações automáticas;
7. O sistema deve permitir o uso de banco de dados interno e externo;
8. A solução deve suportar integração de saída com um sistema NMS que, por padrão, monitore a lista abaixo pronta para uso (sem configuração):
 - a. CPU (Uso em %)
 - b. Disco (Uso em % para cada volume lógico e também para partição /boot)
 - c. E/S (solicitações de leitura e gravação/s para discos)
 - d. Largura de banda da placa de rede incluindo interface loopback(lo) (kb/s)
 - e. Uso de RAM (%)
 - f. NTP (Diferença entre NTP e máquina em segundos)
 - g. Servidor Web (conexões perdidas, solicitações por segundo, conexões manipuladas, etc)
 - h. Banco de dados (ativo conexões, blocos lidos do disco (blocos/min), taxa de acerto do cache do buffer (%), total de transações (tx/min)
 - i. MTA (número de solicitações, tamanho da fila do MTA)
 - j. Expiração da licença SOAR
 - k. Expiração dos certificados SOAR
 - l. Saúde dos conectores configurados SOAR (para cima/para baixo)
 - m. SOAR Playbook fila
9. A solução deve permitir que múltiplos tenants sejam coordenados por um ponto central, permitindo ao cliente atuar como MSSP;
10. A solução deve permitir a comunicação segura entre seus elementos;
11. A solução deve permitir a criação de filas de trabalho e organização de turnos e camadas de analistas (N1, N2, N3). A atribuição de alertas e incidentes aos analistas pode ser feita por um gestor ou de forma automática pela solução;

g. Requisitos de **Auditoria**

1. O sistema deve fornecer uma trilha de auditoria de todo o sistema, abrangendo tanto o sistema (login, logoff, instalações) como eventos de dados (criação de registro, atualização e exclusão);



2. O sistema deve permitir o encaminhamento de eventos para um servidor de log ou solução SIEM. Os protocolos a seguir devem ser compatíveis com um nível de log configurável:
 - a. UDP
 - b. TCP, TCP/TLS
 - c. RELP, RELP/TLS
 3. O sistema deve manter um widget de cronograma de registro de auditoria, rastreando cada evento de registro com detalhes de cada alteração.
- h. Requisitos de **Gerenciamento de Usuários** (USER MANAGEMENT & RBAC)
1. O sistema deve fornecer controle de acesso baseado em função (RBAC) granular e flexível. Os administradores devem poder definir os direitos de acesso para cada tipo de registro em um nível de campo. Por exemplo, o endereço IP de origem é um campo;
 2. A solução deve suportar o gerenciamento de relacionamento de grupos de usuários, onde um grupo deve ser capaz de herdar o escopo de acesso de um grupo ou grupos diferentes em uma hierarquia pai, irmão, filho e que deve ser possível que cada nível superior tenha acesso ao inferior;
 3. A solução deve permitir a colaboração entre analistas através de buscas compartilhadas, comentários em alertas e incidentes, entre outros métodos;
 4. A solução deve permitir autenticação através de autenticação de dois fatores (MFA);
 5. A solução deve permitir autenticação externa de usuários usando LDAP, SAML (SSO).
- i. Requisitos de **Dashboards**
1. A solução deve fornecer vários painéis configuráveis que se integram ao RBAC com controle de acesso por função;
 2. A solução deve fornecer um mecanismo para destacar alertas que estão se aproximando de violações de SLA;
 3. O painel deve exibir informações específicas do analista, como alertas e tarefas atribuídas ao analista;
 4. Deve ser possível importar e exportar modelos de painel;
 5. A solução deve fornecer painéis focados em funções, como; analista de nível 1, analista de nível 2, gerente de SOC;
 6. A solução deve medir métricas de SOC, relevantes, como tempo médio para identificação, confirmação, contenção, erradicação, recuperação. Deve ser possível ainda exibir essas métricas em um painel;
 7. A solução deve suportar configurações de Dashboards em Tenants específicos em um ambiente Multi Tenancy;
 8. A solução deve ter um painel dedicado para monitorar o status de integridade/disponibilidade de cada integração e também a integridade do sistema do próprio SOAR;
 9. A solução deve dar suporte à identidade visual da GUI para diferentes Tenants;
 10. A solução deve fornecer uma estrutura de desenvolvimento de painel baseada em HTML/JSON/JS para permitir que os usuários criem seus widgets de painel personalizados e os importem para a solução SOAR;
 11. A solução deve ter suporte a Inteligência Artificial Generativa, permeando os módulos da solução. Analista deve ser capaz de fazer perguntas, requerer sugestões, interagir com a Inteligência artificial;
 12. A solução deve permitir ao analista criar novos módulos e customizar dashboards;



13. A solução deve possuir sistema de Ajuda, que permite ao analista ou usuário tirar dúvidas. Além disso, a solução deve ter disponível documentação completa, incluindo como construir playbooks, conectores, como customizar o dashboard, como gerenciar a força de trabalho do SOC, como configurar a solução;
14. A solução deve permitir monitorar a saúde do sistema através de dashboard específico para essa função;
15. A solução deve trazer dashboard com métricas (KPIs) de segurança e eficiência do SOC (tempo salvos com playbooks, retorno do investimento);
16. Os dashboards devem permitir auto-refresh;
17. Todas as ações da solução devem ser feitas na mesma interface (não desejamos duas interfaces / sistemas distintos);

j. Requisitos de **Relatórios e Notificações**

1. A solução deve fornecer relatórios gráficos personalizados;
2. Deve ser possível agendar relatórios para serem executados em um horário definido pelo usuário;
3. Os relatórios devem estar disponíveis em formato PDF ou CSV;
4. Deve ser possível enviar relatórios programados para um destinatário de e-mail;
5. A solução deve permitir um controle programático dos relatórios, para que um analista possa criar um playbook para automatizar o processo de geração dos mesmos;
6. O acesso à funcionalidade de relatório deve ser controlado pela função RBAC;
7. A solução deve ter uma trilha de auditoria que identifique a atividade do relatório, incluindo download do mesmo;
8. Deve ser possível incluir uma variedade de gráficos e métricas em relatórios personalizados;
9. Além da exportação automatizada de registros por meio de playbooks, a interface do usuário deve ter um meio que permita aos usuários baixar alguns/todos os registros para sua estação de trabalho;
10. A solução permite customizar Email Templates que são enviados pelo time de SOC;
11. A solução deve ter flexibilidade para envio de notificações externas;

- ii. **SIEM** (Security Information and Event Management): Plataforma que gerencia as informações de segurança (SIM) e os eventos de segurança (SEM). É uma solução de software que coleta, centraliza e analisa logs e eventos de segurança em tempo real, permitindo que a operação identifique e responda rapidamente a ameaças digitais;

a. Requisitos de **Arquitetura de Implementação**

1. A solução deverá permitir a implementação de maneira distribuída ou em um único servidor;
2. A arquitetura da solução permite com que seus componentes possam ser instalados em redes IPv4 e IPv6;
3. A implementação em único servidor deverá permitir a utilização de armazenamento de eventos local ou através de servidor NFS;
4. A solução deverá permitir o aumento da capacidade de processamento de EPS através da adição de novos servidores;



5. A solução deverá possuir coletores para coleta de logs e informações de performance em sites remotos;
6. A solução deve possuir a capacidade de encaminhar qualquer evento recebido em tempo real, nos formatos syslog e netflow;
7. A solução deverá suportar a filtragem dos dados coletados no nível de aplicação, identificando endereço IP, tipo do dispositivo e tipo do evento;
8. A solução deverá permitir que todos os seus componentes sejam virtualizados;
9. A solução deverá suportar a virtualização nos seguintes Hypervisors: VMware ESX, Hyper-V e KVM;
10. A solução deverá permitir Failover e Disaster Recovery em ambiente físico e virtual;
11. A solução pode ser implementada nas seguintes nuvens:
 - a. Azure
 - b. Amazon

b. Requisitos de **MULTI-TENANCY**

1. A solução deverá suportar implementação em ambiente distribuídos;
2. As descobertas efetuadas devem, por padrão, atrelar novos dispositivos automaticamente à empresa/departamento/localidade a qual pertencem;
3. A solução deverá permitir o monitoramento de elementos mesmo quando houver sobreposição de IP's (overlapping);
4. A solução deverá permitir a alocação mínima (garantida) de EPS por organização, bem como alocar EPS dinamicamente entre organizações caso um número excessivo e inesperado de EPS seja recebido.;
5. A solução deverá suportar a definição de uma quantidade máxima de devices por organização;
6. A solução deverá permitir a criação de logins de gerenciamento limitados à uma ou mais organizações, definindo níveis de privilégio para cada.
7. A solução deverá possuir coletores Multi-tenant, permitindo assim pelo menos as seguintes formas de configuração/implementação:
 - a. Multi-tenant Agents;
 - b. Multi-tenant Event Pulling;
 - c. Multi-tenant Collector Pool.

c. Requisitos de **Gerenciamento**

1. A solução deverá permitir ser gerenciada através de interface gráfica Web;
 - a. Deve permitir alteração de idioma de sua interface para Português
2. A solução deverá permitir o controle de acesso granular limitando o acesso a interface gráfica e a diversos níveis de dados;
3. A solução deverá permitir a autenticação de usuários administrativos através dos seguintes diretórios: Local, Microsoft Active Directory, LDAP, Single Sign On and SAML via OKTA;
4. Toda a comunicação entre os módulos deverá ser feita através de HTTPS;
5. A solução deverá permitir a auditoria completa da atividade de usuários do SIEM;
6. Para fins de resolução de problemas, a solução deve possuir ferramentas que permitam: iniciar e parar processos individuais, executar shutdowns e reboots, validar métricas de performance do SIEM e exportar informações de evento em CSV;
7. A solução deverá permitir a visualização de usuários que estiverem logados no sistema, atividades de consulta de usuários e usuários bloqueados;d



8. A solução deverá permitir o backup e recuperação de arquivos de configuração e conteúdo;
9. A solução deverá permitir a atualização dos componentes da solução através de interface gráfica ou através do próprio sistema operacional via linha de comando;
10. A respeito da capacidade em Eventos por Segundo (EPS), se o número de EPS recebido atingir o limite da licença, o SIEM deverá automaticamente gerar um incidente. Deverá ser capaz de receber um número de EPS 10% superior a quantidade de EPS licenciados por um período de até 3 minutos sem descartar nenhum evento;
11. A solução deverá permitir a especificação de um limite de EPS por coletor;
12. A solução deverá permitir a utilização de um túnel SSH reverso para fins de depuração de algum problema;
13. A solução deverá possibilitar o monitoramento da saúde dos coletores exibindo as seguintes informações:
 - a. Nome da Organização onde coletor está instalado
 - b. Nome do Coletor
 - c. Endereço IP
 - d. Status
 - e. Tempo em Operação (uptime)
 - f. Utilização de CPU e Memória
 - g. Versão
 - h. EPS Alocados
 - i. EPS Processados
14. A solução deverá suportar a administração centralizada em uma implementação geograficamente distribuída onde todos os componentes são monitorados e gerenciados a partir de um portal centralizado;
15. A solução deverá permitir a visualização da utilização de licenças através da interface gráfica com, pelo menos, as seguintes informações: dispositivos, EPS e agentes;
16. A solução deverá permitir o arquivamento de dados baseado em políticas;
17. A solução deve permitir o “hashing” de logs em tempo real para o não repúdio e verificação de integridade;
18. A solução deverá possuir compatibilidade e integração através de APIs documentadas e homologadas pelo fabricante, com pelo menos 30 soluções de segurança do mercado, com intuito de complementar a capacidade de análise de atividade maliciosa e resposta a incidentes;
19. A solução deverá prover uma console e visão intuitiva para realizar investigações sobre os dados;
20. A solução deverá possuir a capacidade de navegação contínua sobre os dados em formato “drill down”, sem a obrigatoriedade de realizar pesquisas avançadas;
21. A solução deverá permitir a criação e customização de regras, alertas, gráficos e relatórios na própria interface;
22. A solução deverá permitir o agendamento automático e manual de relatórios, com a possibilidade de envio por email;
23. O fabricante da solução deverá possuir ampla experiência em malwares, assim como possuir seu próprio centro de pesquisa e desenvolvimento e inteligência às novas ameaças;
24. A solução deverá 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;
25. A solução deverá possuir integração aberta com soluções de análise de malware;

	RFP – Request for Proposal	Página 22 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

26. A solução deverá possuir capacidade nativa de gestão de centro de operações de segurança e rede (Security Operations Center – SOC e Network Operations Center) na mesma aplicação;
27. A solução deverá possuir mecanismo de auditoria através da geração de logs das atividades realizadas no console de gerência e investigação;
28. A solução deverá possuir suporte ao framework MITRE ATT&CK, com pelo menos as seguintes características:
 - a. Capacidade de associar uma técnica MITRE a uma regra FortiSIEM (integrada ou personalizada)
 - b. Possuir pelo menos 950 regras integradas para detectar uma ampla variedade de técnicas MITRE
 - c. Capacidade de atribuir técnicas e táticas às regras e pesquisar incidentes por técnicas e táticas
 - d. Possuir Dashboard que exibe regras associadas a uma tática ou técnica
 - e. Possuir Dashboard que exibe incidentes associados a uma tática ou técnica

d. Requisitos de **Coletores**

1. A solução deverá possuir coletores para a obtenção de eventos em sites remotos;
2. A solução não poderá restringir o número de coletores utilizados através de licença;
3. O coletor deverá suportar a instalação em Hypervisor VMware ESX ou diretamente em Bare Metal;
4. O coletor deverá possuir a capacidade de coletar os dados, realizar “parsing”, compressão e envio através de HTTPS;
5. O coletor deverá ser capaz de realizar o armazenamento local das informações caso não haja conectividade com o SIEM. Não deverá haver restrição de tempo para o armazenamento, desde que haja disponibilidade de espaço em disco;
6. A solução deve permitir a atualização dos coletores através da interface gráfica do SIEM.

e. Requisitos de **AGENTES**

1. A solução deverá permitir a utilização de agentes para a coleta de informações mais detalhadas de servidores Windows e Linux;
2. A solução com o agente para Windows deverá ser capaz de coletar as seguintes informações:
 - a. Windows Security Logs
 - b. Windows Application Logs
 - c. Windows System Logs
 - d. Windows DNS Logs
 - e. Window DHCP Logs
 - f. IIS logs
 - g. DFS logs
3. A solução deverá monitorar:
 - a. Integridade de Arquivos
 - b. Mudança de Software Instalado
 - c. Mudança no Registro
 - d. Arquivos
 - e. Saída WMI
 - f. Saída de Power Shell

	RFP – Request for Proposal	Página 23 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

4. A solução deverá, adicionalmente, analisar logs DNS do Windows para incluir IP de Origem, Nome do Destino, IP de Destino, Nome canônico do destino e bytes recebidos;
5. Durante a atualização do agente é evitada a perda da Configuração do Agente no Gerenciador de Agentes do Windows;
6. Limpeza automática de arquivos .SVC quando atinge um determinado tamanho;
7. A solução é capaz de executar verificações de certificado SSL;
8. Possuir capacidade de liberar arquivos de log durante a rotação de arquivos de um arquivo monitorado;
9. Agente Avançado para Linux:
 - a. Sistema de Coleta (Alto Desempenho), Logs de aplicativos e logs de segurança.
 - b. Monitoramento de Integridade de Arquivos.
 - c. Monitoramento de arquivo de log do cliente
10. O agente deverá suportar os seguintes sistemas operacionais, nas versões listadas abaixo, e versões superiores :
 - a. Windows 7, 8, 10 e 11
 - b. Windows Server 2008 R2
 - c. Windows Server 2012
 - d. Windows Server 2012 R2
 - e. Windows Server 2016
 - f. Windows Server 2019
 - g. Windows Server 2022
 - h. Amazon Linux 1
 - i. Amazon Linux 2
 - j. CentOS 7
 - k. CentOS 8
 - l. CentOS 9
 - m. CentOS Stream 8
 - n. CentOS Stream 9
 - o. Debian 10
 - p. Debian 11
 - q. Debian 12
 - r. Oracle Linux 8
 - s. Oracle Linux 9
 - t. Red Hat Enterprise Linux 7
 - u. Red Hat Enterprise Linux 8
 - v. Red Hat Enterprise Linux 9
 - w. Ubuntu 14.04, 16.04, 18.04 LTS, 20.04 LTS, 22.04 LTS e 24.04 LTS
 - x. SUSE Linux Enterprise Server (SLES) 12
 - y. SUSE Linux Enterprise Server (SLES) 15
 - z. Google Chrome
11. Os agentes deverão ser gerenciados por uma aplicação central;

	RFP – Request for Proposal	Página 24 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

12. O agente para Windows poderá ser gerenciado diretamente pela console GUI da solução, dispensando assim a necessidade de um gerenciador central;
13. Os agentes deverão encaminhar logs para a aplicação de gestão dos agentes através da porta TCP 443;
14. O agente deverá permitir sua instalação através de GPO.

	RFP – Request for Proposal	Página 25 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

f. Requisitos de **Dashboard e Relatórios**

1. A solução deverá prover de forma padrão dashboards para monitoramento dos elementos de rede, incluindo VM's;
2. Acessando um dispositivo no dashboard, a solução deverá possibilitar visualização de informações diversas sobre eles, tais como: incidentes, disponibilidade, performance e segurança;
3. A solução deverá possibilitar a customização dos dashboards, adicionando novos widgets e a forma como são exibidos, inserção de outros devices e refresh de tela;
4. A solução deverá permitir ao administrador importar e exportar dashboards;
5. A solução deverá possuir, por padrão, os seguintes dashboards: network, server, AWS, security, NetApp, VNX, Salesforce e Office 365;
6. A solução deverá possuir um dashboard que informe o status de registro dos dispositivos PCI;
7. A solução deverá possuir mais de 2000 reports pré-definidos, envolvendo padrões como PCI, HIPAA, SOX, ISO e GLBA, dentre outros;
8. Deve permitir a criação de novos reports;
9. Por padrão, a solução deverá possuir baselines, definindo padrões de comportamento distintos para dias de semana, finais de semana e para cada hora do dia, permitindo ao operador criar alertas para eventos que fujam ao padrão;
10. A solução deverá possuir baselines de: DNS requests por cliente, tráfego de destino a servidores e de origem, conexões permitidas e negadas pelo firewall, CPU e memória por host, I/O de disco para servidores, tráfego e erros em interfaces de rede, falhas e sucesso de logon, dentre outros baselines;
11. A solução deverá permitir criar reports que associem IP's, endereços MAC, usuários de rede, máquinas e domínios a locais específicos como portas de switch, gateway VPN e controladora wireless;
12. A solução deverá possibilitar o agendamento de reports, que podem ser gerados uma única vez ou de forma recorrente, além permitir notificações quando o report for gerado e até quando ele deverá estar disponível;
13. A solução deverá permitir ao administrador da plataforma realizar auditorias sobre o bom uso dos sistemas, apontando desvios em relação ao sistema operacional utilizado, bem como software instalados nas máquinas, além de permitir especificar o fabricante dos equipamentos a serem submetidos à auditoria;
14. A solução deverá permitir exportar o report de auditoria, tanto em PDF, CSV e RTF, bem como possibilitar o agendamento;
15. A solução deverá ser possível integrar a plataforma à sistemas de Business Intelligence.

	RFP – Request for Proposal	Página 26 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

g. Requisitos de **Carregamentos de Dados**

1. Deve ser capaz de receber logs de diversos dispositivos diferentes, incluindo dados estruturados e não estruturados;
2. Deve ser capaz de receber logs de, pelo menos, 200 dispositivos diferentes sem necessidade de criação de parsers customizados;
3. Deve ser capaz de receber logs de dispositivos de segurança de rede, tais como: roteadores, switches, dispositivos de prevenção contra intrusão, web proxies, gateway de proteção de e-mail, DNS e servidores DHCP de diversos fabricantes;
4. Deve ser capaz de receber logs de sistemas operacionais de diversos fabricantes;
5. Deve ser capaz de receber logs de aplicações de segurança, tais como: servidores web, servidores de aplicações, banco de dados e sistemas de proteção de endpoints;
6. Deve ser capaz de receber logs via syslog, traps SNMP, Netflow, SFlow, JFlow, FTP e SCP;
7. Deve ser capaz de obter dados através de JDBC, JMX, Cisco SDEE e CheckPoint LEA;
8. Deve ser capaz de coletar qualquer arquivo de logs de sistemas operacionais Windows através de agente próprio;
9. Deve permitir que arquivos de log formatados em CSV personalizados possam ser carregados através da console GUI para análise mais detalhada;
10. Deve ser capaz de obter logs de aplicações Cloud através de API's específicas, tais como: Google Apps, Office 365 e Salesforce CRM;
11. Deve ser capaz de inserir contexto aos dados obtidos;
12. Deve ser capaz de realizar o parsing, armazenar, analisar e exibir conteúdo de pacotes TCP/UDP em eventos que são gerados por sistemas de prevenção de intrusão;
13. Permitir ao usuário analisar arquivos PCAP. Incluindo os atributos IP, TCP / UDP e HTTP.

h. Requisitos de **Enriquecimento de Dados**

1. Deve ser capaz de obter informações de uma variedade de fontes públicas e privada de dados para enriquecer os dados obtidos;
2. Deve fornecer uma base de dados de localização de endereços IP (GeoIP) e ser capaz de obter informações de cada endereço de IP público recebido nos eventos, sendo cada evento enriquecido com informações de localização geográfica, tais como: cidade, país, ASN, longitude e latitude;

	RFP – Request for Proposal	Página 27 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

3. Deve permitir que os administradores da solução possam pesquisar informações sobre endereços IP e reputação de domínio de qualquer website público;
4. Deve permitir o agrupamento de ativos de rede de forma automática e realizar a sua classificação através de segmento de rede, sistema operacional, aplicação e etc;
5. Deve permitir a criação de grupos customizados e regras de mapeamento;
6. Deve ser capaz de utilizar informações de serviços de DHCP e de diretório para gerar alertas e relatórios;
7. Deve ser capaz de monitorar a atividade de servidores DNS com o objetivo de detecção de malwares;
8. Possui capacidade de verificações de reputação (indicadores de comprometimento) como IP, Domínio, URL e Hash

i. Requisitos de **Classificação de Dados**

1. Deve ser capaz de classificar diferente tipos de dados coletados para auxiliar na sua utilização em consultas analíticas ou “ad hoc” por analistas do SOC. Também deve ser capaz de classificar esses dados com base em sua sensibilidade ou proteção de segurança / privacidade necessários;
2. Deve ser capaz de agrupar dados semelhantes;
3. A solução deve ser capaz de analisar o tipo do evento e atribuí-lo a um grupo de tipo de evento;
4. A solução deve possuir, pelo menos, 200 grupos de tipo de eventos incorporados;
5. Deve permitir a utilização de expressões regulares para fazer correspondência nos dados recebidos;
6. Permite a definição de tags, que podem ser usadas em regras e incidentes.

j. Requisitos de **Armazenamento, Gerenciamento e Arquivamento de Dados**

1. Deve prover integridade dos logs através de criptografia dos dados;
2. Deve permitir a execução de relatórios para validar a integridade dos dados e identificar possíveis blocos de dados que tenham sido modificados;
3. A solução deve permitir armazenamento de dados on-line e off-line;
4. A solução deve permitir o gerenciamento da retenção de logs através de políticas;
5. Deve permitir a criação de regras baseadas na identificação do cliente, tipo do evento, dispositivos e especificar o número de dias no armazenamento on-line e off-line;

	RFP – Request for Proposal	Página 28 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

6. Deve ser capaz de arquivar os dados em tempo real em qualquer sistema Big Data através do barramento de mensagens Kafka (unidades básicas de dados que trafegam pela plataforma);
7. Deve ser capaz de tornar anônimo qualquer campo de log analisado que contenha informações (PII), incluindo endereços IP, nomes de host, nomes de usuários, endereços MAC e endereços de e-mail;
8. Deve permitir que os Eventos coletados sejam armazenados em Elasticsearch;
9. Deve pelos menos suportar as seguintes configurações do Elasticsearch:
 - a. Nó Único (All-in-One)
 - b. Cluster
10. Deve permitir o uso do Elastic Cloud como base de armazenamento dos eventos pelo menos do Amazon Elasticsearch;
11. Deve ser capaz de arquivamentos dos eventos através de sistema de arquivo distribuído (HDFS), garantindo uma maior escalabilidade no armazenamento dos eventos arquivados;

k. Requisitos **ANALYTICS**

1. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;
2. A solução deve possibilitar a busca de eventos históricos e em tempo real;
3. Efetuar a análise dos eventos em tempo real;
4. Realizar a correlação dos eventos antes dos dados serem armazenados na base de dados;
5. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;
6. A solução deve fornecer atualizações predefinidas de regras de correlação e atualizações de software;
7. A solução deve suportar a realização de um filtro dos dados coletados antes de realizar a correlação;
8. A solução deve possuir mais de 500 regras pré-definidas, incluindo regras de segurança, disponibilidade/performance e mudanças de configuração;
9. Permitir a criação de novas regras e a edição das regras existentes;
10. A solução deve permitir a criação de regras de correlação, unificando todos os eventos, como logs de segurança, disponibilidade, performance, storage e mudanças de configurações;

	RFP – Request for Proposal	Página 29 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

11. A solução deve ser capaz de gerar alertas automáticos e notificações quando alcançar os limites de dados coletados, sem descartar os dados;
12. Deve permitir buscas simples em raw data (não estruturadas), através de palavra-chave, bem como definir quais campos serão apresentados no resultado, o período da busca e a organização (ambientes multi-tenant);
13. Deve permitir salvar a consulta, definindo o tempo que ela estará disponível para uso futuro;
14. Deve permitir salvar e enviar por e-mail o resultado da busca, como PDF e CSV;
15. Deve possibilitar buscas estruturadas, baseadas em atributos, inserindo múltiplas condições. Deve haver opção para agrupamento de eventos;
16. Ao operador será possível definir: de qual elemento ele deseja verificar os logs, eventos cuja ação tomada pelo dispositivo foi "negar" e filtrar por dispositivos presentes em uma determinada categoria da base de conhecimento, de forma condicional (AND) ou excludente (OR);
17. Deve possibilitar uma busca que mostre mudanças em logins/grupos do domínio não executadas por usuários de um determinado grupo de admins do domínio;
18. O uso de expressões regulares deve ser permitido nas buscas;
19. A depender do tipo de informação buscada, a solução deve exibir gráficos nos formatos de: tendência, tabela, barra, dispersão (correlação entre duas variáveis) e árvore (análise de componentes dominantes) e heat map (intensidade);
20. Deve permitir, de forma simples, converter uma busca histórica em tempo real, sem que haja necessidade de reinserir os mesmos filtros para essa nova busca;
21. A partir de uma busca, deve ser possível criar uma regra reaproveitando os filtros já definidos, e gerar um alerta, a fim de notificar o administrador sobre um determinado evento;
22. As buscas simples devem aceitar os seguintes operadores: AND, OR e AND NOT;
23. As buscas estruturadas devem aceitar os seguintes operadores: =, !=, >, >=, IN, BETWEEN, IS, CONTAINS e REGEXP;
24. Deve listar, por padrão, atributos que podem ser utilizados nas queries;
25. Adicionalmente, deve permitir buscar atributos presentes na base de conhecimento, filtrando por funcionalidade e equipamento;
26. Deve mostrar, quando possível, a localização geográfica de um IP (origem ou destino), tais como: país, cidade, estado, longitude e latitude;
27. Deve exibir, em formato de mapa, os resultados da query no que tange países envolvidos no tráfego resultante do filtro;

	RFP – Request for Proposal	Página 30 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

28. O administrador deve ser capaz de salvar filtros de pesquisas, que podem ser reutilizados no futuro;
29. A solução deve suportar análise de dados históricos de segurança, eventos, dispositivos e sistemas ou dados de aplicativos de longo prazo;
30. A solução deve possibilitar o uso de "queries" em formato "SQL like" para minimizar a curva de aprendizado para administradores familiarizados em banco de dados relacionais;
31. A solução 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;
32. A solução deve permitir buscas utilizando expressões regulares e palavras-chave em todo o conteúdo dos dados e metadados capturados;
33. A solução deve prover uma console e visão altamente intuitiva para realizar investigações sobre os dados;
34. A solução deve possuir um módulo de análise avançada de eventos, podendo comparar metadados e correlacionar eventos em uma base histórica;
35. A solução deve permitir a criação customizada de interpretadores (parsers) através de linguagem XML para identificação de protocolos de rede específicos;
36. A solução deve ser capaz de suportar análises preditivas;
37. A solução deve ser capaz de suportar análises avançadas como anomalias estatísticas;

I. Requisitos de **Monitoramento**

1. A solução deve suportar a aplicação de filtros na camada de rede e de aplicação, no mínimo MAC, IP, usuário e palavras-chave;
2. A solução deve ser capaz de auto descobrir dispositivos e recursos que estão sendo monitorados através de protocolos e credenciais como SNMP, WMI, SSH/Telnet e outros;
3. Para casos onde será utilizado o WMI como coletor de logs, a solução deverá ser capaz de criar filtros para obtenção dos mesmos. Estes filtros podem contemplar todos os Logs, ou logs como: Eventos de Sistema, Segurança ou Aplicação;
4. A solução deve automaticamente classificar os dispositivos por tipo ou grupos, sendo depois referenciados em relatórios, regras, queries e outros;
5. A solução deve suportar a monitoração de dispositivos como disponibilidade, mudanças de configuração, performance e outros;
6. A solução deve suportar no mínimo os protocolos: TCP, UDP baseado em syslog, Netflow, Sflow, Jflow, SNMP trap, JDBC, Cisco SDEE, Microsoft WMI, Checkpoint LEA,



banco de dados JDBC para Oracle, banco de dados do servidor SQL, banco de dados IBM DB2, JDBC para Snort, JDBC para McAfee Foundstone, SSH / telnet para arquivos de configuração, VMware SDK para descoberta VMware e coleção de logs. Para as métricas de desempenho e disponibilidade, o SIEM deve usar SNMP, JMX, Windows WMI, JDBC para vários bancos de dados, NetApp ONTAP API, EMC Navisphere, VMware SDK;

7. A solução deve suportar a monitoração de seus próprios processos internos com possibilidade de geração de alertas;

m. Requisitos de **Alertas e Incidentes**

1. Como resultado de regras, deverá ser capaz de executar ações automáticas, tais como:
 - a. Executar script, como reiniciar um processo, remover arquivos de um diretório, mudança de configuração ou execução de comandos dentro outros.
 - b. Criação de um TRAP SNMP.
 - c. Enviar e-mail para uma lista de usuários.
 - d. Enviar mensagem para o usuário conectado no console;
 - e. Criar um ticket no sistema de troubleshooting interno ou externo;
2. A solução deve organizar os incidentes em categorias e subcategorias, permitindo assim que esses campos possam ser usados em pesquisas;
3. A solução deve permitir a criação e acompanhamento de Incidentes de Segurança, com no mínimo as seguintes características:
 - a. 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;
 - b. 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;
 - c. Possibilidade de manter o histórico de atividades realizadas pelos analistas, tais como criação de registros, atualização de campos, etc;
 - d. 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;
 - e. Permitir inserir comentários dos analistas no incidente, de tal forma a possibilitar o registro de todas as atividades de análise;
 - f. 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;

	RFP – Request for Proposal	Página 32 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- g. Permitir análise comportamental para detecção automática de incidentes relacionados às atividades de Comando e Controle (C2), permitindo a detecção de Movimentos Laterais para identificação de atividades de login suspeitas em ambientes Windows e Linux;
4. Possuir integração nativa com ferramenta de gerenciamento de incidentes externa, tais como: ServiceNow, Sales Force, Remedy e ConnectWise;
5. A solução deverá possuir atributos para resolução de incidentes, com as seguintes opções:
 - a. Positivo
 - b. Falso Positivo
 - c. Aberto
6. Os atributos de resolução de incidentes podem ser usados em pesquisas;
7. Deve ser capaz de encaminhar logs para um sistema externo usando o formato Common Event Format (CEF) sobre UDP ou TCP;
8. Deve permitir que os Incidentes detectados sejam visualizados através de todas as categorias definidas pela matriz MITRE ATT&CK;
9. Permite a integração com soluções externas de incidentes/Secops via JSON REST API.
- n. Requisitos de **Integração ao CMDB**
 1. A solução deve possuir integração ou integrar-se à sistemas de CMDB (Configuration Management Database), atendendo de forma nativa ou através de composição os requisitos listados nesse documento;
 2. A solução deve prover informações detalhadas sobre devices, aplicações, usuários e qualquer outro componente de rede compatível com protocolos de gerência (SNMP, SYSLOG, NETFLOW, etc), de forma nativa. Para elementos desconhecidos, deve ser possível a criação de scripts que permitam a correta identificação dos mesmos;
 3. Deve permitir realizar um discovery da rede, de forma dinâmica, evitando a adição manual dos elementos ao CMDB;
 4. O discovery deve promover categorização dinâmica, alocando os elementos nos devidos grupos;
 5. Deve informar: nome do dispositivo gerenciado, IP, tipo, versão, protocolo utilizado para coleta dos dados e organização a qual pertence;
 6. Deve ser capaz de mostrar os elementos gerenciados de forma tabelada e em topologia, posicionando cada elemento conforme configurações/logs analisados;
 7. Deve mostrar estatísticas relativas à performance do dispositivo, tais como: tráfego, memória, disco e CPU;

	RFP – Request for Proposal	Página 33 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

8. Ao selecionar um dispositivo específico, deve permitir visualizar seus logs em tempo real (analytics), sem necessidade de criar um filtro manual para tal;
 9. Deve permitir agregar dispositivos e aplicações que suportam um determinado serviço dando ao operador uma visão macro sobre o serviço em si;
 10. Quando aplicável, deve informar ao operador o software, hardware e configuração utilizados pelo dispositivo;
 11. De forma simples, deve informar os incidentes e eventos de disponibilidade, performance e segurança relacionados a um elemento monitorado;
 12. Deve prover, por padrão, listas de domínios (threat feeds) conhecidos por gerar spam, suportar botnets, participar de ataques DDoS e conter malwares. O operador deve ser capaz de adicionar novas listas;
 13. A solução deve prover uma lista de credenciais padrão utilizadas por equipamentos. Caso a plataforma identifique um dispositivo que as use, um alerta deve ser gerado;
 14. Ao operador deve ser possível agrupar em listas elementos que devem ser acompanhados com maior atenção. Exemplo: logins que são constantemente bloqueados e máquinas cujos discos apresentam falta de espaço;
 15. Deve prover reports que informem dispositivos aprovados no CMDB, usuários descobertos, sistemas operacionais utilizados, hardwares, serviços em execução em máquinas Windows, softwares e patches instalados, dentre outros;
- o. Requisitos de **Gerenciamento de Usuários**
1. Dado o grande escopo abordado pela solução, se torna difícil a um único administrador gerenciar performance, disponibilidade, mudanças e segurança em equipamentos de rede, servidores e aplicações. A solução ofertada deve permitir a divisão de tarefas por função (RBAC), localidade/área, dispositivos/sistemas e nível de criticidade da informação;
 2. A solução deve possuir controle de acesso baseado em perfis de usuários e ser multi-tenant;
 3. Por padrão, a plataforma deve disponibilizar os seguintes tipos de gerência: escrita e leitura, equipamentos de rede, sistemas, servidores, Windows, segurança, helpdesk e apenas leitura;
 4. Deve permitir a criação de funções customizadas;
 5. Deve suportar o uso de logins locais e externos para autenticação na gerência da solução, nesse último caso: LDAP, RADIUS e SAML via Okta;
 6. Deve suportar duplo fator de autenticação em logins de gerência;

	RFP – Request for Proposal	Página 34 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

p. Requisitos de **Inteligência de Ameaças** (Threat Intelligence)

1. A solução deve suportar a obtenção de informações de inteligência de ameaças;
2. Deve ser capaz de obter, pelo menos, as seguintes informações: domínio de malware, IP de malware, URL de malware, Hash de malware, redes anônimas incluindo proxies abertos e VPN, User Agent de malware;
3. A solução deverá prover importação via STIX/TAXII;
4. Deve ser capaz de obter informações de inteligência de ameaças nativamente das seguintes fontes: Emerging Threat, Malware Domain List, Zeus e Threat Stream (Anomali);
5. Deve ser capaz de obter informações de inteligência de ameaças nativamente da fonte AlienVault OTX pelos menos os seguintes itens:
 - a. IPs Maliciosos
 - b. URLs Maliciosas
 - c. Hashs de Ameaças

iii. **NMS (Network Management System)/Observabilidade Unificada:** solução de software, ou conjunto de ferramentas, usada para monitorar, administrar e otimizar em tempo real as diferentes redes e serviços existentes, garantindo que todos os dispositivos e conexões funcionem corretamente;

- a. A solução de observabilidade deverá atuar como camada unificada de coleta, correlação e contextualização de telemetria de rede, infraestrutura, segurança e aplicações, integrando e enriquecendo operacionalmente os ecossistemas da Telebras e RPG, de forma complementar e não substitutiva às ferramentas especializadas, sendo 100% compatível as ferramentas/soluções contidas no escopo dessa RFP;
- b. Deverá monitorar qualquer dispositivo, independentemente de fabricante, modelo ou sistema operacional, com descoberta automática e contínua de ativos;
- c. Deverá suportar integração universal de coleta, incluindo, no mínimo:
 1. SNMP (v1/v2c/v3) e ICMP;
 2. Syslog (UDP/TCP/TLS);
 3. API REST/SOAP;
 4. NetFlow, sFlow e IPFIX;
 5. JMX, WMI e JDBC;
 6. arquivos (CSV/XML).
- d. Deverá prover interface única e painel centralizado, com dashboards interativos e personalizáveis, incluindo gráficos, mapas de geolocalização e mapas de rede;
- e. Deverá prover mapas topológicos dinâmicos, atualizados por descoberta automática de rede, com representação do estado operacional em tempo real;

	RFP – Request for Proposal	Página 35 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- f. Deverá possuir arquitetura multitenant nativa, em que departamentos, órgãos ou unidades acessem exclusivamente seus dashboards, alarmes e dados;
- g. A solução deverá prever, como capacidade valorável e ativável futuramente sem substituição da plataforma, o suporte a sondas passivas de tráfego IP (via TAP ou port-mirror) e a sondas ativas de tráfego sintético para monitoramento proativo de disponibilidade e latência fim a fim, sob a perspectiva do usuário final. Tal funcionalidade não integra o escopo de fornecimento desta contratação, sendo valorada a sua disponibilidade nativa no ecossistema da solução para eventual habilitação futura, conforme necessidade;
- h. Deverá possuir motor de alarmes e correlação avançada, com correlação temporal e causal de múltiplas fontes, supressão de ruído, agrupamento inteligente e priorização por criticidade;
- i. Deverá suportar ações automáticas sobre alarmes, incluindo abertura automática de tickets, notificações multicanais e acionamento de rotinas de remediação autorizadas;
- j. Deverá possuir capacidades de inteligência artificial integradas, incluindo:
 1. detecção de anomalias por modelos estatísticos adaptativos;
 2. forecasting de capacidade, com identificação proativa de gargalos;
 3. análise de causa raiz multidimensional, correlacionando logs, métricas, fluxos (NetFlow/sFlow/IPFIX ou similares) e eventos.
- k. Deverá disponibilizar interação em linguagem natural (assistente conversacional) para consultas operacionais com contexto real da infraestrutura;
- l. Será valorada a capacidade das funcionalidades de inteligência artificial serem executadas em appliances dedicados de IA, implantados na infraestrutura do EAF, considerando o caráter on-premises da solução e os requisitos de soberania e confidencialidade do dado, sem exportação de informação para nuvens públicas ou serviços externos de terceiros, e sem dependência de consumo por tokens, chamadas a APIs externas ou licenciamento variável associado ao volume de uso, garantindo custo previsível e total isolamento dos dados operacionais. Trata-se de item de caráter valorável (não obrigatório), objeto de pontuação técnica e não de desclassificação;
- m. Deverá prover geração automática de relatórios agendados e personalização de relatórios pelo administrador;
- n. Deverá possuir integração bidirecional com CMDBs e ferramentas de ITSM e API REST aberta para integração com qualquer sistema do ecossistema;
- o. A solução NMS/Observabilidade deverá ser dimensionada para suportar, inicialmente, no mínimo 3.000 elementos/dispositivos monitorados, podendo essa capacidade ser ampliada de acordo com o inventário e a volumetria reais da RPCAF. A solução deverá permitir escalabilidade horizontal mediante a adição de nós de coleta e processamento, sem necessidade de substituição da arquitetura existente;
- p. Deverá ser disponibilizada em modelo on-premises, compatível com os requisitos de soberania de dados e segurança da informação exigidos para infraestruturas críticas da

	RFP – Request for Proposal	Página 36 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

APF, compatível com hypervisors de mercado (por exemplo, soluções de virtualização corporativas de mercado);

- q. Deverá complementar cada tecnologia do ecossistema com integrações específicas, incluindo, no mínimo:
1. enriquecimento de alertas para o SOAR via API/Syslog;
 2. filtragem e enriquecimento de eventos para o SIEM;
 3. correlação de sessões privilegiadas (PAM/TACACS+) com mudanças de configuração detectadas;
 4. inventário dinâmico para o NAC;
 5. monitoramento de pools e backends dos balanceadores;
 6. monitoramento de desempenho, configurações e VPNs dos firewalls;
 7. monitoramento de storage e virtualização.
- r. Deverá gerar relatórios de SLA e de desempenho por órgão/cliente da Administração Pública Federal, com exportação automática para repositório externo designado pela EAF, para retenção pelo período contratual;
- s. A solução deverá monitorar a qualidade dos enlaces (latência, jitter e perda de pacotes) por circuito e por órgão, admitindo-se qualquer mecanismo de coleta tecnicamente adequado à fonte de dados (SNMP, API, telemetria, syslog, IP SLA ou equivalente), com armazenamento de série histórica e cálculo automático de linha de base (baseline) por métrica, permitindo a configuração de alarmes por desvio em relação ao comportamento esperado;
- t. Deverá prover análise de protocolos de fluxos como Netflow ou equivalente, provendo visões de top talkers, aplicações e conversações, permitindo drill-down do agregado até o fluxo individual;
- u. Deverá suportar janelas de manutenção programáveis com supressão de alarmes e anotações, além de perfis de acesso somente leitura para visões compartilhadas com os órgãos;
- v. Deverá gerar relatórios de capacidade e inventário (ocupação de portas e top N de utilização), com projeção de crescimento para planejamento de expansões;
- w. Deverá suportar a execução de testes sintéticos de serviços de rede, quando houver coletores, agentes ou pontos de execução habilitados, por exemplo DNS, DHCP, HTTP/S e ICMP, com alertas por degradação;
- x. Deverá gerar mapas topológicos automáticos de camadas 2 e 3, com descoberta de vizinhança (LLDP/CDP) e visualização do caminho fim a fim entre dois pontos da rede;
- y. Deverá disponibilizar API REST para consulta de métricas, alarmes e inventário, e webhooks para notificação de eventos a sistemas externos autorizados;
- z. Deverá prover contabilização de consumo por órgão e por circuito (tráfego total e por aplicação), com relatórios mensais exportáveis, apoiando os processos de faturamento e rateio (BSS) da EAF;



- aa. Deverá suportar telemetria por streaming (por exemplo, gNMI/NETCONF-YANG) em complemento ao SNMP, para coleta de métricas em alta frequência dos elementos que disponham do recurso;
 - bb. Para elementos que não contenham orquestrador de mesmo fabricante, a plataforma deverá prover gestão de configurações dos dispositivos de rede (NCM), com cópia de segurança agendada das configurações, versionamento, comparação de alterações (diff), alerta de mudanças não autorizadas e restauração de configuração;
 - cc. Deverá prover painéis de parede (wallboard) para o NOC, com rotação automática de visões, indicadores de status das redes/serviços por domínio tecnológico e destaque de alarmes críticos;
 - dd. Deverá gerar relatório executivo mensal automático por órgão, consolidando disponibilidade, desempenho, capacidade e principais eventos do período;
 - ee. A plataforma de observabilidade deverá ser independente de fabricante de rede, monitorando de forma nativa e agnóstica a infraestrutura multifabricante existente e futura da RPCAF, por meio de padrões abertos (SNMP, NetFlow/sFlow/IPFIX, telemetria por streaming gNMI/NETCONF e API), sem exigir malha (fabric), agente ou rede nativa de um fabricante específico;
 - ff. A descoberta e o inventário dos ativos de rede deverão ser independentes de fabricante, cobrindo nativamente redes/serviços multifabricantes por meio de padrões abertos, sem depender de malha (fabric) ou agente proprietário de um fabricante específico, disponibilizando esse inventário de rede à ferramenta CMDB;
- iv. **PAM (Privileged Access Management):** solução que gerencia credenciais e acessos de usuários com privilégios elevados. É usada para controlar, monitorar e proteger o acesso de contas privilegiadas dentro do ambiente operacional e/ou corporativo;
- a. Deve permitir o gerenciamento centralizado de acessos privilegiados;
 - 1. Entende-se por acessos privilegiados os tipos de acesso a ativos e a sistemas de tecnologia, além dos acessos realizados por um usuário comum, geralmente realizados por administradores de redes, administradores de servidores e administradores de sistemas;
 - b. A solução deve controlar o acesso baseado em função, com recursos de auditoria e de segurança, provendo no mínimo as seguintes funcionalidades:
 - 1. **Cofre de credenciais:** funcionalidade onde os usuários não precisam ter conhecimento das credenciais, reduzindo-se o risco de vazamento, incluindo o rotacionamento automático dessas credenciais;
 - 2. **Controle de acesso a contas privilegiadas:** funcionalidade onde é possível estabelecer níveis de privilégios de cada usuário, incluindo funcionalidades de fluxo de aprovação de acessos a determinados recursos;
 - 3. **Monitoramento e registro de eventos:** funcionalidade onde é possível monitorar, registrar e auditar as atividades dos usuários privilegiados, incluindo informações das sessões, tais como: pressionamento de teclas, eventos de mouse, etc.;



- c. A solução deve ser do tipo appliance virtual, compatível com pelo menos os Hypervisors VMware ESXi, Microsoft Hyper-V e Linux KVM;
- d. A solução deve suportar a implementação em cluster de alta disponibilidade (HA), com suporte a implementação de um nó remoto para fins de Disaster Recovery;
- e. As chaves criptográficas devem ser armazenadas internamente na solução e protegidas por tecnologia TPM ou vTPM;
- f. A solução deve prover interface de API para integração com sistemas ou soluções de terceiros;
- g. A solução deve diferenciar os usuários da plataforma entre:
 - 1. **Usuários comuns:** aqueles que apenas executam as tarefas de gerenciamento dos sistemas de destino, como por exemplo a equipe de TI, um contratado da TI, um administrador de banco de dados (DBA). Geralmente estes usuários são Gerentes de TI e Administradores de Sistemas de TI;
 - 2. **Usuários administradores:** aqueles que são responsáveis pelas tarefas de gerenciamento da solução;
- h. A solução deve operar pelo menos nos seguintes modos:
 - 1. **Modo Proxy:** toda conexão aos sistemas de destino é interceptada pela solução, que fica responsável pela conexão final ao sistema de destino. Nesse modo, a máquina cliente não tem acesso direto as credenciais de acesso e o administrador da solução pode interromper conexões se um comportamento estranho for detectado;
 - 2. **Modo Não-Proxy:** toda conexão aos sistemas de destino parte diretamente da máquina cliente e a solução fornece ao cliente as credenciais para esse acesso;
- i. A solução deve armazenar de forma segura o nome de usuário e a senha/chave dos servidores como segredos. Os segredos podem conter informações sobre login, credenciais e o endereço IP do servidor de destino. O usuário final pode usar o segredo para acessar os servidores;
- j. As credenciais reais devem ser protegidas e os usuários da solução não podem acessar as credenciais, exceto em alguns casos configuráveis pelo administrador. As credenciais de login podem ser alteradas automaticamente e também manualmente, a depender dos diferentes casos de uso;
- k. A solução deve permitir a configuração de políticas comuns e um sistema de fluxo de aprovação hierárquico e auditável para acesso a informações sensíveis;
- l. Os critérios de gerenciamento de senha devem ser configuráveis para atender à política organizacional de frequência de alteração de senha/controle de aprovação de uso/alteração após o uso;
- m. Deve incluir e não se limitar aos seguintes recursos de Sistemas e Protocolos e Ferramentas: AD, Windows, Linux/Unix, Oracle DB, MS SQL, CISCO, AS400, Microsoft SQL, Microsoft SQL Shell, MySQL CLI, MySQL Shell, PostgreSQL CLI, VNC, WEB SMB, WEB SSH, Web RDP, Web SFTP;
- n. Deve permitir a construção de um conector de plataforma personalizado e integração A2A;



- o. Deve oferecer suporte para aprovação de credencial dupla, exigindo aprovações de usuários designados antes de permitir o acesso a credenciais para contas gerenciadas;
- p. Deve oferecer suporte a funcionalidades de fluxo de trabalho para controles de liberação de senha e sessão, incluindo suporte para vários níveis de autorização, capacidade de agrupar autorizadores;
- q. Deve suportar a capacidade de expirar a solicitação de aprovação após um período de tempo;
- r. Deve fornecer a capacidade de permitir recursos de check-out e check-in para secrets;
- s. Deve permitir a autenticação de uma sessão sem revelar a senha por meio da máquina do usuário final;
- t. Sessões privilegiadas devem ser transmitidas por proxy por meio de um hardware seguro ou dispositivo virtual;
- u. O proxy de sessão deve ser capaz de entrar em uma conta sem liberar uma senha para o usuário privilegiado;
- v. A solução deve permitir o uso do modo cliente, com o uso de agentes, e deve oferecer suporte ao modo somente navegador, onde nenhum software cliente/agente é necessário;
- w. Os seguintes modos de cliente e navegador devem ser suportados:
 - 1. Modo cliente: PuTTY, Windows Remote Desktop, RealVNC, TightVNC e WinSCP etc;
 - 2. Modo de navegador: Web SSH, Web RDP, Web VNC, Web SMB, Web SFTP e Web Account;
 - 3. No modo navegador, deve possibilitar o uso de pelo menos as seguintes funcionalidades: acesso a senhas, sessões e administração da solução;
- x. Deve possuir iniciadores de conexão para pelo menos: MySQL (CLI e Shell), Microsoft SQL CLI, PostgreSQL CLI, SSH (PuTTY, SSH CLI e SecureCRT), Remote Desktop e VNC (TightVNC e VNC Viewer);
- y. As sessões devem permitir a inclusão ou exclusão de comandos executados durante uma sessão sem a necessidade de um agente;
- z. Deve suportar registro/monitoramento de pelo menos os seguintes protocolos de sessão - Telnet, SSH, RDP, ICA, VNC, SQL Plus, SQL Windows, Http & Https, x5250, x3270
- aa. Deve permitir a auditoria das atividades administrativas da própria solução;
- bb. As solicitações de acesso privilegiado devem ser feitas usando um modelo de solicitação/liberação, no mínimo;
- cc. Não deve permitir que um administrador da solução realize o bypass do fluxo de aprovação para obter uma senha ou ativar uma sessão;

	RFP – Request for Proposal	Página 40 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- dd. A solução deve oferecer suporte à sessão remota de auditoria no modo não transparente ou transparente, sem alteração no fluxo de trabalho para acessar a sessão remota usando ferramentas nativas do cliente, incluindo injeção direta de credencial;
- ee. Deve suportar monitoramento e gravação de sessão (para análise posterior) e seu monitoramento em tempo real (para vigilância em tempo real), permitindo que o administrador encerre as sessões, caso necessário;
- ff. As gravações do vídeo da sessão devem usar formatos disponíveis publicamente;
- gg. Deve ser possível gerar alertas de e-mail quando um usuário executa um comando restrito e a detecção de tais comandos não devem depender do uso de agentes;
- hh. Deve suportar diferentes métodos de autenticação e integração com sistemas corporativos como: Active Directory, LDAP, SAML, RADIUS;
- ii. Deve possuir suporte a múltiplo fator de autenticação (MFA) através de Token da Solução, SMS e E-Mail;
- jj. Deve permitir a configuração de OTP (One Time Password) via e-mail;
- kk. Deve permitir a verificação de arquivos transferidos entre o endpoint e os ativos protegidos, realizando-se a varredura contra conteúdos maliciosos;
- ll. Deve suportar o uso de verificações contra vazamento de dados (DLP) nos arquivos transferidos;
- mm. Deve suportar o bloqueio da área de transferência dos ativos privilegiados, para impedir a cópia de informações desses ativos;
- nn. Deve fornecer a funcionalidade de Break Glass para acesso emergencial as credenciais armazenadas na solução;
- oo. Deve restringir o acesso a console dos ativos protegidos pela solução;
- pp. Deve proteger o acesso à rede dos ativos protegidos pela solução;
- qq. Deve armazenar todas as senhas em um cofre seguro com criptografia AES-256;
- rr. Deve permitir que qualquer login/senha usado para acesso a ativos protegidos seja armazenado internamente e com segurança e deve permitir que os usuários se conectem aos ativos protegidos sem o conhecimento do login/senha utilizado;
- ss. Deve alterar automaticamente as senhas para um grupo de recursos;
- tt. Deve estabelecer acesso granular às senhas;
- uu. Deve impedir os usuários vejam a senha em texto puro;
- vv. Deve permitir que as credenciais sejam injetadas diretamente nos sistemas, dando acesso aos usuários sem que eles vejam ou forneçam credenciais;



- ww. Deve suportar o controle de acesso sem o uso de VPN;
- xx. Deve permitir que as sessões sejam mantidas e compartilhadas com os auditores para interação (colaboração de sessão);
- yy. Deve permitir que os auditores monitorem usuários privilegiados sob demanda e em tempo real;
- zz. Deve integrar um sistema de fluxo de trabalho para permitir o acesso administrativo às máquinas identificadas;
- aaa. A solução deve permitir acesso ao recurso de destino, sem agente, pelo menos nos protocolos RDP, SSH, TELNET, VNC, HTTPS;
- bbb. Deve possibilitar o bloqueio do usuário no caso de uma execução de uma ação restrita;
- ccc. Deve permitir rastreabilidade das conexões;
- ddd. Deve permitir visualizar todas as conexões ativas;
- eee. Deve permitir rastreabilidade e controle de transferências de arquivos;
- fff. Deve permitir a configuração de notificações de e-mail em um determinado número de indicadores, como eventos relacionados ao tráfego (falha de conexão, falha de autenticação, etc.);
- ggg. Deve permitir integração com soluções SIEM para relatórios avançados e processamento em tempo real de detecção de comportamento malicioso;
- hhh. Deve possuir logs de auditoria completos e pesquisas avançadas, como pesquisas de texto para isolar incidentes;
- iii. Os logs de auditoria da solução devem mostrar claramente quem acessou qual dispositivo de destino, bem como a duração (hora de início e hora de término);
- jjj. Deve fornecer logs para o histórico de aprovação de sessões privilegiadas;
- kkk. Deve possuir um painel para exibir os usuários conectados no momento;
- III. Deve permitir relatórios personalizáveis.
- v. **TACACS+** (Terminal Access Controller Access-Control System Plus): protocolo de autenticação, autorização e auditoria (AAA) usado em redes, especialmente em ambientes operacionais e/ou corporativos, para controlar acessos administrativos a elementos como roteadores, switches e firewalls;
- a. A solução deverá prover serviço de autenticação, autorização e accounting (AAA) centralizado para acesso administrativo a equipamentos de rede, com suporte aos protocolos TACACS+ e RADIUS;

	RFP – Request for Proposal	Página 42 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- b. Deverá integrar-se a Active Directory/LDAP e à solução de IAM para autenticação de administradores, com suporte a MFA;
- c. Deverá prover autorização granular por comando e por perfil de administrador, com registro (accounting) de todos os comandos executados;
- d. Deverá operar em alta disponibilidade entre os dois Data Centers, sem ponto único de falha;
- e. Deverá exportar os registros de autenticação e comandos para o SIEM e para a camada de observabilidade, permitindo correlação entre sessões administrativas e mudanças operacionais;
- f. As comunicações AAA entre os equipamentos e os servidores deverão ser criptografadas, com perfis de autorização por grupo (mapeados ao AD/LDAP), níveis de privilégio e listas de comandos permitidos e negados por perfil de administrador;
- g. Deverá ser dimensionada para o parque completo de equipamentos da RPCAF (no mínimo, 6.500 equipamentos), com servidores distribuídos nos dois Data Centers e failover transparente para os clientes AAA;
- h. Deverá suportar simultaneamente os protocolos TACACS+ RADIUS, incluindo atributos específicos por fabricante (VSAs), para e autorização granular em equipamentos multivendor;
- i. Deverá permitir o cadastro de dispositivos em massa (importação por CSV/API) e delegação administrativa com RBAC, registrando trilha de auditoria das alterações realizadas na própria plataforma;
- j. Deverá prover relatórios de accounting por administrador, por dispositivo e por período, com exportação e agendamento;
- k. Deverá operar em alta disponibilidade com sincronização automática de configuração entre as instâncias dos dois Data Centers;
- l. O acesso administrativo à própria plataforma deverá suportar MFA e integração com o IAM do ecossistema, com trilha de auditoria das ações;
- m. Deverá permitir a validação prévia das políticas de autorização (simulação/teste) antes da aplicação em produção, reduzindo o risco de bloqueio indevido de administradores;
- n. O serviço de autenticação de administração de dispositivos (TACACS+/AAA) deverá operar em alta disponibilidade, com redundância de servidores e mecanismo de contingência, garantindo a continuidade do controle de acesso em caso de falha de um nó;

	RFP – Request for Proposal	Página 43 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- vi. **NAC** (Network Access Control): solução de segurança que regula quem ou o que pode se conectar a rede operacional e/ou corporativa, garantindo que apenas dispositivos e usuários autorizados tenham acesso;
- a. Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;
 - b. Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do órgão;
 - c. Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive, Enterasys e Huawei, pelo menos;
 - d. A solução deve ser licenciada por número de dispositivos conectados/online;
 - e. A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
 - f. Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;
 - g. A licença contemplada deverá suportar todas as características exigidas neste termo de referência;
 - h. A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;
 - i. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;
 - j. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:
 1. Consultas em DHCP Fingerprint;
 2. Consultas via protocolos HTTP/HTTPS;
 3. Consultas via protocolo SNMP;
 4. Consultas via protocolo SSH;
 5. Consultas via protocolo Telnet;
 6. Consultas de portas TCP;
 7. Consultas de portas UDP;
 8. MAC OUI;
 9. Consultas via protocolo WMI;
 10. Protocolo ONVIF;
 11. Protocolo NetFlow;
 12. Base assinaturas pré-definidas;
 - k. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:
 1. Endereço MAC;
 2. Endereço IP;
 3. Sistema operacional;



4. Nome do host;
 5. Horário de conexão;
 6. Usuário conectado;
 7. Localização.
- l. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:
1. Android;
 2. Apple iOS para iPhone, iPod e iPad;
 3. Chrome OS;
 4. Linux;
 5. MacOS X;
 6. Windows 7, 8 e 10;
- m. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;
- n. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;
- o. Deve permitir a recategorização periódica de dispositivos;
- p. Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;
- q. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;
- r. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;
- s. A solução deve suportar RADIUS Change of Authorization;
- t. A solução deve suportar MAC Address Bypass;
- u. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;
- v. A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;
- w. Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;
- x. Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;
- y. A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;



- z. A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;
- aa. A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;
- bb. A solução deve possuir ferramenta que permita a criação de credenciais para eventos;
- cc. Deve permitir a definição de complexidade da senha dos usuários visitantes;
- dd. Deve ser possível definir um período de validade para as contas de usuários visitantes;
- ee. Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;
- ff. A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;
- gg. Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;
- hh. A solução deve vincular o login do visitante à máquina utilizada no acesso;
- ii. Deve suportar a validação de credenciais:
 - 1. Em base local interna à ferramenta;
 - 2. Em servidores RADIUS;
 - 3. Em servidores LDAP.
- jj. A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn, Twitter, Instagram e outras;
- kk. A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;
- ll. Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;
- mm. A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;
- nn. Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;
- oo. Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;
- pp. Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;

	RFP – Request for Proposal	Página 46 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- qq. A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
- rr. Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;
- ss. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;
- tt. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;
- uu. Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;
- vv. Se um dispositivo não passar os testes de conformidade, deve ser possível:
 1. Não forçar a remediação;
 2. Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
 3. Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;
- ww. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:
 1. Windows 7;
 2. Windows 8;
 3. Windows 10;
 4. MacOS;
 5. Linux.
- xx. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:
 1. Presença de software de anti-vírus instalado e em execução;
 2. Versão do sistema operacional;
 3. Nome de domínio do Active Directory ao qual a estação Windows pertença;
 4. Serviços em execução para estações Windows;
 5. Informações sobre um determinado certificado digital em estações Windows;
 6. Registros ou chaves de registro para estações Windows;
 7. Processos em execução para estações Windows, Linux e MacOS;
 8. Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;
 9. Pacotes instalados em estações Linux e MacOS.
- yy. A solução deve ser capaz de monitorar quando um serviço requerido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;
- zz. Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;
- aaa. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:
 1. Programas de gerenciamento e distribuição de software;



2. GPO do Active Directory;
 3. Captive Portal;
- bbb. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;
- ccc. O agente instalado nos computadores devem notificar os usuários com mensagens informativas em casos de eventos;
- ddd. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;
- eee. A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;
- fff. No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;
- ggg. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;
- hhh. Deve suportar integração com soluções de patching;
- iii. Deve suportar integração com soluções de análise de vulnerabilidades;
- jjj. A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;
- kkk. A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;
- III. A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;
- mmm. A solução deve armazenar os eventos internamente e permitir que sejam exportados;
- nnn. A solução deve permitir a exportação dos eventos através de syslog;
- ooo. Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;
- ppp. A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;
- qqq. Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;
- rrr. Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc, para correlacionar alertas de segurança e restringir, isolar ou bloquear

	RFP – Request for Proposal	Página 48 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

dispositivos comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;

sss. Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;

ttt. Deve possibilitar o rastreo de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

uuu. A Proponente deve avaliar qualquer solução de logs existente compatível com o NAC ofertado, cabe a Proponente incluí-la na proposta, sem ônus, considerando licenciamento e/ou hardware adequado para retenção dos logs;

vvv. Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;

www. Permitir o correlacionamento de eventos

xxx. Permitir ações estendidas com trilhas de auditoria

yyy. Permitir trabalhar com workflows

zzz. Permitir integrações com eventos de segurança de entrada e saída da solução

vii. **SYSLOG:** protocolo de comunicação e sistema de registro de logs usado para coletar, armazenar e analisar mensagens e eventos;

- a. O ecossistema deverá prover serviço centralizado de coleta de Syslog (UDP/TCP/TLS) para todos os elementos da RPCAF, com normalização, indexação e retenção dos registros;
- b. Deverá permitir a exibição centralizada de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa;
- c. A coleta de logs, eventos e telemetria de todas as fontes do ambiente deverá ser centralizada na camada de observabilidade/SYSLOG com função de data broker, responsável por receber, normalizar, filtrar e enriquecer os registros na origem e encaminhá-los seletivamente a cada subsistema, conforme sua responsabilidade funcional: os eventos relevantes de segurança ao SIEM; a telemetria operacional à observabilidade; o inventário e as dependências à CMDB; e demais destinos autorizados;
- d. A camada de data broker deverá reter integralmente os registros para consulta, troubleshooting e auditoria, exportando ao SIEM apenas o subconjunto necessário;
- e. A função de filtragem deverá ser capaz de reduzir significativamente o volume ingerido pelo SIEM, e a PROPONENTE deverá apresentar referências e mecanismo de configuração das políticas de filtragem;



- f. Deverá suportar os formatos e padrões usuais de mercado (RFC 3164/5424, CEF, LEEF e JSON), com encaminhamento seletivo e simultâneo para múltiplos destinos e fila persistente (armazenar e encaminhar), integrados à licença da solução, para o caso de indisponibilidade temporária do destino por no máximo 4 horas;
- g. Deverá garantir a integridade dos registros armazenados (hash/assinatura) e prover compressão eficiente para otimização do armazenamento de longo prazo;
- h. Deverá possuir capacidade de mascaramento/anonimização de campos sensíveis antes do encaminhamento dos registros, em apoio ao atendimento da LGPD;
- i. Deverá suportar rotulagem e enriquecimento dos registros por origem e por órgão (tags), com controle de taxa por fonte (rate limiting) para proteção contra rajadas de eventos;
- j. Deverá detectar e alertar fontes silenciosas (interrupção do envio de logs por elemento monitorado), assegurando a completude da coleta para fins de auditoria;
- k. Deverá disponibilizar painéis de volumetria por fonte e por destino, com retenção configurável por classe de log;
- l. Deverá operar em alta disponibilidade, com failover automático entre os coletores, sem ponto único de falha na cadeia de coleta;
- m. Deverá ser dimensionada para ingestão mínima de 500 GB/dia de logs, com margem de expansão de pelo menos 100% sem substituição da arquitetura;
- n. Deverá permitir o reenvio (replay) de eventos retidos para reprocessamento em destinos selecionados, em janelas de tempo definidas, sem duplicação indevida de registros;
- o. Deverá proteger os buffers locais de retenção com criptografia em repouso e controle de acesso, preservando a confidencialidade dos logs em toda a cadeia de coleta;
- p. Deverá coletar e normalizar telemetria, fluxos e logs do parque de SD-WAN, de segurança e de gerência já existente na RPCAF, com função de data broker;

	RFP – Request for Proposal	Página 50 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

4. Condições Gerais

- a) A solução proposta pela PROPONENTE deve atender a todos os requisitos mandatórios da Statement of Compliance (SoC) ao longo deste documento;
- b) Além disso, existem requisitos que são específicos para a resposta da PROPONENTE;
- c) A resposta da PROPONENTE deve descrever como todos os requisitos de SOW serão atendidos pela solução proposta e deve atender a todos os requisitos mandatórios de RFP;
- d) É facultado à EAF flexibilizar ou não requerimentos, considerados inicialmente como mandatórios, em caso de atendimento parcial (Parcialmente em Conformidade), ou não atendimento (Não Conforme), desde que a resposta e ou explicação da PROPONENTE evidencie que não haverá impacto negativo no projeto;
- e) Requisitos de Documentação
 - e.1. A PROPONENTE deve fornecer documentação para as funções de software e plataformas de hardware, incluindo a descrição do produto, descrição funcional, descrição das interfaces da arquitetura;
 - e.2. A PROPONENTE deve fornecer relatórios de teste confirmando a conformidade com as normas exigidas e a documentação necessária atestando a homologação no Brasil (Anatel), quando necessário;
 - e.3. A PROPONENTE deve fornecer documentação para dar suporte aos serviços de implantação e operações, incluindo um guia de Dimensionamento, um guia de Instalação, Configuração e Comissionamento, bem como um guia de Operação e Manutenção, para cada ferramenta/solução de OSS/BSS;
 - e.4. A PROPONENTE deve apresentar as seguintes documentações, não se limitando a:
 - a. Relação de empresas subcontratadas e fornecedores críticos envolvidos na prestação dos serviços;
 - b. Documento de descrição detalhada da solução técnica;
 - c. Arquitetura e descrição do sistema;
 - d. Relação de todos os elementos/funcionalidades oferecidos na proposta, com suas respectivas capacidades;
 - e. Descrição do produto;
 - f. Descrição das Features;
 - g. Casos de usuários, fluxos de chamadas e de serviços;
 - h. Instalação de hardware e software;
 - i. Documentos de configuração;
 - j. Resolução de problemas (Troubleshooting) e código de erro;
 - k. Contadores e estatísticas;
 - l. Relatórios de KPI;
 - m. Descrição de parâmetros;
 - n. Certificados de Homologação;

	RFP – Request for Proposal	Página 51 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- o. **Plano de Treinamento** com cronograma, quantidade de turmas, quantidade de treinandos por turma e ementa de cada treinamento.

f) Licenciamento – Suporte e garantia do produto

- f.1. A PROPONENTE deve fornecer o controle de descrição de licença de todos os elementos da solução;
- f.2. A PROPONENTE deve fornecer a descrição detalhada de todas as licenças e certificados integrados no sistema que são fornecidas pela própria, ou por terceiros, bem como indicar os dados dos eventuais terceiros a serem utilizados para expressa aprovação pela EAF;
- f.3. As licenças de uso de software, de usuários, ou de serviços deverão ser perpétuas, sem data para expirar;

g) Políticas e alinhamentos de segurança da informação:

- g.1. A solução deve atender às políticas e diretrizes de segurança da informação solicitadas pela EAF;
- g.2. É essencial que as leis governamentais vigentes sobre segurança cibernética e proteção de dados do Brasil sejam cumpridas, bem como as leis da Agência Nacional de Telecomunicações do Brasil (ANATEL);
- g.3. A PROPONENTE tem a obrigação de gerar um documento no qual seja estabelecido o devido cumprimento do regulamento, especificando como e de que forma cada artigo corresponde aos regulamentos das resoluções;

h) Roadmap de Hardware e Software:

- h.1. A PROPONENTE deverá fornecer Roadmap detalhado de hardware e software pelo menos para os próximos 3 anos;
- h.2. A PROPONENTE deve fornecer o ciclo de vida detalhado (hardware e software) do sistema (desde a disponibilidade geral (GA) até o fim da vida útil (EOL));
- h.3. Todos os tipos de hardware devem ser da versão mais recente, não devem estar com término de comercialização (end-of-sale) anunciado (os produtos devem estar em produção e serem comercializados pelo fabricante no momento da assinatura do contrato) e ter, pelo menos, 5 anos antes do fim do suporte, contados a partir do tempo de contrato assinado;
- h.4. Durante o ciclo de vida do hardware, no caso de atualização de software que requeira adição/substituição de hardware, o fornecedor será responsável por fornecê-lo gratuitamente;
- h.5. Todas as versões de software devem ser a versão mais recente e ter pelo menos 3 anos antes do fim do suporte, além de suporte para desenvolver novos patches de software de correção, contando a partir do tempo de contrato assinado;

	RFP – Request for Proposal	Página 52 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- h.6. A PROPONENTE deve garantir que uma nova versão do software ou firmware contenha todas as funções das versões anteriores e que a introdução desta não prejudique a interoperabilidade da mesma na rede;
- h.7. Durante todo o período de garantia, a PROPONENTE deve substituir, recuperar e/ou modificar os softwares e firmwares instalados, sem ônus de qualquer natureza à EAF, nos casos comprovados de mau funcionamento, de modo a ajustá-los aos resultados que atendam às especificações técnicas solicitadas para a nova solução de telecomunicações, ou para a parte de gerência.

i) Certificado de Conformidade

- i.1. A exigência de Certificado de Homologação ANATEL aplica-se exclusivamente aos componentes fornecidos como appliance de hardware sujeitos ao Regulamento de Avaliação da Conformidade e de Homologação (Resolução ANATEL nº 715/2019);
- i.2. O certificado de conformidade não se aplica aos componentes de software e aos componentes entregues de forma virtualizada;
- i.3. Para os appliances de hardware, a PROPONENTE deverá apresentar o Certificado de Homologação quando a natureza do produto assim o exigir. Em caso de dispensa dessa certificação por característica do produto, a PROPONENTE deve apresentar documento da ANATEL confirmando a não necessidade dessa homologação;
- i.4. Esse Certificado de Homologação deverá ser apresentado no envio da PROPOSTA Técnica/Comercial;
- i.5. Todos os custos associados à homologação, quando necessário, serão por conta da PROPONENTE;
- i.6. O equipamento deve ser etiquetado de acordo com os requisitos do Regulamento de Avaliação da Conformidade e de Homologação (Resolução ANATEL nº 715/2019).

j) Sobressalentes

- j.1. A PROPONENTE deverá disponibilizar peças sobressalentes para o sistema na ativação comercial. As peças sobressalentes devem representar pelo menos 5% do valor total do hardware do sistema;
- j.2. Após o término da garantia, a PROPONENTE deverá fornecer sobressalentes que sejam compatíveis em forma, montagem e funcionamento pelo prazo de 2 (dois) anos;
- j.3. O preço dos sobressalentes deverá ser cotado unitariamente em LPU, conforme o "03_Anexo_C-LPU-Proposta_Comercial_OSS_BSS";
- j.4. Se após o período de 05 (cinco) anos a PROPONENTE tender a descontinuar a fabricação de quaisquer partes dos suprimentos, objeto deste contrato, a PROPONENTE deverá notificar a EAF com pelo menos 01 ano de antecedência dessa descontinuação. A PROPONENTE deverá oferecer a EAF a oportunidade de solicitar, a um preço razoável, as quantidades de peças de reposição que a EAF possa razoavelmente exigir em relação à vida útil prevista dos suprimentos.

k) Requisitos de Manutenção e Suporte Operacional

	RFP – Request for Proposal	Página 53 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- k.1. A PROPONENTE deverá estabelecer contato com a equipe de Operação e Manutenção da EAF e prover atualizações sobre os problemas relacionados ao Hardware/Software, que possam ser gerados e/ou resolvidos em qualquer outro mercado/operação, em periodicidade mensal;
 - k.2. A escalção ao Terceiro Nível de suporte será gerenciada pelos termos do Acordo de Nível de Serviço (SLAs), sendo gerenciada pelos representantes responsáveis da equipe de Operação e Manutenção da EAF de nível 2 (L2), onde a PROPONENTE precisa estar em cooperação total com os representantes de Operação e Manutenção da EAF;
 - k.3. Após restaurações de falhas, o suporte nível 3 (L3) deverá enviar um relatório por escrito contendo a descrição detalhada dos problemas, com recomendações de ações para mitigação e resolução, as quais deverão ser revisadas e acompanhadas em reuniões regulares com a operadora e os representantes da equipe de Operação e Manutenção da EAF;
 - k.4. Com o objetivo de apoiar a EAF na operação da rede, a PROPONENTE deverá oferecer serviço de Operação Assistida no período de 12 (doze) meses em regime de 8x5;
 - k.5. Para o serviço de Operação Assistida, a PROPONENTE deverá manter localmente (on-site), no mínimo, 1 (um) recurso, além dos recursos que ficarão disponíveis remotamente;
 - k.6. A emissão do Termo de Aceitação Definitiva (TAD), ou a entrada da Solução em Operação Comercial, marca o início dos serviços de Operação Assistida.
- I) Desenvolvimento de Competências e Transferência de Conhecimento
- I.1. A PROPONENTE deverá executar o desenvolvimento de competências e serviços de transferência de conhecimento para viabilizar à EAF a construção de competência técnica e conhecimento a todos os recursos existentes de operações/otimização e Serviços Gerenciados, aumentando assim, a eficiência e qualidade dos serviços entregues, satisfação do usuário final e redução de custos, garantindo a confiabilidade, segurança e a informação atualizada durante o contrato;
 - I.2. A PROPONENTE deverá disponibilizar informações corretas no tempo adequado às Equipes do Cliente e Serviços Gerenciados que requeiram tais informações, a fim de possibilitar ao Cliente a correta tomada de decisões. As responsabilidades da PROPONENTE dos serviços de gerenciamento de conhecimento deverão incluir:
 - a. Atualização de banco de dados de conhecimento contendo todos os eventos, incidentes e problemas, com a revisão do conteúdo em periodicidade semanal;
 - b. Acesso completo aos especialistas da PROPONENTE e ao sistema de treinamentos/transferência de conhecimento pelas equipes da EAF e de Serviços Gerenciados;
 - c. Treinamentos adequados ao uso do banco de dados de conhecimento às equipes da EAF e Serviços Gerenciados;
 - d. Plano completo de treinamentos, desenvolvimento de competências e transferência de conhecimento com pontos de controle (“milestones”) claramente definidos, Estrutura Analítica de Projetos (EAP) - conhecida também como WBS,

	RFP – Request for Proposal	Página 54 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

tópicos de treinamento e desenvolvimento, pré-requisitos, entregáveis esperados, prazos, relatando periodicamente o andamento da implementação deste plano à EAF;

- I.3. A PROPONENTE proverá treinamentos e o desenvolvimento contínuo de transferência de competências às equipes da EAF e Serviços Gerenciados sempre e quando necessário, incluindo treinamentos de produtos e plataformas da empresa fornecedora, suporte à operação e manutenção e otimização de performance de todos os equipamentos da PROPONENTE e todo e qualquer produto de terceiros se houver, incluindo e não limitado a:
- a. Gerenciamento de Falhas;
 - b. Configuração de Sistema;
 - c. Gerenciamento de Mudanças;
 - d. Gerenciamento de Performance;
 - e. Vigilância e monitoração da rede e performance;
 - f. Gerenciamento de Problemas;
 - g. Atualizações e upgrades de software e implementações de FNI;
 - h. Aceitação de novos elementos de rede e comissionamento;
 - i. Conceitos básicos sobre expansão de hardware e software da solução;
 - j. Upgrades de hardware;
 - k. Monitoração de performance de rede e otimização;
 - l. Integração de rede, rollout e serviços de implantação;
- I.4. O escopo de tais treinamentos e a transferência de competências devem incluir as equipes da EAF e de Serviços Gerenciados responsáveis pela operação e manutenção e otimização dos sistemas disponibilizados pela PROPONENTE;
- I.5. A PROPONENTE deve oferecer treinamentos (presenciais, ou remotos) que possibilitem a EAF a operar o sistema;
- I.6. A PROPONENTE deve disponibilizar as ementas dos respectivos treinamentos;
- I.7. A PROPONENTE não fará alterações de atualizações tecnológicas nos equipamentos, e/ou software, e/ou mudanças nos serviços suportados, a menos que as equipes da EAF e de Serviços Gerenciados tenham recebido treinamento com antecedência nos novos equipamentos, e/ou software, e/ou serviços de suporte relacionados;
- I.8. A PROPONENTE prontamente notificará a EAF de quaisquer requisitos de treinamento, para assegurar a certificação.

	RFP – Request for Proposal	Página 55 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

5. Serviços Previstos

a) Projeto – Implantação

- a.1. Validação do modelo de licenciamento e dimensionamento da solução;
- a.2. Site Survey – avaliação do local físico onde serão instalados os equipamentos, para verificações de questões relacionadas à localização de bastidores, energização, aterramento, caminho de fibras, calhas, esteiras, pontos de conexão com a rede da EAF, etc;
- a.3. Elaboração de Relatório PPI (Projeto Provisório de Instalação) fotográfico e com as informações do site, para validação da EAF;
- a.4. Após o aceite da instalação pela EAF, a PROPONENTE deverá elaborar/atualizar o Relatório PDI (Projeto Definitivo de Instalação);
- a.5. A PROPONENTE deverá fornecer documentação completa do projeto com HLD (High Level Design) e LLD (Low Level Design), incluindo nesses documentos, a descrição detalhada de toda a solução;
- a.6. A PROPONENTE deverá disponibilizar Projeto Executivo, HLD e LLD por ferramenta/solução a ser fornecida, objeto dessa RFP;
- a.7. A PROPONENTE deverá apresentar um cronograma de implantação, seguindo sugestões de priorização, para cada ferramenta/solução a ser fornecida, objeto dessa RFP;
- a.8. O cronograma deve contar com a fase inicial de levantamento e investigação do ecossistema existente e da Rede Privativa de Governo, onde serão definidas as informações que serão utilizadas no projeto.

b) Entrega de Equipamentos

- b.1. É de responsabilidade da PROPONENTE a entrega, recebimento, conferência e acomodação de todos os materiais e equipamentos desta contratação, até a sua instalação final;
- b.2. A entrega de cada equipamento deverá ser realizada no destino final de instalação;
- b.3. Entre a fase de recebimento do material e entrega definitiva em campo pela PROPONENTE, o armazenamento deverá ser feito em Warehouse da própria PROPONENTE, sem custos para a EAF.

c) Instalação;

- c.1. Instalação de todos os elementos de rede nos gabinetes/bastidores;

	RFP – Request for Proposal	Página 56 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- c.2. Energização dos equipamentos, de acordo com o projeto e com as posições de PDU/Disjuntores que forem verificadas e aprovadas na vistoria de implantação (Site Survey);
 - c.3. Passagem de cabos e fibras ópticas, de acordo com o projeto e com o que for aprovado na vistoria de implantação (Site Survey);
 - c.4. As fibras ópticas fornecidas pela PROPONENTE devem ser MONOMODO ou MULTIMODO. Essa definição se dará em tempo de projeto, de acordo com o que for aprovado pela EAF na análise do relatório de Site Survey;
 - c.5. Todos os cabos e fibras devem ser devidamente identificados de acordo com a padronização a ser definida na fase de Service Investigation;
 - c.6. A PROPONENTE deverá fornecer e instalar todos os materiais necessários para a conexão óptica/elétrica e cabos de energia para energização dos equipamentos incluindo as conexões com outros equipamentos existentes, e com elementos de Acesso Remoto a Console (gerência out-of-band), etc., em qualquer horário e qualquer dia de semana. Deverão ser consideradas todas as conexões definidas na Topologia do projeto;
 - c.7. Todos os materiais necessários para a completa instalação dos equipamentos deste projeto deverão ser fornecidos (conectores, cabos de energia e sinal, identificações, , kits de fixação, etc.) pela PROPONENTE;
 - c.8. A PROPONENTE deverá providenciar a retirada do local de sobra de material de instalação e eventuais equipamentos não utilizados, responsabilizando-se pela destinação adequada dos resíduos e materiais gerados e eventuais equipamentos não utilizados.
- d) Comissionamento, Integração e Testes
- d.1. Comissionamento de todos os elementos da solução;
 - d.2. Integração de todos os elementos da solução internamente, e com elementos externos (LAN, BBIP, Roteadores, Switches, SD-WAN, Gerência, Alarmística, etc...) a fim de deixar a solução pronta para os testes fim a fim;
 - d.3. A PROPONENTE deve realizar testes de conectividade em todas as integrações necessárias para o correto funcionamento da Solução;
 - d.4. A PROPONENTE deve realizar testes de funcionalidade (fim a fim) para validação da Solução;
 - d.5. A PROPONENTE deve apoiar a EAF nos testes de aceitação da Solução;
 - d.6. O caderno de testes de aceitação deve ser construído em comum acordo entre a PROPONENTE e a EAF;
- e) Aceitação
- e.1. Devem ser realizados Testes de Aceitação em conjunto (PROponente e EAF) a fim de garantir o correto funcionamento de cada ferramenta/solução de OSS/BSS;

	RFP – Request for Proposal	Página 57 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- e.2. Em relação à parte física, a PROPONENTE deverá comprovar a conformidade com o que foi aprovado no relatório de Site Survey e com o Projeto Técnico;
 - e.3. Em relação à parte lógica, a PROPONENTE deverá comprovar a conformidade com relatório comprobatório de testes;
 - e.4. A EAF emitirá Termos de Aceitação Provisória (TAP), caracterizando o início do Período de Funcionamento Experimental (PFE), para cada ferramenta/solução de OSS/BSS, objeto dessa RFP;
 - e.5. O TAP será emitido ao término dos Testes de Aceitação, se não houver pendências nos serviços executados, ou se a natureza das mesmas não impedir a ativação experimental dos equipamentos e/ou sistemas, ou não comprometer o desempenho e a segurança operacional, bem como as atividades de O&M. Este documento deverá ainda relacionar as eventuais pendências não impeditivas citadas;
 - e.6. O Período de Funcionamento Experimental (PFE), iniciado na data de emissão do Termo de Aceitação Provisória, visa a medição da confiabilidade e/ou desempenho dos equipamentos, serviços e/ou sistemas, com duração de 30 (trinta) dias, após o qual, inexistindo condicionantes pendentes de implantação, a EAF poderá emitir o Termo de Aceitação Definitiva (TAD);
 - e.7. Durante o PFE as ferramentas/soluções poderão ou não ser colocados em Operação Comercial, a critério da EAF;
 - e.8. Durante o PFE poderão ser levantadas novas pendências, não incluídas inicialmente no TAP, as quais deverão ser eliminadas pela PROPONENTE até o término do PFE, ou, em casos de baixa criticidade, acordado um compromisso de data para a resolução entre PROPONENTE e EAF através de Termo de Compromisso;
 - e.9. No caso do surgimento de falhas que comprometam o desempenho e/ou a segurança operacional dos equipamentos e/ou sistemas, o PFE deverá ser reinicializado após a remoção das mesmas, por um novo período de 30 (trinta) dias;
 - e.10. Durante o PFE, contado a partir da emissão do TAP, a PROPONENTE colocará à disposição da EAF, técnicos para a operação e manutenção dos equipamentos, sem ônus para a mesma;
 - e.11. Ao término do PFE, desde que não haja pendências de qualquer natureza, a EAF emitirá TERMO DE ACEITAÇÃO DEFINITIVA (TAD);
 - e.12. A emissão do TAD, ou a entrada da ferramenta/solução em Operação Comercial, marca o início dos Serviços de Suporte Técnico e Operação Assistida.
- f) Gerência de Projeto de Implantação
- f.1. A Gerência do Projeto deverá seguir as melhores práticas de gerenciamento de projetos do mercado;
 - f.2. A metodologia deverá utilizar ferramentas e padrões baseados no PMI – Project Management Institute, permitindo-se adaptações em comum acordo entre PROPONENTE e EAF;

	RFP – Request for Proposal	Página 58 de 58
	Contratação RFP OSS/BSS	Edição Versão 3.0
		Data: 15/07/26

- f.3. A PROPONENTE será responsável por realizar o planejamento do projeto, com acompanhamento da EAF, e garantir um andamento adequado do projeto com relação às metas e objetivos planejados, gerenciando riscos, tomando ações preventivas e corretivas sobre o projeto;
- f.4. O gerenciamento de projetos da PROPONENTE deve coordenar a prestação dos serviços no projeto e interagir constantemente com a EAF, posicionando-a sobre o seu andamento.