Estudo Técnico Preliminar 42/2021

1. Informações Básicas

Número do processo: 02070.005297/2021-34

2. Descrição da necessidade

2.1 Características Institucionais do ICMBio

O Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio), autarquia federal em regime especial, vinculada ao Ministério do Meio Ambiente (MMA), instituído pela Lei n.º 11.516 de 29 de agosto de 2007, tem por missão institucional proteger o patrimônio natural e promover o desenvolvimento socioambiental, mediante a execução de ações do Sistema Nacional de Unidades de Conservação (SNUC), podendo, para tanto, propor, implantar, gerir, proteger, fiscalizar e monitorar as Unidades de Conservação (UCs) instituídas pela União, bem como fomentar e executar programas de pesquisa, proteção, preservação e conservação da biodiversidade, e exercer o poder de polícia ambiental para a proteção das UCs federais.

As ações do ICMBio estão vinculadas ao Planejamento Estratégico Integrado do Ministério do Meio Ambiente de suas Entidades Vinculadas 2020-2023, instituído pela Portaria Conjunta nº 266, de 17 de junho de 2020, que materializa o esforço conjunto das instituições federais de Meio Ambiente em definir uma estratégia que integre a missão, visão de futuro e os objetivos das instituições responsáveis pela formulação e implementação da política ambiental.

Desta forma, o Planejamento Estratégico Integrado é a ferramenta de gestão que orienta os agentes tomadores de decisão e estabelece as prioridades a serem seguidas pelo Ministério do Meio Ambiente - MMA, Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis – IBAMA, Instituto Chico Mendes de Conservação da Biodiversidade – ICMBio, e Jardim Botânico do Rio de Janeiro – JBRJ.

Atualmente, com 334 (trezentas e trinta e quatro) Unidades de Conservação, o Instituto possui uma estrutura institucional apoiada por aproximadamente 4.500 (quatro mil e quinhentos) colaboradores lotados nas diversas Unidades distribuídas em todo o território nacional, equipes que atuam nos 754.599,30 km² (setecentos e cinquenta e quatro mil, quinhentos e noventa e nove, vírgula trinta centésimos de quilômetros quadrados), de áreas protegidas de responsabilidade do Governo Federal.

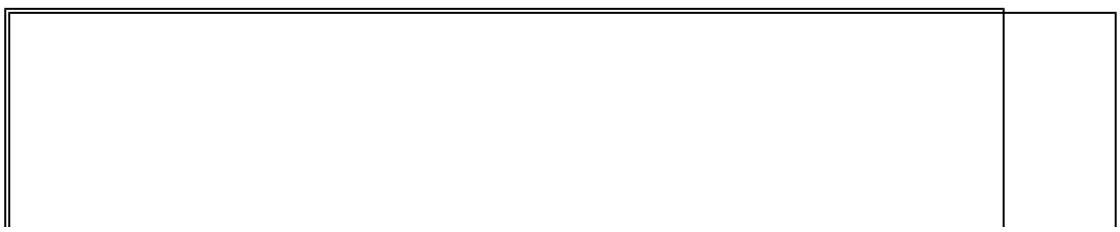
2.2 Modernização da infraestrutura da Rede Nacional de Computadores do ICMBio (Rede-ICMBio)

2.2.1 Características da Rede-ICMBio

Considerando que o ICMBio possui cerca de 241 (duzentos e quarenta e um) circuitos de redes internas de computadores localizadas nas Unidades de Conservação e todas interligadas à Sede em Brasília, compondo assim uma rede nacional de computadores para atender, em média, um total de 4.500 (quatro mil e quinhentos) usuários, é possível observar que, por suas próprias características, a rede nacional de computadores do Instituto é uma estrutura robusta e que requer o uso de recursos tecnológicos capazes de garantir sua alta disponibilidade com segurança e em alinhamento às normas e legislação pertinentes.

Neste contexto, a topologia de rede de infraestrutura do ICMBio do tipo MESH, composta de pontos de acessos e clientes, é utilizada para trafegarem de vários nós/roteadores, que passam a se comportar como uma única e grande rede, possibilitando que os usuários se conectem em qualquer um destes nós.

Desta forma, as Unidades de Conservação - UCs do ICMBio estão conectadas à Sede por meio de conexões via MPLS (conforme *Figura 01 - Topologia MPLS do ICMBi*o, ilustrada abaixo) compondo a rede nacional de computadores do ICMBio, em que a topologia implementada obriga que todos os pacotes de dados enviados e recebidos pelas UCs trafeguem pela Sede, uma vez que é na sede que ocorre todo o monitoramento de tráfego de dados e onde são aplicadas as regras de segurança.



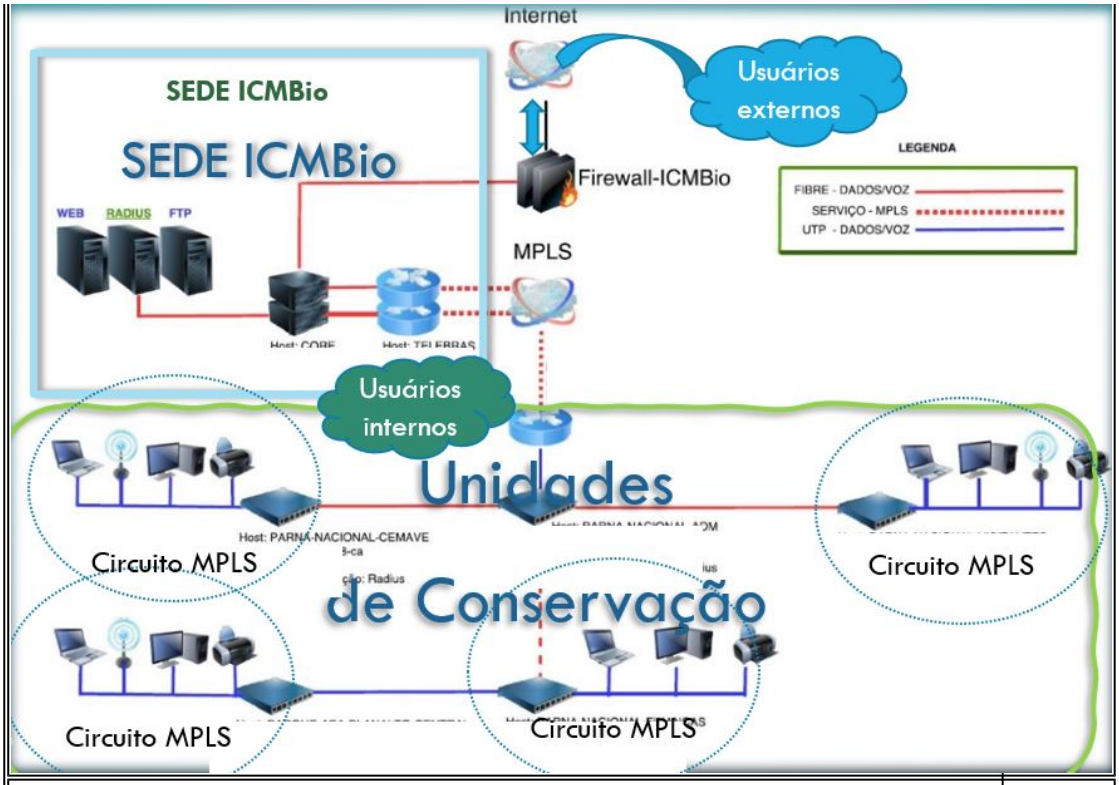


Figura 01 - Topologia MPLS do ICMBio

Conforme consta na Figura 01, o acesso à internet para as UCs depende do link de acesso à internet da Sede do ICMBio, mantido pelo serviço da INFOVIA, por meio do Serviço Federal de Processamento de Dados - SERPRO.

Além dos serviços de acesso à internet, o serviço de Voz sob IP (VOIP) também é mantido utilizando a rede MPLS. Infere-se dos estudos das documentações relacionadas ao histórico da rede ICMBio, que a opção por este tipo de topologia está vinculado à necessidade de garantir a segurança da rede possibilitando ainda o acesso dos Servidores e Colaboradores das Unidades de Conservação, localizadas em diversos estados do Brasil, aos serviços internos localizados na sede em Brasília - DF.

2.2.2 Implantação do Firewall de próxima Geração na Rede-ICMBio

Conforme previsto no PDTIC 2020-2021, em maio de 2021, por meio do Contrato nº 28/2020 celebrado com a L8 Group, foi instalada a solução de segurança composta por um Firewall Check Point modelo QUANTUM 6900 SECURITY GATEWAY, em cluster com 2 appliances incluindo todo o licenciamento de aplicação e software de gerenciamento necessários ao pleno funcionamento da solução com suporte 24x7 por 60 (sessenta) meses.

Para as funções de gerência do firewall Quantum 6900, foi fornecido o Módulo de Gerência R80.40 que se refere à uma solução virtual de gerenciamento unificado para redes físicas e virtuais. Dessa forma, por causa de limitações no Datacenter do ICMBio, essa solução de gerência encontra-se atualmente instalada no Datacenter do Ministério do Meio Ambiente sob gestão da equipe de infraestrutura do ICMBio de forma remota. Ademais, por se tratar de uma solução virtual, o módulo de gerência pode atuar instalado em uma máquina virtual dentro do Datacenter do ICMBio ou em nuvem. Por consolidar todos os aspectos do ambiente de segurança do ICMBio de forma contínua, ele permite a implantação e atualização de proteções em toda a rede.

O módulo de Gerência, mesmo contendo um universo extenso de funcionalidades e requisitos de segurança implementados, possibilita a montagem de recursos de fácil monitoramento, em painel visual personalizável, facilitando a criação de telas de monitoramento que permitem a identificação rápida de situações suspeitas ajudando a simplificar o monitoramento e automatizar os alertas. Além disso, a solução é escalável e extensível, desta forma, à medida que a Rede ICMBio evolui é possível implementar recursos para melhor adequação às necessidades do Instituto.

Com a implantação da solução de segurança, além da Sede, todos os circuitos MPLS (conexões das Unidades de Conservação) passaram a ser monitorados com a aplicação de recursos de firewall de próxima geração, tais como:

- Segurança avançada com prevenção autônoma de ameaças: Sistema autônomo de prevenção de ameaças do setor, todos os gateways são atualizados automaticamente por mais de 60 mecanismos de prevenção de ameaças de Inteligência Artificial (IA) e de Aprendizado de Máquina (ML) para proteção completa contra ameaças de dia zero.

- Resposta ágil às necessidades de segurança com instalação de política mais rápida: O tempo de instalação de política reduzido em até 90%, de minutos para segundos. Além disso, os administradores de segurança podem atualizar centenas de gateways remotos para a nova versão com o clique de um botão.
- Ajuste automático de desempenho: Uso de alocação dinâmica de recursos de gateway em toda a Rede-ICMBio para fornecer automaticamente o melhor desempenho e segurança de hardware.
- Melhoria da segurança para tráfego de rede criptografado (SSL): Utilizando os padrões mais recentes para conectividade segura, incluindo TLS 1.3 e HTTP/2, evita-se que as ameaças se escondam no tráfego criptografado. Desta forma, uma camada de política dedicada permite que o administrador controle a decisão de quanto inspecionar ou ignorar o tráfego de rede.

A ação acrescentou maior agilidade e segurança das transações de pacotes da Rede ICMBio, tanto para a Sede quanto para as conexões MPLS. Para tanto, conforme citado anteriormente, o ICMBio possui o Contrato nº 28/2020, referente à solução integrada de Firewall NEXT GENERATION composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management), traduzido do inglês para Gerenciamento Unificado de Ameaças, conforme ilustrado na *Figura 02 - Topologia MPLS do ICMBio com Firewall de próxima geração*, a seguir:

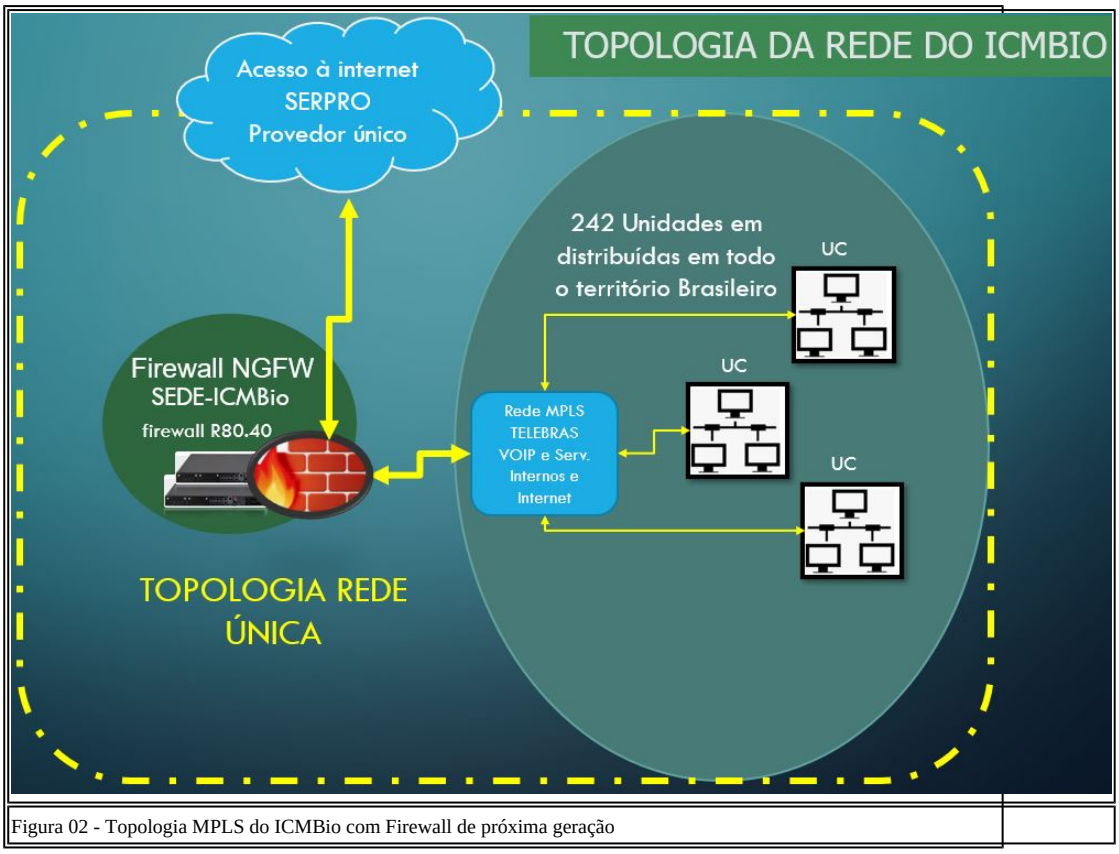


Figura 02 - Topologia MPLS do ICMBio com Firewall de próxima geração

2.2.3 Impactos da utilização de serviços MPLS

Tendo em vista que o ICMBio precisa garantir a segurança do tráfego de dados, além de implementar serviços internos como VPN e Telefonia VOIP, desde a sua criação a rede ICMBio foi projetada considerando-se a tecnologia MPLS como a solução mais viável para atender as necessidades de conectividade e segurança da Rede-ICMBIO. Neste contexto, cabe citar as características gerais destes serviços, conforme definições presentes na wikipedia, *In verbis*:

> "*MPLS, ou MultiProtocol Label Switching, é uma tecnologia de encaminhamento de pacotes baseada em rótulos (labels) que funciona, basicamente, com a adição de um rótulo nos pacotes (O MPLS é indiferente ao tipo de dados transportado, pelo que pode ser tráfego IP ou outro qualquer) à entrada do backbone (chamados de roteadores de borda) e, a partir daí, todo o encaminhamento pelo backbone passa a ser feito com base neste rótulo. Comparativamente ao encaminhamento IP, o MPLS torna-se mais eficiente uma vez que dispensa a consulta das tabelas de roteamento.*
>
> *Este protocolo permite a criação de Redes Virtuais Privadas garantindo um isolamento completo do tráfego com a criação de tabelas de "labels" (usadas para roteamento) exclusivas de cada VPN.*
>
> *Além disso é possível realizar QoS (Quality of Service) com a priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos da VPN. QoS cria as condições necessárias para o melhor uso dos recursos da rede, permitindo também o tráfego de voz e vídeo.*

Os produtos que as operadoras utilizam baseados em MPLS permitem que elas possam agregar valor ao seus produtos, pois passam a não oferecer apenas banda, mas um tráfego diferenciado com: Multimídia (Voz, Vídeo e Dados) e aplicações críticas, com garantias aplicáveis de QoS, através das seguintes classes de serviço:

- *Multimídia: priorização de tráfego dos pacotes multimídia (ex.: vídeo conferência, etc.).*
- *Voz: priorização de tráfego dos pacotes de voz (ex.: interligação de PABX, telefonia IP, etc.).*
- *Dados Expressos: priorização de tráfego de dados de aplicações críticas (ex.: SAP, GVCollege, etc.).*
- *Dados: tráfego de dados sem priorização (Best Effort).*

O MPLS foi concebido para satisfazer as necessidades de infraestrutura de comunicação segura e economicamente viável entre:

- *escritórios de uma mesma empresa em diferentes localidades;*
- *força de trabalho em constante deslocamento;*
- *empresa, clientes, fornecedores.*

O produto baseado em MPLS, oferecidos pelas operadoras, permite que ele possa ser utilizado nas seguintes situações:

- *acesso corporativo a servidores de aplicações centralizadas como sistemas corporativos, e-mail e Intranet;*
- *formação de redes para compartilhamento de arquivos;*
- *integração de sistemas de telefonia;*
- *formação de sistemas de videoconferência;*
- *acesso remoto aos sistemas corporativos."*

Desta forma, o MPLS foi adotado na concepção da Rede-ICMBio tendo em vista a necessidade de atender as demandas dos servidores e colaboradores do ICMBio, uma vez que estão localizados em várias unidades distribuídas em todo o território nacional e portanto, necessitam da utilização de serviços como Telefonia VOIP, Acesso a sistemas, Vídeo-Conferência, Armazenamento de dados, E-mail e Intranet. Algumas características dessa tecnologia implementada no Instituto são:

a) Manutenção complexa - Com o uso do serviço MPLS, os fornecedores precisam manter uma infraestrutura onde todos os pontos de conexão da rede são monitorados. Isso implica em investimentos com ativos de rede e soluções de monitoramento e gerenciamento de bandas e serviços vinculados, além de envolver o custo de subcontratações de serviços de provedores e prestadores de serviços para a garantia do bom funcionamento da rede, fatores que, apesar de agregar valor ao serviço, agregam custos elevados.

b) Custo mensal elevado - Neste cenário de necessidade contínua de manutenção de infraestrutura MPLS, os custos mantidos pelo fornecedor e repassados para o ICMBio (ANEXO I) tornam o contrato bastante oneroso, conforme ilustrado no quadro a seguir:

CUSTO MÉDIO DOS SERVIÇOS MPLS		
QUANTIDADE DE CIRCUITOS	**VALOR MÉDIO**	**VALOR TOTAL MENSAL**
241	R$ 4.605,61	R$ 1.109.952,21
VALOR MÉDIO ANUAL		R$ 13.319.426,52

c) Topologia de rede única - Com o uso dos serviços MPLS, as redes internas das Unidades de Conservação funcionam de forma totalmente dependente do Datacenter do ICMBio localizado na sede, uma vez que todo o tráfego de dados é obrigado a passar pela sede, conforme ilustrado na *Figura 02 - Topologia MPLS do ICMBio com Firewall de próxima geração*. Desta forma, caso ocorra a indisponibilidade do serviço de acesso à internet na Sede, todas as Unidades do ICMBio são desconectadas, ficando impossibilitadas de utilizar qualquer serviço disponível na internet.

d) Qualidade de serviços limitada - Como a contratação dos serviços MPLS está vinculada à infraestrutura do fornecedor, todos os circuitos estão sujeitos à mesma infraestrutura, ou seja, um único fornecedor precisa ser capaz de proporcionar qualidade de serviço em todas as regiões do país. Dessa forma, o fornecedor precisa ter gestão em todos os equipamentos que fazem parte da rede, o que raramente ocorre. De acordo com a experiência adquirida ao longo dos últimos 2 (dois) anos de gestão destes

serviços, restou verificado que em diversas regiões não há gestão célere do fornecedor quanto à melhoria dos circuitos na última milha prejudicando a qualidade dos serviços entregues e morosidade para a correção de falhas.

e) Banda de acesso insuficiente - Devido aos custos elevados dos serviços MPLS frente às limitações orçamentárias, a ampliação das bandas dos links atuais de forma a garantir a melhor experiência de acesso à internet para todas as unidades implicaria em um aumento de custos superior ao limite máximo de 25% permitido pela lei de licitações e contratos.

f) Catálogo de serviço limitado - A atual contratação dos serviços MPLS define um único tipo de serviço para atender a todas as unidades, fato que não atende a demanda do ICMBio, que tem, por suas características de capilaridade e diversidade de necessidades regionais, demandas por serviços diferenciados dependendo da região ou das características da Unidade que vai ser atendida.

2.2.4 Modernização da infraestrutura e serviços da Rede-ICMBio

Com a modernização da infraestrutura da Rede-ICMBio, mais perceptível nos últimos 02 (dois) anos, e ainda com a implementação da solução de segurança ocorrida no ano corrente, o ICMBio passou a ter a possibilidade de implementar outras soluções alternativas ao MPLS, mais baratas e com níveis de segurança similares ou superiores, uma vez que com a evolução das tecnologias utilizadas na Rede-ICMBio, não há mais a dependência dos serviços MPLS para o atendimento das demandas dos servidores e colaboradores do Instituto uma vez que:

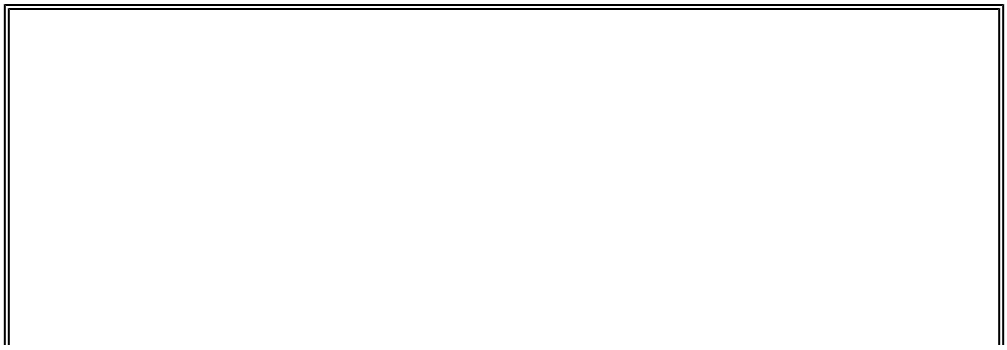
1. Os sistemas do ICMBio por estarem em ambiente web, podem ser acessados de qualquer computador ou dispositivo móvel que tenha internet. Assim sendo, os colaboradores e gestores do Instituto podem verificar e administrar dados remotamente e em qualquer horário.
2. Os serviços de vídeo conferência utilizados pelos usuários da Rede-ICMBio são ofertados por plataformas em nuvem, dispensando a necessidade do uso do serviço MPLS.
3. O Portal do ICMBio, os serviços de e-mail e intranet estão em nuvem, desta forma poder ser acessados de qualquer computador com acesso à internet, o que dispensa a necessidade do serviço MPLS.
4. O serviço de VoIP poderá funcionar por meio de uma VPN site-to-site configurada em um Firewall na UC. Esse teste foi realizado por meio de uma Prova de Conceito - POC, realizada em Goiânia-GO, no Centro Nacional de Pesquisa de Répteis e Anfíbios - RAN, em que foi possível verificar a viabilidade técnica da implantação de um módulo de segurança em uma Unidade de Conservação, transformando-a em uma rede filial.

2.2.5 Características necessárias para a composição da Solução de TI para a infraestrutura e serviços da Rede-ICMBio

2.2.5.1 Ainda que se verifique a possibilidade do uso de soluções alternativas ao serviço MPLS, é necessário que se garanta a evolução das ferramentas de segurança da Rede-ICMBio, uma vez que as demandas por melhorias quanto ao tratamento de dados e segurança cibernética são constantes, a exemplo da implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, legislação que exige o monitoramento constante de acessos e tráfego de dados pessoais, de modo a reduzir o risco de roubo de dados e demais ameaças cibernéticas.

2.2.5.2 Desta forma, a substituição dos serviços MPLS é vista como uma demanda necessária para tornar as redes internas das Unidades de Conservação do ICMBio mais independentes do Datacenter do ICMBio, além de possibilitar a utilização de serviços de acesso à internet diferenciados conforme as condições de cada região, uma vez que as cidades e os estados brasileiros estão em diferentes estágios de desenvolvimento tecnológico no que se refere aos serviços de banda larga e outros tipos de acesso à internet.

2.2.5.3 Conforme consta ilustrado na *Figura 03 - Distribuição dos Circuitos MPLS da Rede-ICMBio no Brasil,* a seguir, verifica-se que os circuitos que atendem as Unidades de Conservação estão distribuídos em todo o território nacional, e portanto, se faz necessário que a solução a ser adquirida seja capaz de possibilitar acesso à internet com segurança para todos os usuários da Rede-ICMBio, utilizando-se para isso, as condições de oferta de serviços de acesso à internet mais adequado a cada localidade.



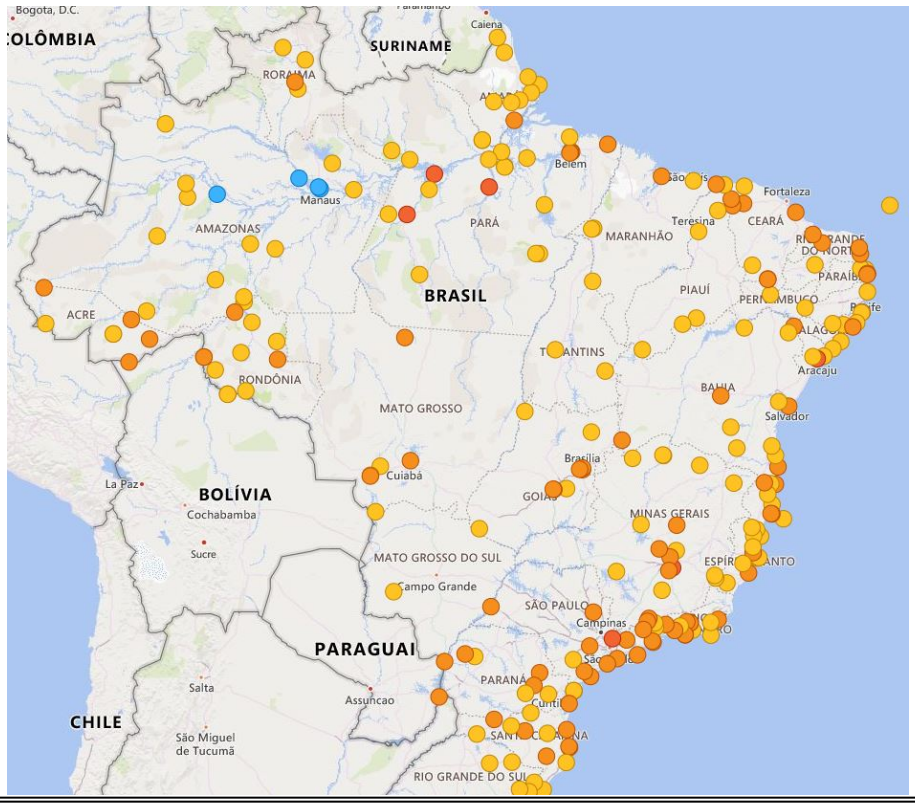


Figura 03 - Distribuição dos Circuitos MPLS da Rede-ICMBio no Brasil

2.2.5.4 Neste cenário em que o ICMBio possui o desafio de encontrar soluções de tecnologia da informação capazes de alcançar o bom funcionamento da Rede-ICMBio garantindo os níveis de segurança necessários e ainda otimizar os recursos de modo a reduzir custos, se faz necessário o estudo de solução de melhoria da infraestrutura da Rede-ICMBio.

2.2.5.5 Além disso, considerando os investimentos já realizados pelo ICMBio que proporcionaram a implementação de ferramentas avançadas de segurança da informação, como: Firewall Check Point modelo QUANTUM 6900 SECURITY GATEWAY e o Módulo de Gerência R80.40, todos com licenciamento e atualização com suporte 24x7 por 60 (sessenta) meses, verifica-se a necessidade de que as soluções a serem implementadas garantam total compatibilidade e integração com essas ferramentas de modo que sejam mitigados os riscos de outras soluções a serem adquiridas, reduzindo o alcance e a eficiência das soluções já implantadas no Instituto.

2.2.5.6 Desta forma, as soluções a serem adquiridas devem ser complementares ou extensões daquelas já em uso no ICMBio, de modo que sejam otimizados os recursos e simplificada a gestão. Neste contexto, o uso de soluções de segurança não compatíveis ou limitadoras daquelas soluções já existentes no ICMBio impossibilita a padronização benéfica do ponto de vista da continuidade de negócio, uma vez que quanto maior o universo de soluções de fabricantes diferentes e tecnologias distintas para o mesmo objetivo, maior será a exigência de capacitação e especialização dos recursos humanos que deverão operá-las, ou pelo menos compreender seu funcionamento para planejar o uso da forma mais adequada às necessidades institucionais, mantendo as condições mais adequadas à garantia de continuidade do negócio.

2.2.5.7 Portanto, a solução a ser adquirida visa melhorar o apoio tecnológico à realização da missão institucional do ICMBio, uma vez que deverá proporcionar a disponibilidade, confiabilidade, integridade e autenticidade dos dados e dos serviços prestados pelo Instituto e que, por sua vez, são necessários para atender com qualidade às expectativas de seus usuários.

2.2.5.8 Diante desses apontamentos, restou verificado que há a necessidade do estudo de extensão da solução de segurança da informação, implantada na sede do ICMBio, para as Unidades de Conservação, considerando os fatores já elencados visando o atendimento das demandas de:

1. Melhoria de segurança da rede;
2. Modernização e implementação de camadas de segurança à rede de computadores do ICMBio;
3. Redução da dependência das Unidades de Conservação para com a Sede;
4. Gerenciamento centralizado, simplificando o monitoramento das políticas de segurança;
5. Implementação de opções de serviços de acesso à internet adequados ao nível de segurança necessário e aos serviços disponíveis nas diversas regiões do Brasil.
6. Garantia de rastreabilidade de eventos que possam ter comprometido a segurança dos dados pessoais tratados no âmbito do ICMBio.

7. Implementação de ferramentas de monitoramento de ativos de redes e estações de trabalho nas Unidades de Conservação.
8. Monitoramento e identificação de atividades cibernéticas suspeitas que venha a ameaçar a segurança das informações institucionais e dados pessoais.

3. Área requisitante

Área Requisitante	Responsável
COTEC	Jaime Heleno Correa de Lisboa

4. Descrição dos Requisitos da Contratação

4.1 Requisitos de negócio

A solução de segurança a ser implementada nas Unidades de Conservação (redes filiais) devem atender aos seguintes requisitos:

4.1.1 Independência da Sede para utilização de serviços de acesso à internet

De modo a garantir às redes filiais da Rede-ICMBio a capacidade de continuarem em pleno funcionamento mesmo quando ocorram indisponibilidades nos serviços do Datacenter da Rede-ICMBio, se faz necessário que a solução de segurança (garantidos os mesmos níveis de proteção do firewall instalado na sede) permita que os usuários lotados nas redes filiais tenham acesso à internet sem a necessidade de que o tráfego dos dados passem pelo datacenter do ICMBio.

A solução deverá permitir com que as Unidades de Conservação utilizem serviços de acesso à internet ofertado por provedores locais de acordo com as tecnologias disponíveis na região: ADSL, satélite, IP dedicado ou modem 4G.

4.1.2 Replicação das mesmas regras e políticas praticadas na Sede

Embora precisem atuar de forma independente em relação à Sede em vários momentos, as redes filiais precisam operar com as mesmas regras de segurança aplicadas na Sede, uma vez que são partes da mesma instituição. Neste sentido, é preciso que a liberação de links ou criação de grupos de usuários com perfis de acesso diferenciados implementados na Sede sejam replicadas para todas as unidades do ICMBio, garantindo assim que em qualquer localidade o usuário tenha os mesmos privilégios de acesso e tenha seus registros controlados, além de facilitar a gestão desses recursos pela COTEC.

4.1.3 Disponibilização de sistema de proteção contra variações de tensão

Devido ao fato de que as Unidades de Conservação estão distribuídas em cidades onde, na maioria das vezes, não existem redes elétricas estabilizadas para a proteção dos equipamentos a serem instalados nestas unidades, se faz necessário a disponibilização de Nobreak/Estabilizador que garanta uma proteção contra descargas elétricas e variações de tensões, dando maior durabilidade aos equipamentos a serem adquiridos.

4.2 Requisitos Tecnológicos

Para garantir a rastreabilidade de acessos indevidos, a solução deverá possuir recurso para armazenamento de eventos relacionados ao tráfego de dados para registro e análise.

Para garantir a análise aprofundada e redução de riscos de acessos a sites e serviços comumente utilizados por hackers e que, portanto representam ameaças ou que prejudicam o uso otimizado dos recursos de acesso à internet, a solução deverá ser capaz de implementar filtragem de pacotes, controle de aplicações, administração de largura de banda, prevenção contra intrusão, rede virtual privada segura, prevenção contra código malicioso, filtro de endereços e controle de acesso à internet.

Possuir ambiente controlado para análise e acesso de endereços e execução de arquivos suspeitos.

A solução deve possuir um gerenciamento centralizado na Sede, fazendo com que todas as regras do Firewall da Sede sejam replicadas para as caixas das UCs, possuindo assim uma gestão unificada da solução.

4.3 Requisitos de Instalação

Tendo em vista que a solução de segurança a ser fornecida deverá funcionar de forma integrada com a solução de segurança já implantada na sede do ICMBio, será necessário que esta solução seja compatível com o equipamento instalado na Sede para que possa ser gerenciada pelo módulo de gestão que é a solução de gestão em operação no ICMBio, e portanto, quando da instalação a CONTRATADA deverá efetuar os procedimentos de integração com o módulo de gestão do ICMBio.

Para garantir a perfeita integração da solução com o parque tecnológico do ICMBio, e ainda, que os serviços de instalação sejam efetuados de acordo com as recomendações do fabricante, os serviços de instalação, configuração, repasse de tecnologia e operação assistida deverão ser executados por técnico certificado pelo fabricante da solução.

Deverá ser exigido à Contratada o repasse de tecnologia abrangendo aspectos gerais da solução de forma a prover informações suficientes para supervisão e gestão do ambiente, contemplando, também, a operação assistida com execução das principais tarefas administrativas do dia-a-dia, atuando em esclarecimentos, ajustes e eventuais correções.

A Contratada deverá fornecer os equipamentos sob demanda, ou seja, de acordo com a solicitação do ICMBio para as Unidades de Conservação que estiverem prontas para receber o equipamento. Portanto, após a solicitação de entrega via Ordem de Fornecimento, a Contratada deverá entregar os *Módulos de Segurança* na Sede do ICMBio. Estes equipamentos deverão ser entregues pré-configurados e com garantia de compatibilidade e integração à Rede-ICMBio.

Tendo em vista que não há servidores ou colaboradores com os conhecimentos técnicos necessários para a fiscalização técnica de recebimento e verificação dos *Módulos de Segurança* nas Unidades de Conservação, após a fase de implantação, a entrega de todos os itens será efetuada na sede do ICMBio, em Brasília - DF.

A opção pelo recebimento dos equipamentos na sede, em que pese o fato de que acarretará custos ao Instituto para o envio às Unidades de Conservação, deverá contribuir com a redução do custo de fornecimento junto aos LICITANTES uma vez que para o processo em questão, estes custos seriam inseridos no preço final, já que o ICMBio possui localidades em todo o Território Nacional, e portanto, todos os LICITANTES iriam considerar em seus custos os desafios logísticos de entregas e instalações em locais de difícil acesso como é o caso de muitas unidades da Região Norte do Brasil ou da ilha de Fernando de Noronha, por exemplo.

Ainda que não seja exigida a instalação de forma presencial em todas as Unidades de Conservação, deverá ser exigido da Contratada a disponibilização de suporte remoto para auxiliar as equipes locais do ICMBio em caso de dúvidas e demais orientações de instalação. Além disso, deverá ser exigido o fornecimento de um manual rápido simplificado de instalação dos equipamentos nas unidades para auxiliar as equipes locais.

5. Levantamento de Mercado

5.1. Quanto às opções tecnológicas para disponibilização dos serviços

Diante dos problemas relacionados aos serviços de acesso à internet entregue pela Rede-ICMBio para as Unidades de Conservação, predominantemente relacionados à utilização dos serviços MPLS, conforme elencados no capítulo 2 deste Estudo Técnico Preliminar, e, de modo à promover a composição de um hall de alternativas para a modernização da infraestrutura da Rede-ICMBio, com a substituição dos serviços MPLS, foram elencadas as seguintes possibilidades:

5.1.1 Alternativa 1 - Manter a Rede-ICMBio totalmente em MPLS (situação atual)

- **Pontos positivos:**
  - Manutenção dos serviços de VOIP;
  - Menor esforço para renovação/contratação de serviço;
  - Todos os serviços prestados pela mesma empresa facilitando a gestão para os fiscais.
- **Pontos negativos:**
  - Elevados custos de manutenção de infraestrutura repassados da CONTRATADA para o ICMBio;
  - Hall limitado de oferta de bandas de acesso à internet;
  - Banda de acesso à internet insuficiente para atendimento da maioria das Unidades de Conservação;
  - Baixa qualidade dos serviços entregues;
  - Demora para solução de incidentes;
  - Demora para instalação ou mudança de links (prazo contratual de 120 dias);
  - Impossibilidade de atuação das equipes de TI do ICMBio nos ativos da CONTRATADA.

5.1.2 Alternativa 2 - Fragmentaçaõ da Rede-ICMBio em redes filiais com a retirada gradativa dos serviços MPLS

- **Pontos positivos:**

- Manutenção dos serviços de VOIP;
- Possibilidade de contratação de links redundantes;
- Possibilidade de contratação de serviços comuns de acesso à internet como: ADSL, IP dedicado e 4G;
- Possibilidade de contratação de bandas maiores do que as com serviços MPLS;
- Possibilidade de monitoramento da disponibilidade tanto da equipe local quanto da equipe da Sede;
- Controle total dos ativos pela equipe de TI do ICMBio;
- Maior agilidade para a correção de incidentes, uma vez que os ativos de rede seriam todos de propriedade do ICMBio e sob gestão da COTEC;
- Redução de aproximadamente 60% do custo mensal dos serviços para as unidades que forem migradas, conforme detalhado no item 6 deste ETP;
- Possibilidade de realização do projeto de forma gradual, reduzindo os riscos e os impactos da mudança.

- **Pontos negativos:**
  - Necessidade de contratação separada de links para as Unidades de Conservação;
  - Necessidade de investimento com a aquisição de módulos de segurança para as redes filiais;
  - Manutenção de algumas Unidades de Conservação com serviços MPLS (que permaneceriam com os pontos positivos e negativos nas condições atuais).

5.1.3 Alternativa 3 - Substituir todos os serviços MPLS por serviços de acesso à internet de banda larga.

- **Pontos positivos:**
  - Manutenção dos serviços de VOIP;
  - Possibilidade de contratação de links redundantes;
  - Possibilidade de contratação de serviços comuns de acesso à internet como: ADSL, IP dedicado e 4G;
  - Possibilidade de contratação de bandas maiores do que as com serviços MPLS;
  - Possibilidade de monitoramento da disponibilidade tanto da equipe local quanto da equipe da Sede;
  - Controle total dos ativos pela equipe de TI do ICMBio;
  - Maior agilidade para a correção de incidentes, uma vez que os ativos de rede seriam todos de propriedade do ICMBio e sob gestão da COTEC;
  - Redução do custo mensal dos serviços;
  - Redução de aproximadamente 60% do custo mensal dos serviços para as unidades que forem migradas, conforme detalhado no item 6 deste ETP.

- **Pontos negativos:**
  - Necessidade de contratação separada de 241 links para as Unidades de Conservação de forma acelerada;
  - Necessidade de investimento com a aquisição de módulos de segurança para as redes filiais;
  - Necessidade da realização de investimento imediato para a aquisição de módulos de segurança;
  - Risco de haver a indisponibilidade de serviços para várias unidades durante a transição das condições atuais para a nova topologia e novos serviços;
  - Necessidade de migração rápida de uma grande quantidade de redes internas;
  - Dificuldades para a fiscalização da implementação dos serviços uma vez que o volume de atividades seria superior à capacidade de acompanhamento da equipe de servidores da COTEC.

5.2. Análise das alternativas elencadas

5.2.1 Considerando que o ICMBio historicamente possui limitações orçamentárias que, ano após ano, impossibilitam a realização de muitas ações de tecnologia da informação previstas no PDTIC, verifica-se que oportunidades de redução de custos devem ser avaliadas com prioridade, e neste sentido, é razoável que a ***Alternativa 01 - Manter a Rede-ICMBio Totalmente em MPLS (situação atual)*** seja descartada como solução a ser mantida na forma proposta, tanto pelo fato de ser a mais cara dentre as opções quanto por apresentar o maior hall de pontos negativos em relação às outras opções.

5.2.2 Verifica-se ainda que a ***Alternativa 3 - Substituir todos os serviços MPLS por serviços de acesso à internet de banda larga*** , embora exija maior investimento inicial em comparação às outras, representaria uma economia mensal superior, porém é a solução que representa maiores riscos de indisponibilidade dos serviços, uma vez que ao se efetuar a retirada dos serviços MPLS todas as Unidades de Conservação teriam o acesso a internet indisponível até que sejam contratados os links locais e instalados os módulos de segurança. Além disso, seria necessário a execução da migração de muitas unidades ao mesmo tempo impossibilitando o acompanhamento das equipes de TI do ICMBio. Desta forma, essa alternativa será descartada, uma vez que as ações de mitigação de riscos e a necessidade de investimentos imediatos tornam esta alternativa inviável.

5.2.3 Considerando que a ***Alternativa 02 - Fragmentaçaõ da Rede-ICMBio em redes filiais com a retirada gradativa dos serviços MPLS***, vai possibilitar a implantação do projeto de forma gradativa, reduzindo assim os riscos de indisponibilidade dos serviços, verifica-se que trata-se da alternativa de substituição dos serviços MPLS mais vantajosa para o ICMBio.

5.2.3.1 Verifica-se ainda, que a implementação gradativa será essencial para que os gestores das Unidades de Conservação com apoio da COTEC, possam avaliar as especificidades de suas redes internas e, caso necessário, efetuar as adaptações necessárias para o recebimento dos equipamentos que deverão ser instalados nas suas Unidades de Conservação.

5.2.4 Restou verificado por meio da análise das opções elencadas no item anterior que a manutenção da Rede-ICMBio da forma atual, ou seja, implementada em sua totalidade com serviços MPLS não é mais uma solução vantajosa para o ICMBio uma vez que tem custos elevados e impõe limitações para o uso de serviços de acesso à internet com menor custo e maior qualidade.

5.2.5 Conforme já relatado no item 2 deste ETP, atualmente o ICMBio possui um contrato junto a TELEBRÁS para o fornecimento de serviço de acesso à internet com o uso de solução implementada por meio de MPLS, onde o custo mensal médio é de R$ 4.745,33 (quatro mil setecentos e quarenta e cinco reais e trinta e três centavos) por circuito.

5.2.6 Embora o serviço MPLS seja essencial para garantir com que todas as transações entre os equipamentos da Rede-ICMBio sejam submetidas às regras de segurança e tenham a proteção da solução de segurança instalada na sede do ICMBio, restou verificado que é possível efetuar a expansão da solução de segurança atualmente instalada na Sede de modo que ela seja implementada nas Unidades de Conservação transformando essas unidades em redes filiais.

5.2.7 Em 08 de julho de 2021, o projeto de mudança da topologia da Rede-ICMBio foi aprovado pelo Comitê de Governança Digital, uma vez que, por meio de uma Prova de Conceito - POC, realizada em Goiânia-GO, no Centro Nacional de Pesquisa de Répteis e Anfíbios - RAN, foi possível verificar a viabilidade técnica da implantação de um módulo de segurança em uma Unidade de Conservação, transformando-a em uma rede filial, possibilitando a utilização de um link de IP Dedicado e outros serviços de comuns de acesso à internet, comercializados por provedores nacionais e provedores locais. Para essa POC, foi gerado a Nota Técnica nº 25/2021 pela CentralIT, conforme ANEXO II.

5.2.8 Para que o fornecimento de serviços de acesso à internet ocorra sob as mesmas políticas de segurança implementadas na sede do ICMBio, o módulo de segurança a ser instalado na localidade deve atuar de forma integrada ao módulo de gerenciamento existente na sede, que replica todas as políticas de segurança utilizadas na sede para o módulo de segurança instalado na Unidade de Conservação.

5.3. Quanto às contratações similares feitas por outros órgãos e entidades

5.3.1 Conforme o inciso II, do art. 11, da IN SGD/ME nº 31, de 2021, é necessário identificar e realizar a análise comparativa das soluções que possam atender às necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas. Neste sentido, temos os seguintes apontamentos:

5.3.2 Após análise dos processos licitatórios listados a seguir, restou verificado que a contratação de solução de firewall tipo UTM contemplando equipamentos e licenciamento é a prática mais comum dentre os órgãos do Governo.

a) Pregão Eletrônico nº 01/2021 - TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ - Objeto: Pregão Eletrônico - Contratação de empresa especializada para o fornecimento de Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças (Firewall UTM) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall); Solução de software para gerenciamento de logs e eventos de segurança (SIEM - Security Information and Event Management), além de suporte técnico e serviços especializados.

b) Pregão Eletrônico nº 02/2020 - CONSELHO REGIONAL DE ADMINISTRAÇÃO DE SÃO PAULO - Objeto: A contratação de empresa especializada para o fornecimento de soluções integradas de segurança de dados, composto por UTM (Gerenciamento Unificado de Ameaças) e Endpoint. As soluções devem possibilitar a visibilidade e controle de tráfego, filtragem de conteúdo Web, prevenção contra ameaças virtuais, filtro de dados, VPN e controle granular de banda de rede, QOS e outras funcionalidades, conforme descritas neste edital e seus anexos.

c) Pregão Eletrônico nº 14/2020 - ESCOLA NAC. DE SAÚDE PÚBLICA SÉRGIO AROUCA - Objeto: Pregão Eletrônico - Solução integrada de Firewall composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management).

d) Pregão Eletrônico nº 01/2020 - TRIBUNAL DE CONTAS DO ESTADO DO RIO GRANDE DO NORTE - Objeto: Pregão Eletrônico - Contratação da solução de Firewall UTM (Central Unificada de Gerenciamento de Ameaças), composta por 2 (dois) appliances (hardware e software na mesma caixa) em alta disponibilidade ativa/passiva, com licenças de uso por, no mínimo, 36 (trinta e seis) meses para atender as demandas do TCE/RN, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.

5.4 Quanto à ampliação ou substituição da solução implantada

5.4.1 Tendo em vista a aquisição por este Instituto e a implementação de recursos típicos de firewall de próxima geração, verifica-se que a hipótese de ampliação da solução atualmente utilizada no ICMBio representa a melhor opção do ponto de vista técnico, uma vez que a eventual utilização de firewalls de outros fabricantes inviabiliza a integração total dos recursos e coloca em risco a qualidade do gerenciamento centralizado.

5.4.2 Importa salientar que cada fabricante possui a sua gerência exclusiva e o uso de mais de um fabricante no ambiente, dificulta o uso da gerência centralizada, sendo necessário uma plataforma de gerência para cada fabricante na rede. Dessa forma, as aplicações das regras, por exemplo, teriam que ser feitas manualmente nesses equipamentos remotos ou através de outra(s) gerência(s), tornando o trabalho muito mais oneroso e crítico.

5.4.3 Cabe ressaltar que, conforme estudos para dimensionamento de esforços para sustentação de infraestrutura comumente presentes em estudos de contratações de serviços de infraestrutura, quanto menos padronizado está o parque maior é a complexidade de gestão e também os custos para a execução destes serviços, uma vez que é necessário envolver especialistas em soluções diferentes para dar suporte ao mesmo tipo de serviço.

5.4.4 Neste sentido, considerando que uma eventual implantação de equipamentos e serviços de fabricantes diferentes daquele já implantado no ICMBio acarretaria:

1. custos adicionais para treinamento das equipes;
2. aumento da complexidade da gestão dos recursos;
3. inviabilidade da padronização das soluções de segurança da informação;
4. impossibilidade de uma gerência unificada;
5. dificuldades para a implementação de regras advindas da política de segurança da informação frente a complexidade de um parque não padronizado.

5.4.5 Portanto, verifica-se que a expansão da solução de segurança já em produção no ICMBio torna-se mais vantajosa do que a substituição por uma outra solução que contemple os recursos de firewall.

5.5 Quanto à vantajosidade da contratação visando uma solução padronizada

5.5.1 De acordo com a Jurisprudência do TCU, a indicação ou preferência por marca em procedimento licitatório só é admissível se restar comprovado que a alternativa adotada é a mais vantajosa e/ou a única que atende às necessidades do Órgão ou Entidade. Adicionalmente, a Súmula/TCU nº 270/2012 relata que "*em licitações referentes a compras, inclusive de softwares, é possível a indicação de marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação*".

5.5.2 Conforme a Súmula/TCU nº 270/2012 em sede doutrinária, cumpre mencionar a lição do ilustre professor Marçal Justen Filho, ao comentar o princípio da padronização:

> "*A padronização é regra. No caso, a Administração deverá ter em vista aquisições passadas e futuras. A padronização aplica-se não apenas a uma compra específica, especialmente quando se trate de bem de vida útil continuada. Ao selecionar o fornecedor para produtos não consumíveis, a Administração deverá ter em vista produtos semelhantes que já integram o patrimônio público, como também deverá prever eventuais futuras aquisições. Somente assim a padronização produzirá os efeitos desejados, consistentes na redução de custos de manutenção, simplificação de mão-de-obra etc.*" (JUSTEN FILHO, Marçal. Comentários à Lei de Licitações e Contratos Administrativos, 13ª ed. São Paulo: Dialética, 2010, p. 176).

5.5.3 Além disso, conforme previsto no art. 15 da lei nº 8.666/93, temos que:

> "*Art. 15. As compras, sempre que possível, deverão:*
>
> *I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;*
> *II - ser processadas através de sistema de registro de preços;*"

5.5.4 Diante do elencar de orientações de Órgãos de controle, verifica-se ainda, as questões de ordem técnica e econômica, que fundamentam a adoção da padronização da atual solução presente no ICMBio, como a solução que traz vantajosidade para o ICMBio, uma vez que:

a) O ICMBio possui uma solução de segurança cibernética, implantada no exercício corrente, com garantia de atualização e suporte 24x7 por 60 (sessenta) meses, composta por um cluster de appliances 6900 do NGFW (Next Generation FireWall) e gerência centralizada versão 80.40 da marca Check Point licenciada para gerenciar até 05 firewalls (ou cinco redes filiais) que é expansível;

b) A equipe de servidores e colaboradores da área de Tecnologia da Informação do ICMBio vem atuando com a operação da solução, implantada no primeiro semestre do presente exercício, e está sendo capacitada para operar tanto o módulo de segurança da sede quanto o módulo de gestão. Desta forma, além dos colaboradores já capacitados pela empresa terceirizada responsável pelo suporte de infraestrutura de TI do ICMBio, foi contratada a capacitação com certificação de pelo menos 2 servidores para atuar em ações de contingência.

c) A integração de um módulo de segurança implantado em uma Unidade de Conservação (transformando-a em uma rede filial) integrada ao módulo de gerência da sede, foi testada e homologada pela equipe de servidores e colaboradores onde ficou constatada a viabilidade técnica da integração de equipamentos do tipo NGFW tipo small business com a gerência centralizada versão 80.40 instalada na sede do ICMBio.

d) A solução de cluster de appliances 6900 do NGFW (Next Generation FireWall) e gerência centralizada versão 80.40 da marca Check Point por já estar presente no parque do ICMBio, faz com que o Instituto esteja preservando investimentos já realizados e consolidados, haja vista que um fator limitador de outro fabricante de firewall em participar do processo licitatório não seria apenas a gerência que está instalada na Sede do ICMBio, que só possibilita gerenciar aparelhos licenciados pela própria Check Point, mas também envolve as questões relacionadas aos custos resultantes do aumento da complexidade de operação e gerenciamento de um parque não padronizado.

e) Conforme é prática padrão na elaboração dos contratos de serviços de sustentação de infraestrutura, a padronização do parque reduz a complexidade de operação e gerenciamento, e portanto, quanto mais complexa a operação maior a necessidade da utilização de diferentes especialistas para garantir o bom funcionamento da infraestrutura de rede e segurança da informação, por sua vez, quanto mais especialistas envolvidos na operação maior o custo das equipes.

f) A opção de padronização encontra justificativa pela economicidade e pela questão técnica, uma vez que a aquisição de módulos de segurança padronizados para as unidades é um procedimento mais vantajoso ao se comparar a um cenário em que fossem utilizados outros produtos que implicariam na aquisição de appliances e de softwares de gerenciamento com questões de licenciamentos e gerenciamentos diferenciados daqueles já implantados.

5.5.3 Em que pese o fato de que a opção pela estratégia de expansão de solução de segurança do ICMBio restrinja ao fabricante checkpoint (que é reconhecidamente pelo Gartner como um dos fabricantes melhores avaliados no mercado e que portanto, possui amplo hall de fornecedores nacionais), restou verificado que tal restrição é necessária e encontra fundamentação técnica quanto às vantagens para a Administração relacionadas a padronização da solução de segurança e seus benefícios para a gestão, operação e monitoramento da segurança da informação no âmbito do ICMBio.

5.5.4 Além de todos os pontos expostos nesse item 5 do ETP, a equipe de Planejamento da Contratação achou viável a solicitação via e-mail de esclarecimentos do fabricante Checkpoint (ANEXO III) se haveria alguma incompatibilidade de comunicação de equipamentos de outros fabricantes com o Modelo Check Point R80.40. Em resumo, foi detalhado que cada fabricante possui a sua gerência exclusiva, e portanto, o uso de mais de um fabricante no ambiente, impossibilita o uso da gerência centralizada, sendo necessário uma plataforma de gerência para cada fabricante na rede.

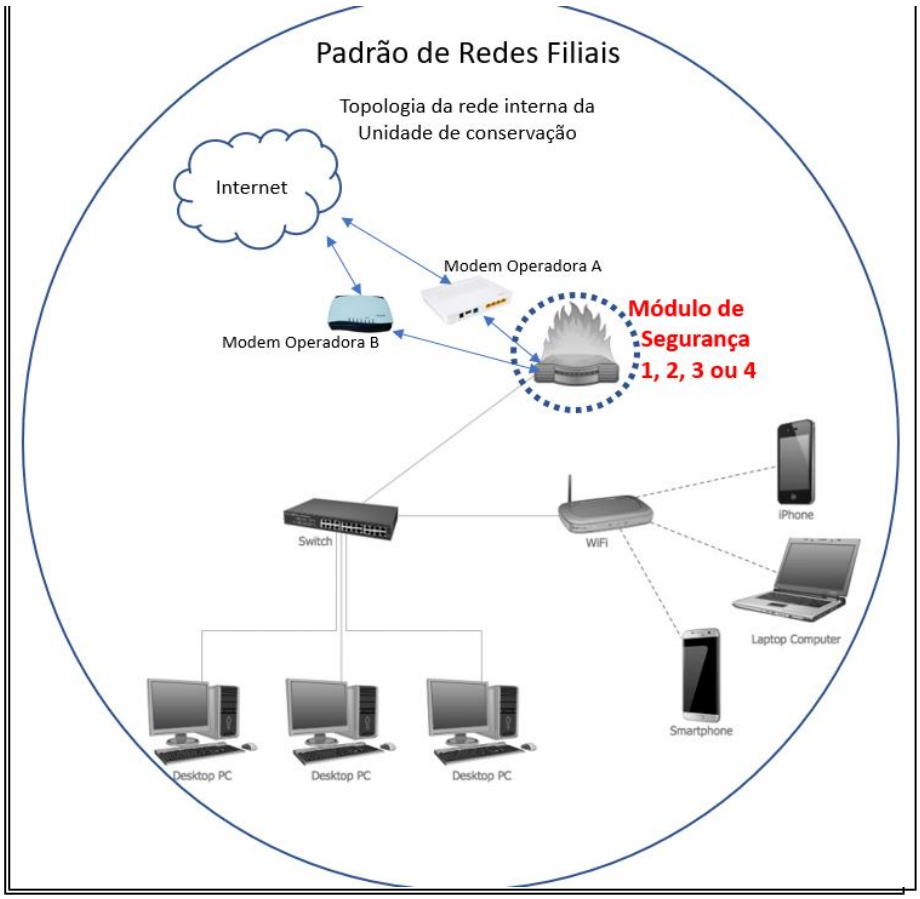
6. Descrição da solução como um todo

6.1 Considerando a necessidade da substituição dos serviços MPLS, mantendo garantida a continuidade dos serviços de monitoramento e implantação das políticas de segurança do ICMBio das redes internas da Unidades de Conservação do Instituto, esse ETP visa detalhar o processo de contratação de expansão da solução integradora de Firewall NEXT GENERATION, composta de hardware e software de segurança da informação do tipo UTM (Unified Threat Management), para interligar de forma segura a rede central do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) a suas Unidades Descentralizadas.

6.2 Atualmente a aplicação das regras de segurança da informação, definidas pela legislação atual e institucionalizadas pela Política de Segurança da Informação do ICMBio, são implementadas por meio da solução de segurança em operação no ICMBio que é composta por um cluster modelo 6900 e por uma gerência centralizada versão 80.40 da Checkpoint.

6.3 Desta forma, considerando a viabilidade de expansão da solução de modo a tornar possível a aplicação das mesmas regras de segurança existentes na sede para as Unidades de Conservação, estas passarão a funcionar como redes filiais, que embora sejam gerenciadas pela Rede-ICMBio, terão o acesso à internet independente da Sede do ICMBio. Com a instalação de qualquer um dos 04 (quatro) tipos de *módulos de segurança (firewall local)*, será possível a utilização de links de uma ou mais operadoras de serviços de acesso à internet, conforme ilustrado na figura à seguir:

Topologia padrão para redes filiais - UCs



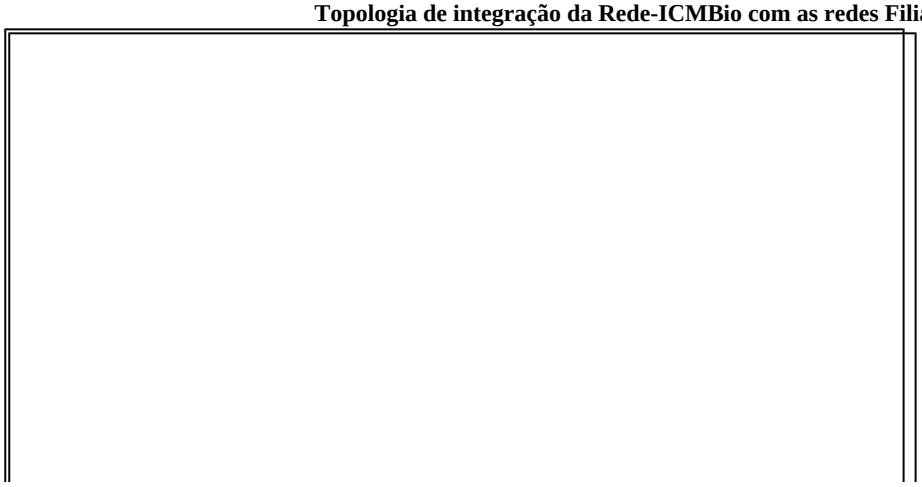
6.3.1 Assim, mesmo que ocorram indisponibilidades de serviços de acesso à internet na sede, as redes filiais permanecerão com seus serviços disponíveis, uma vez que os *Módulos de Segurança* implantados nas localidades estarão em pleno funcionamento aplicando as regras de segurança e gerenciando o link de acesso à internet do provedor local, sem a necessidade de conexão com a sede.

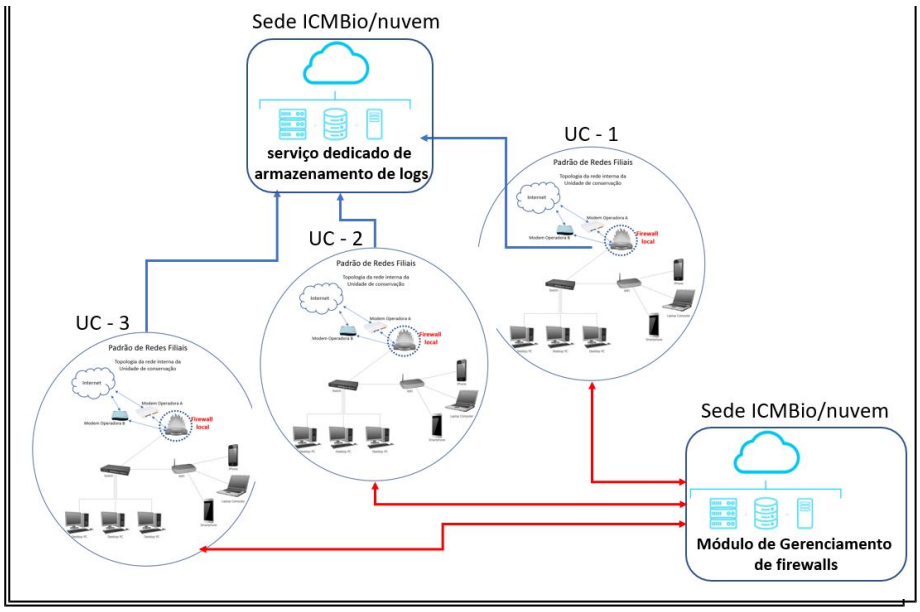
6.3.2 Desta forma, os *Módulos de Segurança (tens 01, 02, 03 e 04)* deverão possuir capacidade de atuar com no mínimo dois links de acesso à internet gerenciando esses recursos para garantir redundância dos serviços de acesso à internet para a rede interna da Unidade de Conservação.

6.3.3 Considerando que as Unidades de Conservação não possuem técnicos capacitados para efetuar configurações avançadas nos Módulos de Segurança, a CONTRATADA deverá encaminhar para a Sede os equipamentos pré-configurados simplificando ao máximo a instalação local, devendo ainda fornecer um manual rápido com o passo a passo de conexão dos Módulos às redes internas das Unidades de Conservação.

6.3.4 Por sua vez, as redes filiais passarão a atuar de forma integrada à Rede-ICMBio, de maneira que o *Serviço dedicado de Armazenamento de logs* e o *Serviço de gerenciamento dos módulos de segurança* serão mantidos pela Sede, conforme ilustrado na figura a seguir:

Topologia de integração da Rede-ICMBio com as redes Filiais





6.3.5 Embora os *Módulos de Segurança (tens 01, 02, 03 e 04)* sejam destinados às Unidades de Conservação, os equipamentos passarão por testes e configurações na Sede do ICMBio em Brasília - DF, desta forma será exigido que a contratada entregue os módulos de segurança nas dependências da sede do ICMBio em Brasília-DF, para que sejam testados e aprovados pela COTEC, reduzindo a complexidade da instalação dos módulos nas Unidades.

6.3.6 Assim, a CONTRATADA deverá fornecer os equipamentos já configurados com regras e políticas replicadas do firewall da Sede do ICMBio, podendo para tanto, utilizar o laboratório da COTEC para a realização de testes e configurações dos equipamentos preparando-os para que a COTEC possa testá-los e enviar para as Unidades de Conservação prontos para serem conectados pelas equipes locais do Instituto, com orientações da equipe de suporte da CONTRATADA e da COTEC.

6.3.7 Todos os appliances deverão ser gerenciados pelo módulo de gestão R80/R81 centralizado que deverá receber um Upgrade de Licenciamento (item 05) para se tornar capaz de gerenciar no mínimo até 200 (duzentos) *Módulos de Segurança (tens 01, 02, 03 e 04)* com garantia de atualização de licenças e suporte técnico pelo período mínimo de 60 (sessenta) meses.

6.4 Com relação ao Upgrade de Licenciamento Seccuritty Management R80, atualmente o ICMBio possui um módulo de gerenciamento de firewalls que possui licenciamento para gerenciar até 05 (cinco) equipamentos. Esse módulo é responsável pelo monitoramento dos equipamentos e para o gerenciamento de funcionalidades e aplicação de políticas de segurança, desta forma, considerando que serão adquiridos outros firewalls até o limite de 200 (duzentas) unidades, se faz necessária a realização de UPGRADE de licença para que seja possível efetuar o gerenciamento de todos os equipamentos a serem adquiridos.

6.5 Já no que se refere ao serviço dedicado de armazenamento de logs, trata-se de serviço centralizado instalado em nuvem ou em datacenter sob gestão do ICMBio, que é destinado ao armazenamento dos registros de acessos à internet executados por usuários lotados nas Unidades de Conservação. Desta forma, o registro destes logs serve para garantir o nível de rastreabilidade necessário para uso das autoridades em casos de investigações de crimes cibernéticos ou uso indevido dos recursos de acesso à internet. Cabe ressaltar que a disponibilização destas informações só poderá ser realizada sob determinação judicial conforme legislação pertinente.

6.5.1 A opção pela utilização deste serviços de forma centralizada reduz o custo dos equipamentos instalados nas Unidades de Conservação uma vez que ao enviar os logs para um serviço centralizado na sede, os equipamentos das localidades não necessitam de sistema físico adicional de armazenamento de dados.

6.6 Por conseguinte, se faz necessário a aquisição de um nobreak/estabilizador senoidal de 1,5kva para cada *Módulo de Segurança (tens 01, 02, 03 e 04)*, devido ao fato de que as Unidades de Conservação não possuem rede elétrica estabilizada, visando mitigar o risco de eventuais danos aos módulos de segurança por problemas relacionados à baixa qualidade das redes de distribuição de energia elétrica.

6.7 Comparação do TCO da solução com a manutenção dos serviços MPLS conforme contrato vigente.

6.7.1 Neste item foi considerado o *Total Cost of Ownership* (TCO), em português Custo Total de Propriedade, que é a métrica de análise que tem como objetivo calcular os custos de vida e de aquisição de um produto, ativo ou sistema.

6.7.2 No quadro a seguir é possível identificar o custo médio anual de R$ 11.736.870,42 (onze milhões setecentos e trinta e seis mil, oitocentos e setenta reais e quarenta e dois centavos) para 200 (duzentos) circuitos MPLS, com um custo médio anual de R$ 4.890,36 (quatro mil oitocentos e noventa reais e trinta e seis centavos) por circuito MPLS.

CUSTO MÉDIO DOS SERVIÇOS MPLS		
QUANTIDADE DE CIRCUITOS	VALOR MÉDIO	VALOR TOTAL MENSAL
200	R$ 4.605,61	R$ 921.122,17
VALOR MÉDIO ANUAL		R$ 11.053.465,99
VALORES OBTIDOS CONFORME HISTÓRICO DE EXECUÇÃO DO CONTRATO CELEBRADO ENTRE O ICMBio e a TELEBRAS. (o quantitativo de circuitos foi ajustado proporcionalmente para efeito de comparação com TCO - Custo total de Propriedade relacionado ao projeto em análise		
CUSTO MÉDIO ANUAL DOS SERVIÇOS MPLS (A1+A2+A3+A4+A5/5)		R$ 11.736.870,42
CUSTO MÉDIO MENSAL POR CIRCUITO MPLS (C1+C2+C3+C4+C5/5)		R$ 4.890,36

PROJEÇÃO DO CENÁRIO DE CUSTOS DOS SERVIÇOS MPLS PARA 05 ANOS - considerando uma taxa hipotética de ajuste contratual anual de 3% a.a.				
ANO 1	ANO 2	ANO 3	ANO 4	ANO 5
(A1) Custo anual para 200 Circuitos MPLS	(A2) Custo anual para 200 Circuitos MPLS	(A3) Custo anual para 200 Circuitos MPLS	(A4) Custo anual para 200 Circuitos MPLS	(A5) Custo anual para 200 Circuitos MPLS
R$ 11.053.465,99	R$ 11.385.069,97	R$ 11.726.622,07	R$ 12.078.420,73	R$ 12.440.773,35
(B1) Custo mensal para 200 Circuitos MPLS (A/12)	(B2) Custo mensal para 200 Circuitos MPLS (A/12)	(B3) Custo mensal para 200 Circuitos MPLS (A/12)	(B4) Custo mensal para 200 Circuitos MPLS (A/12)	(B5) Custo mensal para 200 Circuitos MPLS (A/12)
R$ 921.122,17	R$ 948.755,83	R$ 977.218,51	R$ 1.006.535,06	R$ 1.036.731,11
(C1) Custo mensal por circuito MPLS (B/200)	(C2) Custo mensal por circuito MPLS (B/200)	(C3) Custo mensal por circuito MPLS (B/200)	(C4) Custo mensal por circuito MPLS (B/200)	(C5) Custo mensal por circuito MPLS (B/200)
R$ 4.605,61	R$ 4.743,78	R$ 4.886,09	R$ 5.032,68	R$ 5.183,66

6.7.3 De acordo com o Manual de boas práticas, orientações e vedações para a contratação de ativos de TIC - Versão 4, disponível no link: BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC – Versão 4, aquisições de equipamentos ativos de rede com as características constantes desta solução de extensão de solução de segurança da informação, devem contemplar, preferencialmente, garantia de suporte 24x7 com substituição de peças e componentes durante a vida útil dos equipamentos. *In verbis:*

> 1.2. AQUISIÇÃO DE ATIVOS COM GARANTIA VERSUS CONTRATAÇÃO DE SERVIÇOS DE MANUTENÇÃO
>
> 1.2.1 Os ativos de TI devem ser adquiridos com garantia de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico.
>
> 1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil. Ainda, os contratos de manutenção têm seus custos elevados na medida em que os bens manutenidos se tornam obsoletos. Ou seja, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco do fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

6.7.4 Desta forma, para o estudo comparativo da expansão da solução de segurança da informação do ICMBio, o valor total da aquisição foi diluído ao longo dos 05 (cinco) anos de garantia, conforme ilustrado no quadro à seguir:

CENÁRIO 01 - CONSIDERANDO IMPLANTAÇÃO TOTAL				
REGISTRO DE PREÇOS				
LOTE	ITEM	DESCRIÇÃO DO ITEM	UNIDADE	QUANT.
1	1	Módulo de Segurança Tipo 1 (Compatibilidade de Appliance – redes com até 30 usuários)	UN	40
	2	Módulo de Segurança Tipo 2 (Compatibilidade de Appliance – redes de 30 até 70 usuários)	UN	100
	3	Módulo de Segurança Tipo 3 (Compatibilidade de Appliance – redes de 70 até 150 usuários)	UN	50
	4	Módulo de Segurança Tipo 4 (Compatibilidade de Appliance – redes acima de 150 usuários)	UN	10
	5	Upgrade de Licenciamento Security Manager R80 – Modelo de Gerenciamento de até 200 módulos	UN	1
	6	Log Server R80 – Licenciamento para Implementação de Serviço de Armazenamento de logs dedicados.	UN	1
MÉDIA DO VALOR VALOR TOTAL PARA O LOTE 01				R$ 5.701.000,80

ANÁLISE DE CUSTOS PARA 05 ANOS - considerando a implentação total da solução com módulo de gerenciamento integrado e serviço de armazenameno de logas dedicado para um total de 200 módulos de segurança 200, com suporte e atualização por 05 (cinco) anos.				
ANO 1	ANO 2	ANO 3	ANO 4	ANO 5
Custo total anual 200 módulos	Custo total anual 200 módulos	Custo total anual 200 módulos	Custo total anual 200 módulos	Custo total anual 200 módulos
R$ 1.140.200,16	R$ 1.140.200,16	R$ 1.140.200,16	R$ 1.140.200,16	R$ 1.140.200,16
Custo anual por módulo	Custo anual por módulo	Custo anual por módulo	Custo anual por módulo	Custo anual por módulo
R$ 5.701,00	R$ 5.701,00	R$ 5.701,00	R$ 5.701,00	R$ 5.701,00
Custo mensal por módulo implantado	Custo mensal por módulo implantado	Custo mensal por módulo implantado	Custo mensal por módulo implantado	Custo mensal por módulo implantado
R$ 475,08	R$ 475,08	R$ 475,08	R$ 475,08	R$ 475,08

6.7.5 Desta forma, ao efetuar a comparação dos dois cenários (cenário 01 - manutenção dos serviços MPLS com as mesmas condições contratuais existentes e cenário 02 - substituição dos circuitos MPLS pela implantação dos módulos de segurança conforme proposto neste Estudo Técnico Preliminar) verificou-se que a solução proposta nestes estudos deverá resultar em economia mensal ao ICMBio capaz de recuperar o investimento ainda no primeiro ano, conforme demostrado na figura a seguir:

	MÉDIA MENSAL	MÉDIA ANUAL	5 ANOS
CUSTO DOS SERVIÇOS MPLS POR CIRCUITO	**R$ 4.890,36**	**R$ 58.684,35**	**R$ 293.421,76**
(A) CUSTO DE IMPLANTAÇÃO DA SOLUÇÃO DE SEGURANÇA POR CIRCUITO	R$ 493,10	R$ 5.917,15	R$ 29.585,73
(B) Custo médio de serviços de link de acesso à internet banda larga no Brasil (Conforme pesquisa disponível no link https://melhoresofertas.net/blog/internet-banda-larga/qual-o-preco-medio-da-internet-no-brasil).	R$ 400,00	R$ 4.800,00	R$ 24.000,00
(A+B) CUSTO DE IMPLANTAÇÃO DA SOLUÇÃO DE SEGURANÇA POR CIRCUITO somado ao custo médio de serviços comuns de acesso à internet banda larga.	**R$ 893,10**	**R$ 10.717,15**	**R$ 53.585,73**
Economia gerada com a substituição do serviço MPLS pela extensão da solução de segurança da sede POR CIRCUITO	**R$ 3.997,27**	**R$ 47.967,21**	**R$ 239.836,03**

6.7.6 Desta forma, considerando que a economia anual por circuito é de R$ 47.967,21 e que o custo total (valor total de investimento) para a implantação da expansão da solução, por circuito é de R$ 29.585,73 é possível afirmar que nos primeiros 18 meses de execução do projeto, (que possui 60 meses) o ICMBio terá recuperado todo o investimento por meio da redução das dos custos atualmente pagos para manter a solução MPLS, conforme ilustrado na figura à seguir:

6.8 Diante destes apontamentos restou verificada a vantajosidade técnica e econômica para o ICMBio quanto a implantação da da expansão de solução de segurança da informação nos moldes propostos neste Estudo Técnico Preliminar.

7. Estimativa das Quantidades a serem Contratadas

7.1 Para a composição da solução que representa maior vantajosidade para a Rede-ICMBio foi efetuado um levantamento prévio sobre as condições gerais de infraestrutura das redes internas das Unidades de Conservação, por meio de estudo do histórico de chamados de suporte aos serviços de acesso à internet, e também por meio de vistorias feitas pelo Coordenador de Tecnologia da Informação e Comunicação às unidades: Gerência Regional 03 - Goiânia - GO, Gerência Regional 04 - RJ, Gerência Regional 01 Santarém - PA, NGI Itaituba - PA, Parque Nacional de Anavilhanas - AM, Parque Nacional da Serra dos Órgãos - RJ, Parque Nacional da Chapada dos Veadeiros - GO, Parque Nacional da Tijuca - RJ, NGI - Tefé - PA, Parque Nacional da Chapada dos Guimarães - MT, RAN - Goiânia - GO, Base Avançada de Manaus - AM, Floresta Nacional de Brasília - DF e Parque Nacional de Brasília - DF.

7.2 Desta forma, para melhor estimar os quantitativos de equipamentos e as configurações mínimas necessárias para o atendimento das necessidades do ICMBio, ainda que não tenham sido feito um estudo mais detalhado, foi utilizada a técnica da análise das unidades visitadas como amostra, considerando o registro histórico de chamados para o universo de 241 (duzentas e quarenta e uma) redes internas (***conforme planilha com todos os circuitos atualmente fornecidos pelo contrato de serviços MPLS***), foi possível definir as características mais relevantes para o projeto conforme elencadas a seguir:

a) Condições do local destinado para abrigar os ativos de rede e o *Módulo de Segurança* - O local destinado a instalação do *Módulo de Segurança*, quando da instalação da solução, deverá possuir sistema que mantenha a temperatura do ambiente dentro dos limites recomendados pelo fabricante, com rack adequado para instalação de switches e demais ativos de rede, energia estabilizada e nobreak para proteção dos ativos de rede.

b) Público a ser atendido com a instalação do *Módulo de Segurança* - Total de usuários que utilizam os serviços de acesso à internet na Unidade e o total de setores e Unidades que compartilham o recurso.

c) Serviços de banda larga ofertados na região da Unidade de Conservação - Verificar se existem serviços de banda larga com IP dedicado, serviços do tipo ADSL e demais serviços que adotem tecnologias compatíveis com a *Módulo de Segurança* a ser implantado.

d) Nível de segurança exigido (baixo, médio, alto) - Avaliação quanto a necessidade da implementação de recursos de segurança baseada nas atividades desenvolvidas na unidade, ou seja, verificar se a unidade possui servidores de rede, bancos de dados, ambientes de escritórios ou outras atividades que exijam a implementação de procedimentos e recursos de segurança, conforme previstos na Política de Segurança do ICMBio.

c) Quantidade de unidades institucionais interligadas - Avaliação do quantitativo de ativos de rede e suas conexões com outras unidades do Instituto, seja na mesma edificação ou em edificações diferentes.

7.3 Diante do levantamento das informações sobre as características gerais, coletadas por meio de amostra (obtida por meio das visitas às unidades), das redes internas das Unidades de Conservação do ICMBio e ainda, de modo a disponibilizar o mapeamento da demanda de forma clara que possa subsidiar a identificação do tipo de solução mais adequado à necessidade de cada Unidade de Conservação, a demanda estimada considerou a divisão do universo de 241 (duzentos e quarenta e uma) redes internas em 05 (cinco) grupos conforme elencados a seguir:

7.3.1 Bases ou Unidades de Conservação com ***infraestrutura simplificada*** - nessas localidades a infraestrutura implementada geralmente deverá ser composta de um modem e um roteador wi-fi. Não há a necessidade de outros ativos de rede por não haver o uso destas bases como escritório.

7.3.1.1 Trata-se de bases de observação ou apoio a visitação onde o uso da rede é destinado a disponibilizar internet para visitantes e para postos de vigia.

7.3.1.2 Para este tipo de unidade **não será implementado um módulo de segurança.**

7.3.2 Redes internas com até 30 usuários - Unidades de Conservação com estações de trabalho, ativos de rede, onde existem servidores e colaboradores executando atividades de escritório redes. Com estas características estima-se um total de 40 (quarenta) unidades;

7.3.3 Redes internas de 30 até 70 usuários - Unidades de Conservação com estações de trabalho, ativos de rede, onde existem servidores e colaboradores executando atividades de escritório redes, servidores de rede e conexões com outras unidades. Com estas características estima-se um total de 100 (cem) unidades;

7.3.4 Redes internas de 70 até 150 usuários - Unidades de Conservação com estações de trabalho, ativos de rede, onde existem servidores e colaboradores executando atividades de escritório redes, servidores de rede e conexões com outras unidades. Com estas características estima-se um total de 50 (cinquenta) unidades;

7.3.5 Redes internas acima de 150 usuários - Unidades de Conservação com estações de trabalho, ativos de rede, onde existem servidores e colaboradores executando atividades de escritório redes, servidores de rede e conexões com outras unidades, centros de treinamentos e atividades de grande vulto. Com estas características estima-se um total de 10 (dez) unidades;

7.3.6 Implantação de um serviço dedicado de armazenamento de logs (capacidade mínima de armazenamento 1 (um) Terabyte) - serviço centralizado, instalado em nuvem ou em datacenter sob gestão do ICMBio que é destinado ao armazenamento dos registros de acessos executados nas Unidades de Conservação.

7.3.6.1 O registro destes logs é importante para que o ICMBio possa apresentar às autoridades em casos de investigações de crimes ou uso indevido dos recursos de acesso à internet. Cabe ressaltar que a disponibilização destas informações só poderá ser realizada sob determinação judicial conforme legislação pertinente.

7.3.6.2 A implementação de um serviço de armazenamento centralizado trata-se de uma opção mais econômica para o ICMBio comparando a uma eventual opção pelo armazenamento local, que implicaria na aquisição de módulos de segurança com sistema de armazenamento para todas as unidades o que acarretaria custos adicionais.

7.3.7 Expansão de licenciamento do serviço de gerenciamento de módulos de segurança - Tendo em vista que o ICMBio já possui uma solução de segurança totalmente implementada na sede que contempla um serviço de gerenciamento de módulos de segurança, cujo contrato garante suporte técnico com manutenção corretiva e evolutiva por 05 (cinco) anos, verifica-se que a expansão do licenciamento da solução para até 200 módulos é mais vantajosa do que a aquisição de uma nova solução que além de representar custos adicionais para implantação e migração, traria impacto aos serviços já em operação além de desperdiçar o investimento já realizado para a implantação da solução que ocorreu no primeiro semestre deste exercício.

7.3.8 Nobreak/estabilizador - Além dos módulos que deverão ser instalados nas Unidades de Conservação, tendo em vista a preservação do investimento do ICMBio, juntamente com os equipamentos a serem instalados nas unidades, verifica-se a necessidade da instalação de um nobreak/estabilizador bivolt para a proteção contra variações de tensão provocadas por quedas de energia elétrica ou por problemas de qualidade das redes elétricas, para este item foi estimado um equipamento para cada módulo, totalizando 200 (duzentas) unidades.

7.4 Desta forma, elencada a metodologia adotada, restaram estimados os itens e quantitativos que deverão compor o registro de preços conforme quadro ilustrado a seguir:

Composição da solução de TI

COMPOSIÇÃO DA SOLUÇÃO					
LOTE	**ITEM**	**DESCRIÇÃO**	**UNIDADE**	**CATMAT/CATSER**	**QUANT.**
1	01	Módulo de segurança tipo 01 (compatibilidade do Appliance - redes com até 30 usuários)	UN	150100	40
	02	Módulo de segurança tipo 02 (compatibilidade do Appliance - para redes de 30 até 70 usuários)	UN	150100	100
	03	Módulo de segurança tipo 03 (compatibilidade do Appliance - redes de 70 até 150 usuários)	UN	150100	50
	04	Módulo de segurança tipo 04 (compatibilidade do Appliance -redes acima de 150 usuários)	UN	150100	10
	05	Upgrade Licenciamento Securitty Management R80 - para gerenciamento de até 200 firewalls	UN	27502	1
	06	Log Server Dedicado R80 - licenciamento para implementação de serviço de armazenamento de logs Dedicado	UN	27502	1
2	07	Nobreak Senoidal 1,5kva	UN	474218	200

7.5 Cabe ressaltar que os quantitativos estimativos consideram cada circuito MPLS, uma potencial rede interna a ser transformada em rede filial, portanto deverá constar do plano de implantação a análise pontual das condições elencadas no item 7.2 de cada circuito para o qual for solicitado o fornecimento, antes da abertura da Ordem de Serviço.

8. Estimativa do Valor da Contratação

8.1 O levantamento dos valores para a aquisição de bens e contratação de serviços em geral para os órgãos e entidades participantes do SISG - Sistema de Serviços Gerais, deve seguir os procedimentos administrativos definidos pela Instrução Normativa nº 65/2021 da Secretaria de Gestão (SEGES) do Ministério da Economia. Este levantamento servirá para balizar a viabilidade financeira do projeto.

8.2 Com relação à pesquisa de preços, cabe informar que esse item 8 - Estimativa do Valor da Contratação do ETP será dividido em duas partes, pois no que se refere ao Lote I - solução de Firewall para as UCs, não foram encontrados pregões similares. Pelo fato de o objeto ser muito singular, ou seja, tratar de aquisição de appliances menores de firewalls da checkpoint, ficou inviável encontrar pregões similares no painel de preços. Por esse motivo, a pesquisa do Lote I será realizada exlcusivamente com fornecedores. Esse fato justifica o art. 3º da IN 65/2021, que diz que a pesquisa de preços será materializada em documento que conterá, no mínimo, a justificativa da escolha dos fornecedores, no caso da pesquisa direta de que dispõe o inciso IV do art. 5º.

8.3 Pesquisa de Preços referente ao Lote 1 - Solução de Firewall para as UCs

8.3.1 Seguindo o determinado pela IN SEGES/ME nº 65, de 7 de julho de 2021 que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional, a pesquisa de preços para o lote I será realizada via pesquisa direta com fornecedores, conforme determina o inciso IV do art. 5º:

> "*Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:*
>
> *I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;*
>
> *II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;*
>
> *III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;*
>
> *IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou*
>
> *V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.*" *(grifo nosso)*

8.3.2 Ainda de acordo com a IN 65/2021, a pesquisa com os fornecedores deverá se atentar ao § 2º do art. 5º:

> "*Art. 5º (...)*
>
> *§ 2º Quando a pesquisa de preços for realizada com fornecedores, nos termos do inciso IV, deverá ser observado:*
>
> *I - prazo de resposta conferido ao fornecedor compatível com a complexidade do objeto a ser licitado;*
>
> *II - obtenção de propostas formais, contendo, no mínimo:*
>
> *a) descrição do objeto, valor unitário e total;*
>
> *b) número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica - CNPJ do proponente;*
>
> *c) endereços físico e eletrônico e telefone de contato;*
>
> *d) data de emissão; e*
>
> *e) nome completo e identificação do responsável.*
>
> *III - informação aos fornecedores das características da contratação contidas no art. 4º, com vistas à melhor caracterização das condições comerciais praticadas para o objeto a ser contratado; e*
>
> *IV - registro, nos autos do processo da contratação correspondente, da relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação de que trata o inciso IV do caput.*" *(grifo nosso)*

8.3.3 Visando realizar a pesquisa de preços com os fornecedores se baseando na IN 65/2021, foi realizado uma pesquisa direta mediante solicitação formal via e-mail a 8 (oito) empresas, a citar: Embratel, Telefônica, NTSEC, APTUM, NGSX, NGXIT, L8 Group e OI.

8.3.3.1 Da solicitação formal, somente 3 (três) empresas responderam, a citar: L8 Group (ANEXO IV), NTSEC (ANEXO V) e APTUM (ANEXO VI).

8.3.4 A tabela a seguir apresenta a compilação das propostas recebidas dos fornecedores visando calcular o valor médio das propostas:

LOTE	ITEM	DESCRIÇÃO	UNID.	QUANT.	L8 GROUP (R$)	NTSEC (R$)	APTUM (R$)	VALOR MÉDIO UNITÁRIO (R$)	VALOR MÉDIO TOTAL (R$)
01	01	Módulo de segurança tipo 01 (compatibilidade do Appliance - redes com até 30 usuários)	UN.	40	14.446,27	15.513,31	16.488,88	15.482,82	619.312,80
	02	Módulo de segurança tipo 02 (compatibilidade do Appliance - redes de 30 até 70 usuários)	UN.	100	18.438,38	21.088,11	22.602,66	20.709,72	2.070.971,67
	03	Módulo de segurança tipo 03 (compatibilidade do Appliance - redes de 70 até 150 usuários)	UN.	50	25.446,26	27.423,70	28.913,67	27.261,21	1.363.060,50
	04	Módulo de segurança tipo 04 (compatibilidade do Appliance - redes acima de 150 usuários)	UN.	10	70.115,04	76.493,24	80.345,65	75.651,31	756.513,10
	05	Upgrade de Licenciamento Security Management R80 - Módulo de gerenciamento de até 200 firewalls	UN.	1	891.237,73	973.155,53	1.032.486,65	965.626,64	965.626,64
	06	Log Server Dedicado R80 - Licenciamento para implementação	UN.	1	137.850,35	139.144,99	147.990,40	141.661,91	141.661,91

		de serviço de armazenamento de logs dedicado							

8.4 Pesquisa de Preços referente ao Lote 2 - Solução de Nobreak/Estabilizador

8.4.1 Já com relação ao Lote 2 - aquisição de Nobreaks/Estabilizadores, foi realizada a análise de projetos similares, em que foram identificadas contratações similares na Administração Pública, conforme detalhado nos ANEXOS VII (pesquisa de preços resumida) e VIII (pesquisa de preços completa) deste ETP. Nesta análise, foram obtidos os preços referentes à média, mediana e menor preço, como parâmetros, conforme detalhado abaixo:

8.4.2 Para a composição dos custos unitários do objeto, foi utilizado o previsto na IN 65/2021, em seu artigo 5º, inciso I:

> "*Parâmetros*
>
> *Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:*
>
> *I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;*
>
> *II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;*
>
> *III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;*
>
> *IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou*
>
> *V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia." (grifo nosso)*

8.4.3 Visto isso, com base na consolidação dos preços pesquisados e utilizando como composição de custos o menor valor comparando a média com a mediana (o menor valor de R$ 564,00 foi desconsiderado neste caso, pois os valores da média e da mediana destoam mais de 50% do seu valor), o valor total estimado para o lote 2 é de R$ 176.900,00 (cento e setenta e seis mil e novecentos reais).

LOTE	ITEM	DESCRIÇÃO	UNIDADE	QUANT.	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
02	07	Nobreak Senoidal 1,5kva	UN.	200	884,50	176.900,00

8.5 A estimativa do valor da contratação está detalhada na tabela abaixo:

LOTE	ITEM	DESCRIÇÃO	UNIDADE	QUANT.	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
01	01	Módulo de segurança tipo 01 (compatibilidade do Appliance - redes com até 30 usuários)	UN.	40	15.482,82	619.312,80
	02	Módulo de segurança tipo 02 (compatibilidade do Appliance - redes de 30 até 70 usuários)	UN.	100	20.709,72	2.070.971,67
	03	Módulo de segurança tipo 03 (compatibilidade do Appliance - redes de 70 até 150 usuários)	UN.	50	27.261,21	1.363.060,50
	04	Módulo de segurança tipo 04 (compatibilidade do Appliance - redes acima de 150 usuários)	UN.	10	75.651,31	756.513,10
	05	Upgrade de Licenciamento Security Management R80 - Módulo de gerenciamento de até 200 firewalls	UN.	1	965.626,64	965.626,64
	06	Log Server Dedicado R80 - Licenciamento para implementação de serviço de armazenamento de logs dedicado	UN.	1	141.661,91	141.661,91
02	07	Nobreak Senoidal 1,5kva	UN.	200	884,50	176.900,00
VALOR GLOBAL DA SOLUÇÃO (R$)						**6.094.046,62**

8.6 Com base na consolidação dos preços pesquisados, o valor estimado para contratação é de **R$ 6.094.046,62 (seis milhões, noventa e quatro mil, quarenta e seis reais e sessenta e dois centavos).**

9. Justificativa para o Parcelamento ou não da Solução

9.1 Conforme dispoẽ o Inciso I, § 2º, art. 12, da IN SGD/ME nº 31/2021, "*A Equipe de Planejamento da Contratação avaliará a viabilidade de realizar o parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovarem técnica e economicamente viáveis, justificando-se a decisão de parcelamento ou não da solução*".

9.2 Considerando-se que os serviços que deverão estar associados ao objeto dependem da definição do produto a ser fornecido durante o processo licitatório e **considerando que os nobreaks podem ser contratados em lote separado, por se tratar de item de simples aquisição e por não interagir com a solução de segurança**, restou verificado que, para os demais itens, não é viável particionar o objeto da contratação, uma vez que colocaria em risco o objetivo final desejado.

9.3 Ademais, a aquisição do objeto da licitação em 02 (dois) lotes, sendo um lote exclusivo para os nobreaks e um outro lote para a solução de segurança, vai possibilitar a unicidade técnica dos processos, assim como o nível de serviços prestados, permitindo que a empresa contratada esteja capacitada tecnicamente para trabalhar de forma integrada com os componentes desta solução.

9.4 Outro fator importante a ser levado em consideração é a otimização dos recursos necessários à gerência de um único contrato, para o gerenciamento da solução de segurança e o foco na melhoria do processo, visto que a COTEC possui uma equipe de servidores públicos reduzida, além de ser responsável pela gestão de outros contratos de TI.

9.5 Já a viabilidade econômica significa que o parcelamento deve trazer benefícios para a Administração licitante, proporcionando um aumento da competitividade e uma consequente diminuição dos custos para a execução do objeto, fato que será observado com a separação do item de nobreak dos demais itens. No entanto, para uma real noção da viabilidade econômica do parcelamento, é preciso obter a redução de custos proporcionada pela economia de escala sem que o resultado do processo acrescente custos para a gestão dos serviços, processos e fiscalização do objeto.

9.6 Nesse sentido, a aquisição em dois lotes conforme aqui proposta, apresenta vantagem para a Administração do ponto de vista da eficiência técnica, por manter a qualidade da solução de TI, haja vista que o gerenciamento permanece todo o tempo a cargo de um mesmo administrador. Nesse ponto, as vantagens seriam o maior nível de controle pela Administração na execução dos serviços, a maior interação entre as diferentes fases da implantação/implementação, a maior facilidade no cumprimento do cronograma preestabelecido e na observância dos prazos, concentração da responsabilidade pela execução em uma só pessoa e concentração da garantia dos resultados.

9.7 Dessa forma, por suas especificidades, esta contratação ao estar alinhada às práticas de mercado, deverá ter a sua adjudicação da licitação pelo menor preço global. Ademais, o parcelamento do objeto conforme proposto não restringe a competitividade do certame e nem traz prejuízo ao erário, visto que os itens agrupados que compõem o objeto são de mesma natureza e guardam relação entre si.

10. Contratações Correlatas e/ou Interdependentes

10.1 Para a implantação da solução nas Unidades de Conservação será necessária a contratação de serviços de acesso à internet, para que sejam alcançados os requisitos de economicidade e independência dos serviços de acesso à internet atualmente fornecidos pela sede.

10.1.1 Embora a implantação por completo da solução dependa da contratação de serviços comuns de acesso à internet, o custo médio mensal destes serviços, somado ao custo médio mensal do investimento diluído pelos 60 (sessenta) meses representa economia para o ICMBio se comparado ao custo médio atual dos serviços MPLS, conforme detalhado no item 6 deste ETP.

11. Alinhamento entre a Contratação e o Planejamento

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
OE. 11	Fortalecer a comunicação e a imagem institucional
OE. 15	Fortalecer e integrar os instrumentos de gestão
OE. 18	Estruturar e implementar a gestão do conhecimento
OE. 20	Modernizar tecnologicamente o Instituto
OE. 21	Ampliar recursos e melhorar a eficiência e transparência nos gastos
OE. 22	Prover e gerenciar de forma eficiente a infraestrutura

ALINHAMENTO AO PDTIC 2020-2021						
ID	**Tipo de Necessidade**	**Descrição da Necessidade de TI**	**ID**	**Ação do PDTIC**	**ID**	**Meta do PDTIC associada**
TI04	Infraestrutura de TI	Prover recursos de comunicação de rede local, metropolitana e à Internet	**A6.07**	Manter o serviço de comunicação de rede e acesso a internet no âmbito de todas as unidades do ICMBio	**M6**	Manter o serviço de rede operacional
TI13	Infraestrutura de TI	Prover recursos de segurança da informação	**A15.01**	Adquirir/Contratar firewall	**M8**	Garantir a segurança do ambiente corporativo de TI

ALINHAMENTO AO PAC 2021	
Item	**Descrição**
532	ACESSO A INTERNET VIA SATELITE
533	ACESSO A INTERNET VIA CABO
873	FIREWALL

12. Resultados Pretendidos

12.1 O processo de Planejamento da Contratação deverá produzir documentação técnica que possibilite ao ICMBio a aquisição de uma solução que atenda aos seguintes resultados:

a) Prover segurança nos acessos aos recursos de TI necessários para a implementação dos programas e projetos sob a responsabilidade do Instituto;

b) Aprimorar a segurança, proteção e autenticidade dos dados sensíveis da organização, controlando pro-ativamente as vulnerabilidades em recursos de TI;

c) Proteger a rede de computadores da sede do ICMBio, redes filiais que atendem as unidades descentralizadas, de ataques cibernéticos, implementar níveis de segurança na camada das aplicações e otimizar os recursos de acesso à internet;

d) Expandir os recursos de segurança a nível de gerenciamento centralizado para firewals a serem implantados nas redes filiais, possibilitando o uso de links locais reduzindo os custos com serviços MPLS;

e) Prover uma infraestrutura de segurança da informação formada por equipamentos modernos e com capacidade de suportar todos os serviços constantes do Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC, e ainda, possibilitar o alcance das necessidades de negócio do Instituto fortalecendo a segurança dos dados;

f) Garantir que a infraestrutura da rede do ICMBio possua os requisitos necessários para suportar todas as demandas de serviços constantes do PDTIC, e ainda, a possibilidade de ampliação gradativa da capacidade tecnológica para demandas futuras;

g) Disponibilizar uma solução de segurança baseada em equipamento e software totalmente licenciada com garantia de suporte técnico e capacitação de pessoal para atuar quando houver necessidade de atuar em contingência;

h) Possibilitar a implementação de recursos de segurança da informação diretamente nas Unidades descentralizadas de forma gerenciada pelas equipes de TI da sede.

i) Possibilitar a contratação de serviços de acesso à internet mais vantajosos de acordo com as características dos serviços ofertados nas regiões onde se encontram as Unidades de Conservação, mantendo os níveis de segurança necessários ao ICMBio.

j) Reduzir os custos dos serviços de acesso à internet utilizados no ICMBio ampliando o hall de serviços disponíveis para a contratação.

k) Reduzir a dependência das Unidades de Conservação junto a Sede quanto ao uso de serviços de acesso à internet que atualmente dependem totalmente da conexão com a sede do ICMBio.

l) Padronizar as infraestruturas das redes internas da Unidades de Conservação implementando módulo de segurança e pelo menos um equipamento de proteção contra descargas elétricas e variações de tensão, promovendo ampliação da vida útil dos ativos de rede.

13. Providências a serem Adotadas

13.1 Para a implantação da solução constante destes estudos nas Unidades de Conservação do ICMBio, será necessário a contratação de serviços de acesso à internet, preferencialmente do tipo IP Dedicado. Para tanto, as especificações técnicas deste serviço a ser contratado pelas Unidades de Conservação com apoio das áreas de licitações deste ICMBio, serão fornecidas pela COTEC em processo vinculado ao processo que originou estes estudos.

13.2 Além disso deverá ser encaminhado aos gerentes regionais um documento com as orientações gerais quanto:

a) as providências necessárias para a adequação dos ambientes que receberão os ativos de rede;

b) as rotinas de verificação e conservação dos ambientes;

c) canais de comunicação para solucionar dúvidas quanto à preparação de ambientes;

d) canais de comunicação para registros de problemas quanto à instalação ou operação dos equipamentos na Unidade;

e) os modelos de processo para contratação de serviços de acesso à internet.

14. Possíveis Impactos Ambientais

14.1 Os equipamentos fornecidos deverão possuir funcionalidades que promovam a economia de energia elétrica, como, por exemplo, modo de economia de energia.

14.2 Os equipamentos deverão possuir seleção manual ou automática para a tensão de alimentaçaõ de 100/127 volts e 220 volts.

14.3 Os equipamentos somente serão instalados com o uso de Estabilizador/Nobreak.

14.4 As Unidades de Conservação deverão ser avaliadas pela COTEC quanto às condições dos ambientes em que serão instalados os módulos de segurança, de modo a garantir que estejam adequados quanto às questões de isolamento físico, climatização e instalações elétricas e lógicas.

14.5 O laboratório da COTEC na sede do ICMBio deverá ser adaptado para realizar o recebimento, a preparação e os testes dos equipamentos antes do envio para as Unidades de Conservação.

14.6 As Unidades de Conservação deverão auxiliar a COTEC quanto aos estudos sobre os serviços e fornecedores de banda larga disponíveis na sua região.

15. Mapa de Gerenciamento de Riscos

15.1 O Mapa de Gerenciamento de Riscos contém a descrição, a análise e o tratamento dos riscos e ameaças que possam vir a comprometer o sucesso em todas as fases da contratação e da execução contratual.

15.2 A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste documento.

Id	Risco	Relacionado ao(à):[1]	P[2]	I[3]	Nível de Risco (P x I)[4]
1	Atraso no trâmite da documentação processual	Planejamento da Contratação	5	10	50
2	Não aprovação da instrução processual pela autoridade competente	Planejamento da Contratação	5	10	50
3	Insuficiência de servidores para habilitar o vencedor e receber os equipamentos	Planejamento da Contratação	7	10	70
4	Não habilitação técnica do vencedor da contratação	Planejamento da Contratação	5	10	50
5	Atraso ou a não assinatura do contrato	Planejamento da Contratação	5	10	50
6	Atraso na entrega dos equipamentos	Planejamento da Contratação	5	10	50
7	Valor contratado superior ao estimado	Seleção do Fornecedor	5	5	25
8	Incompatibilidade técnica dos equipamentos	Gestão Contratual e Solução Tecnológica	5	5	25
9	Não cumprimento de prazos e garantia contratual	Gestão Contratual e Solução Tecnológica	5	10	50
10	Falência da Empresa ou desaparecimento da contratada	Gestão Contratual e Solução Tecnológica	5	10	50
11	Qualificação técnica e operacional insuficiente dos Fiscais Técnicos do contato	Gestão Contratual e Solução Tecnológica	7	10	70

Legenda: P – Probabilidade; I – Impacto.

[1] A qual natureza o risco está associado: fases do Processo da Contratação ou Solução Tecnológica.

[2] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[3] *Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).*

[4] *Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).*

5 = Probabilidade baixa, Impacto baixo

7 = Probabilidade média, Impacto médio

10 = Probabilidade Alta, Impacto alto

AVALIAÇÃO E TRATAMENTO DOS RISCOS IDENTIFICADOS

Risco 01	**Risco:**		Atraso no trâmite da documentação processual.
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Atraso na contratação e consequente impossibilidade de atender a necessidade do ICMBio
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Priorizar o processo junto aos setores competentes.	CGATI
	Id	**Ação de Contingência**	**Responsável**
	1	Manter a utilização do firewall atualmente em operação	COTEC
	2	Mitigação e eliminação das causas que obstruem o processo licitatório.	Equipe de Planejamento da Contratação

	Risco:	Não aprovação da instrução processual pela autoridade competente.
	Probabilidade:	Baixa
	Impacto:	Alto
	Dano 1:	Não contratação e consequente impossibilidade de atender a necessidade do ICMBio

Risco 02	**Tratamento:**		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Revisar o processo em todas as suas etapas de instrução para evitar que não esteja apto a ser aprovado pela autoridade competente.	CGATI
	Id	**Ação de Contingência**	**Responsável**
	1	Manter a utilização do firewall atualmente em operação	COTEC
	2	Não há ação de contingência em caso de reprovação pela autoridade competente. A equipe de contratação deverá rever e adequar às necessidades e capacidades do ICMBio.	Equipe de Planejamento da Contratação

Risco 03	**Risco:**		Insuficiência de servidores para habilitar o vencedor e receber os equipamentos.
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Atraso no recebimento dos equipamentos.
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Nomear preferencialmente a equipe de fiscalização como sendo a mesma da contratação.	CGATI
	Id	**Ação de Contingência**	**Responsável**
	1	Prover as áreas envolvidas com servidores de outras áreas	CGATI

	Risco:	Não habilitação técnica do vencedor da contratação.
	Probabilidade:	Baixa
	Impacto:	Alto

Risco 04	**Dano 1:**	Atraso na contratação e consequente impossibilidade de atender a necessidade do ICMBio	
	Tratamento:	Mitigar.	
	Id	**Ação Preventiva**	**Responsável**
	1	Estabelecer objetivamente os critérios para a habilitação técnica.	CGATI
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar os critérios estabelecidos em lei para convocação do próximo licitante.	COTEC

Risco 05	**Risco:**	Atraso ou a não assinatura do contrato.	
	Probabilidade:	Baixa	
	Impacto:	Alto	
	Dano 1:	Atraso na contratação e consequente impossibilidade de atender a necessidade do ICMBio	
	Tratamento:	Mitigar.	
	Id	**Ação Preventiva**	**Responsável**
	1	Estabelecer prazo e sanções relativas a assinatura do contrato.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar as sanções e demais possibilidades previstas na contratação.	CGATI

	Risco:	Atraso na entrega dos equipamentos
	Probabilidade:	Baixa
	Impacto:	Alto

Risco 06	**Dano 1:**	Atraso na contratação e consequente impossibilidade de atender a necessidade do ICMBio	
	Tratamento:	Mitigar.	
	Id	**Ação Preventiva**	**Responsável**
	1	Estabelecer prazo e sanções relativas a assinatura do contrato.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar as sanções e demais possibilidades previstas na contratação.	CGATI

Risco 07	**Risco:**	Valor contratado superior ao estimado.	
	Probabilidade:	Baixa	
	Impacto:	Baixo	
	Dano 1:	Atraso na contratação e consequente impossibilidade de atender a necessidade do ICMBio	
	Tratamento:	Evitar.	
	Id	**Ação Preventiva**	**Responsável**
	1	Atenção com relação a contratação direta do fornecedor.	CGATI
	Id	**Ação de Contingência**	**Responsável**
	1	Não há ações contingencias nesse caso.	CGATI

	Risco:	Incompatibilidade técnica dos equipamentos.
	Probabilidade:	Baixa
	Impacto:	Baixa

Risco 08	**Dano 1:**	Incompatibilidade dos equipamentos com o parque e as características do ICMBio.	
	Tratamento:	Mitigar.	
	Id	**Ação Preventiva**	**Responsável**
	1	Conferir adequadamente o equipamento ofertado com as exigências que constam nas especificações técnicas do termo de referência.	COTEC
	Id	**Ação de Contingência**	**Responsável**
	1	Solicitar ao licitante que atenda aos requisitos do edital e, se for o caso, aplicar os critérios estabelecidos em lei para convocação do próximo licitante.	CGATI

Risco 09	**Risco:**	Não cumprimento de prazos e garantia contratual.	
	Probabilidade:	Baixa	
	Impacto:	Alto	
	Dano 1:	Paralisação do equipamento, acarretando falha na prestação do serviço.	
	Tratamento:	Mitigar.	
	Id	**Ação Preventiva**	**Responsável**
	1	Definir e exigir a confirmação do prazo de garantia contratual.	Equipe de Planejamento da Contratação/COTEC
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar os critérios estabelecidos em lei e na contratação para punir as faltas do licitante vencedora /contratada.	CGATI

	Risco:	Falência da Empresa ou desaparecimento da contratada.
	Probabilidade:	Baixa

Risco 10	**Impacto:**		Alto
	Dano 1:		Descumprimento contratual
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Exigir qualificações financeiras e técnicas que levem à seleção de uma empresa com capacidade de fornecimento até o final da garantia dos equipamentos.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar os critérios estabelecidos no edital e em lei para o caso concreto, inclusive acionando os meios jurídicos.	CGATI

Risco 11	**Risco:**		Qualificação técnica e operacional insuficiente dos Fiscais Técnicos do contato.
	Probabilidade:		Média
	Impacto:		Alto
	Dano 1:		Impossibilidade de acompanhamento da gestão contratual.
	Tratamento:		Mitigar.
	Id	**Ação Preventiva**	**Responsável**
	1	Fornecer os meios necessários para capacitação da equipe de fiscalização contratual.	CGAT/COTEC
	Id	**Ação de Contingência**	**Responsável**
	1	Verificar em outras áreas servidor com o conhecimento necessário para realizar a fiscalização contratual.	CGATI/COTEC

16. Declaração de Viabilidade

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

16.1. Justificativa da Viabilidade

As informações constantes deste Planejamento da Contratação e seus anexos estão de acordo com as normas técnicas pertinentes ao assunto e atendem as necessidades do ICMBio quanto aos serviços constantes do objeto do pleito desta contratação.
Assim, diante do exposto acima, entendemos ser VIÁVEL a contratação da solução demandada.

17. Responsáveis

FELIPE FINGER SANTIAGO
Analista em TI

GUILHERME PALMA DE SOUSA
Técnico Administrativo

JOSÉ LUIZ ROMA
Coordenador de Infraestrutura e Logística

JAIME HELENO CORREA DE LISBOA
Coordenador de Tecnologia da Informação e Comunicação

Lista de Anexos

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

- Anexo I - Custo dos links MPLS.pdf (332.67 KB)
- Anexo II - Nota Técnica 25 - Caderno de testes - POC FW RAN GOIANIA.pdf (507.74 KB)
- Anexo III - Resposta_Checkpoint.pdf (482.69 KB)
- Anexo IV - Proposta Comercial - L8 Group.pdf (1.02 MB)
- Anexo V - Proposta Comercial - NTSEC.pdf (794.83 KB)
- Anexo VI - Proposta Comercial - APTUM.pdf (1.24 MB)
- Anexo VII - Pesquisa de Preço NOBREAK 1.5kva senoidal RESUMIDA.pdf (87.21 KB)
- Anexo VIII - Pesquisa de Preço NOBREAK 1.5kva senoidal COMPLETA.pdf (115.94 KB)

Anexo I - Custo dos links MPLS.pdf

LEVANTAMENTO DE DESPESAS COM A MANUTEÇÃO DOS CIRCUITOS MPLS - CONTRATADOS JUNTO A TELEBRAS

CONTROLE DAS UNIDADES - ATUALIZADA AGOSTO 2019							
CIRCUITO	CUSTO MENSAL	VELOCIDADE (MBps)	DESCRIÇÃO - UNIDADE	ENDEREÇO	CIDADE	UF	FASE ATUAL
ACL3000012	4.016,95	2	FLORESTA NACIONAL DE MACAUÃ – (BASE AVANÇADA)	RIO MACAUÃ - COLOCAÇÃO SANTA ROSA, CEP: 69.940-000	SENA MADUREIRA	AC	Ativo Satélite
ACL3000013	4.016,95	2	RESERVA EXTRATIVISTA CAZUMBÁ-IRACEMA - (BASE AVANÇADA)	RIO CAETÉ, COMUNIDADE CAZUMBÁ, CEP: 69.940-000	SENA MADUREIRA	AC	Ativo Satélite
ACL3000015	4.016,95	2	NÚCLEO DE GESTÃO INTEGRADA DE SENA MADUREIRA (FLONA SANTA ROSA DO PURUS / FLONA MACAUÃ / FLONA SÃO FRANCISCO / RESEX CAZUMBÁ-IRACEMA)	AVENIDA AVELINO CHAVES, N° 1935 – BOSQUE, CEP: 69.940-000	SENA MADUREIRA	AC	Ativo Terrestre
ACL3000016	4.016,95	2	NÚCLEO DE GESTÃO INTEGRADA CRUZEIRO DO SUL (RESEX RIOZINHO DA LIBERDADE / RESEX ALTO JURUÁ / PARNA SERRA DO DIVISOR)	RUA JAMINAUAS, 1556 - B. CRUZEIRÃO, CEP: 69.980-000	CRUZEIRO DO SUL	AC	Ativo Terrestre
ACL3000017	4.016,95	2	NÚCLEO DE GESTÃO INTEGRADA EM BRASILÉIA – (RESEX CHICO MENDES / ARIE SERINGAL NOVA ESPERANÇA)	AVENIDA MANUEL MARINHO MONTES, 1028 – B. ELDORADO, CEP: 69.932-000	BRASILÉIA	AC	Ativo Terrestre
ACL3000018	4.016,95	4	PARNA DA SERRA DO DIVISOR	Rua Moa, s/n, Destacamento São Salvador do 61° BIS (Batalhão de Infantaria de Selva)	MÂNCIO LIMA	AC	Ativo Satélite
ACL3000019	9.155,99	10	CNPT - CENTRO NACIONAL DE PESQUISA E CONSERVAÇÃO DA SÓCIO-BIODIVERSIDADE ASSOCIADA A POVOS E COMUNIDADES TRADICIONAIS – (RESEX CHICO MENDES, RESEX ALTO TARAUACÁ, FLONA IQUIRI, COORDENAÇÃO REGIONAL 07)	RUA HENRIQUE DIAS, Nº 162, BAIRRO BOSQUE, CEP: 69.900-568	RIO BRANCO	AC	Ativo Terrestre
ALL3000006	4.078,07	10	ESTAÇÃO ECOLÓGICA DE MURICI	RUA MARINO VIEIRA DE ARAÚJO N°32 – CIDADE ALTA	MURICI	AL	Ativo Satélite
ALL3000007	3.301,47	10	ÁREA DE PROTEÇÃO AMBIENTAL DE PIAÇABUÇÚ	AV. BEIRA MAR, S/N, POVOADO DO PONTAL PEBA CAIXA POSTAL COMUNITÁRIA N° 154	PONTAL DO PEBA	AL	Ativo Satélite
ALL3000008	4.078,07	4	BASE AVANÇADA DA APA COSTAS DOS CORAIS	Sítio Funil I, s/n, Tatuamunha, estrada da boca do rio Tatuamunha, a 2 km da AL 101 norte, CEP: 57948-000	PORTO DAS PEDRAS	AL	Ativo Satélite
ALL3000009	4.078,07	2	ÁREA DE PROTEÇÃO AMBIENTAL COSTA DOS CORAIS	RUA ANTÔNIO BALTAZAR, 96 – BARRA UM	BARRA DE SANTO ANTÔNIO	AL	Ativo Terrestre
ALL3000010	4.078,07	4	RESERVA EXTRATIVISTA MARINHA DA LAGOA DO JEQUIÁ	RUA SANTO ANTONIO, 886 CENTRO, CEP: 57255-000	JEQUIÁ DA PRAIA	AL	Ativo Satélite
ALL3000011	4.078,07	4	RESERVA BIOLÓGICA DE PEDRA TALHADA	SÍTIO GAVIÃO, APÓS A FAZENDA RIACHÃO - ZONA RURAL	QUEBRANGULO	AL	Ativo Satélite
AML3000012	3.301,49	4	NÚCLEO DE GESTÃO INTEGRADA DE BOCA DO ACRE – (FLONA DO PURUS / FLONA MAPIÁ-INAUINI / FLONA IQUIRI / RESEX ARAPIXI)	RUA C.A – PLATÔ DO PIQUIÁ	BOCA DO ACRE	AM	Ativo Satélite
AML3000013	3.301,49	4	RESERVA EXTRATIVISTA AUATI-PARANÁ	ESTRADA DA BARÉ, S/N - BAIRRO MÃE CREUZA, CEP:	FONTE BOA	AM	Ativo Satélite
AML3000014	3.301,49	4	NÚCLEO DE GESTÃO INTEGRADA DE TAPUÁ – (REBIO DO ABUFARI / PARNA NASCENTES DO LAGO JARI)	AV. PRESIDENTE COSTA E SILVA, 56 - B. MANOEL COSTA	TAPAUÁ	AM	Ativo Satélite
AML3000015	3.301,49	4	NÚCLEO DE GESTÃO INTEGRADA DE NOVO AIRÃO - (PARNA DE ANAVILHANAS / PARNA DO JAÚ / RESEX DO RIO UNINI / FLONA AMAZONAS)	RUA ANTENOR CARLOS FREDERICO, 69 - B. NOSSA SENHORA AUXILIADORA	NOVO AIRÃO	AM	Ativo Satélite
AML3000016	3.301,49	4	PARQUE NACIONAL DO JAÚ – (BASE AVANÇADA)	ACESSO A PARTIR DE NOVO AIRÃO, 100KM (3 HORAS DE VOADEIRA) SUBINDO O RIO NEGRO	NOVO AIRÃO	AM	Ativo Satélite
AML3000017	4.078,07	4	RESERVA BIOLÓGICA DO UATUMÃ	AV. RIO NEGRO, 8 - CENTRO COMERCIAL - DISTRITO VILA DE BALBINA	PRESIDENTE FIGUEIREDO	AM	Ativo Satélite
AML3000018	3.301,49	4	RESERVA EXTRATIVISTA CAPANÃ GRANDE	TRAVESSA D. PEDRO II, 581 - B. N. S. AUXILIADORA	MANICORE	AM	Ativo Satélite
AML3000019	3.301,49	4	RESERVA EXTRATIVISTA MÉDIO JURUÁ	RUA ARCANJO PESSOA, N° 100 – CENTRO	CARAUARI	AM	Ativo Satélite
AML3000021	3.301,49	4	RESERVA EXTRATIVISTA BAIXO JURUÁ	RUA SENADOR JOÃO BOSCO, 36 - CENTRO	JURUÁ	AM	Ativo Satélite
AML3000022	9.735,67	10	COORDENAÇÃO REGIONAL 02 / ARIE DINAMINCA BIOLOGICA DE FRAGMENTOS FLORESTAIS / PFE	Caracara	MANAUS	AM	Ativo Terrestre
AML3000023	5.838,94	6	CEPAM – CENTRO NACIONAL DE PESQUISA E CONSERVAÇÃO DA BIODIVERSIDADE AMAZÔNICA	CAMPUS DA UNIVERSIDADE FEDERAL DO AMAZONAS – UFAM. AVENIDA GENERAL RODRIGO OTAVIO, 3000 – B. COROADO, CEP: 69077-000	MANAUS	AM	Ativo Terrestre
AML3000024	3.301,49	10	NÚCLEO DE GESTÃO INTEGRADA DE LÁBREA – (RESEX DO RIO ITUXI / RESEX DO MÉDIO PURUS)	RUA LUIZ FALCÃO, 2595 - B. BARRA LIMPA	LÁBREA	AM	Ativo Satélite
AML3000025	3.301,49	4	NÚCLEO DE GESTÃO INTEGRADA DE TEFÉ - (FLONA DE TEFÉ / ESEC JUTAÍ SOLIMÕES / ESEC JUAMI JAPURÁ / RESEX RIO JUTAÍ / RESEX BAIXO JURUÁ / RESEX AUATI PARANÁ)	ESTRADA DO AEROPORTO, 725 - CENTRO	TEFÉ	AM	Ativo Satélite
AML3000027	3.301,49	4	PARQUE NACIONAL PICO DA NEBLINA	AVENIDA DOM JOSÉ, 52 - CENTRO	SÃO GABRIEL DA CACHOEIRA	AM	Ativo Satélite
AML3000028	3.301,49	4	NÚCLEO DE GESTÃO INTEGRADA DE MAUES (FLONA DE PAU-ROSA e ESEC ALTO MAUES)	Rua Eduardo Ribeiro, 3198, Jauari I, CEP: 69104-128	ITACOATIARA	AM	Ativo Satélite
APL3000013	4.065,12	4	ESTAÇÃO ECOLÓGICA DE MARACÁ-JIPIOCA	MARGEM DIREITA DO IGARAPÉ INFERNO - ILHA DE MARACÁ NORTE	MACAPÁ	AP	Ativo Satélite
APL3000014	4.065,12	2	NÚCLEO DE GESTÃO INTEGRADA DE MACAPÁ – (REBIO DO LAGO PIRATUBA / RESEX DO RIO CAJARI)	RODOVIA JUSCELINO K. DE OLIVEIRA, KM02, CAMPOS MARCO ZERO DO EQUADOR – SALA 04	MACAPÁ	AP	Ativo Terrestre
APL3000015	3.288,52	4	FLORESTA NACIONAL DE AMAPÁ	SAINDO DE MACAPÁ ATÉ A SEDE DO MUNICÍPIO DE PORTO GRANDE. SUBINDO O RIO ARAGUARI ATÉ SUA CONFLUÊNCIA COM O RIO FALSINO (45 KM)	FERREIRA GOMES	AP	Ativo Satélite
APL3000016	3.288,52	4	PARQUE NACIONAL DO CABO ORANGE – (BASE AVANÇADA)	MARGEM ESQUERDA DO RIO CATIPORÉ	OIAPOQUE	AP	Ativo Satélite
APL3000017	3.288,52	4	NÚCLEO DE GESTÃO INTEGRADA DE OIAPOQUE – (PARNA DO CABO ORANGE / PARNA MONTANHAS DO TUMUCUMAQUE)	RUA GETÚLIO VARGAS, 235 - BAIRRO PARAÍSO	OIAPOQUE	AP	Ativo Satélite

LEVANTAMENTO DE DESPESAS COM A MANUTEÇÃO DOS CIRCUITOS MPLS - CONTRATADOS JUNTO A TELEBRAS

APL3000018	4.065,12	4	PARQUE NACIONAL MONTANHAS DO TUMUCUMAQUE – (BASE AVANÇADA)		SERRA DO NAVIO	AP	Ativo Satélite
APL3000019	3.288,52	4	RESERVA BIOLÓGICA DO LAGO PIRATUBA	COMUNIDADE DO TABACO, MARGEM ESQUERDA DO RIO ARAGUARI	TARTARUGALZINHO	AP	Ativo Satélite
APL3000020	4.065,12	4	RESERVA BIOLÓGICA DO LAGO PIRATUBA - BASE DE CUTIAS DO ARAGUAI	RUA RIO ARAGUAI, S/N° – B. BEIRA RIO	Cutias	AP	Ativo Satélite
APL3000021	4.065,12	4	RESERVA BIOLÓGICA DO LAGO PIRATUBA - (BASE DA VILA DO SUCURIJI)	RUA RIO ARAGUAI, S/N° – B. BEIRA RIO (VILA DO Sucuriju)	Cutias	AP	Ativo Satélite
BAL3000019	4.052,55	4	FLORESTA NACIONAL DE CONTENDAS DO SINCORÁ (base)	BA 026, km 106, Zona Rural, Contendas do Sincorá/BA, coordenadas geográfica 13°55'1.64"S e 41°6'55.39"W	CONTENDAS DO SINCORÁ	BA	Ativo Satélite
BAL3000020	4.052,55	2	CEPENE - CENTRO DE PESQUISA E GESTÃO DE RECURSOS PESQUEIROS DO LITORAL NORDESTE - (BASE AVANÇADA) - (RESEX DO CASSURUBÁ)	GETULIO VARGAS 326 - PONTA DE AREIA	CARAVELAS	BA	Ativo Terrestre
BAL3000021	4.052,55	2	PARNA MARINHO DOS ABROLHOS (escritório)	PRAIA DO KITONGO, S/N - B. KITONGO	CARAVELAS	BA	Ativo Terrestre
BAL3000022	4.052,55	4	PARQUE NACIONAL MARINHO DOS ABROLHOS	Parna Marinho de Abrolhos - ILHA SANTA BÁRBARA (DENTRO DO PARQUE)	CARAVELAS	BA	Ativo Satélite
BAL3000023	4.052,55	4	PARQUE NACIONAL DO PAU BRASIL – (BASE AVANÇADA)	ESTRADA VELHA ARRAIAL D´AJUDA - ITABELA	PORTO SEGURO	BA	Ativo Satélite
BAL3000024	4.052,55	2	PARQUE NACIONAL DA CHAPADA DIAMANTINA	RUA BARÃO DO RIO BRANCO NR. 80	PALMEIRA	BA	Ativo Terrestre
BAL3000025	4.052,55	4	RESERVA BIOLÓGICA DE UNA (REVIS DE UNA)	RODOVIA BA-001 TRECHO ILHÉUS/UNA, KM 45 - ZONA DO MARUIM, CEP: 45690-000	UNA	BA	Ativo Satélite
BAL3000027	4.052,55	4	PARQUE NACIONAL HISTORICO DE MONTE PASCOAL	BR 498, KM 0, ALDEIA PÉ DO MONTE, ZONA RURAL	PORTO SEGURO	BA	Ativo Satélite
BAL3000028	4.052,55	4	RESERVA EXTRATIVISTA MARINHA BAIA DE IGUAPE	RUA CEL ANTONIO FELIPE DE MELO, N°52 - CAJÁ	MARAGOGIPE	BA	Ativo Satélite
BAL3000029	4.052,55	2	RVS RIO DOS FRADES / PARNA DO PAU BRASIL/PARNA ALTO CARIRI	Rua Dona Candi, nº 99, Pacatá, Porto Seguro/BA	PORTO SEGURO	BA	Ativo Terrestre
BAL3000030	4.052,55	2	PARQUE NACIONAL ALTO CARIRI	RUA VIENA S/N, BAIRRO DINAH BORGES, CEP: 45820-858	EUNÁPOLIS	BA	Ativo Terrestre
BAL3000031	4.052,55	2	MONUMENTO NATURAL DO RIO SÃO FRANCISCO – (ESEC RASO DA CATARINA)	AVENIDA MARANHÃO, 79 – FAZENDA CHESF	PAULO AFONSO	BA	Ativo Terrestre
BAL3000032	4.052,55	4	ESTAÇÃO ECOLÓGICA RASO DA CATARINA	ZONA RURAL DE PAULO AFONSO, PRÓXIMO POVOADO MOSQUITO, CEP: 48609-999	PAULO AFONSO	BA	Ativo Satélite
BAL3000033	4.052,55	10	PARQUE NACIONAL DO DESCOBRIMENTO (RESEX CORUMBAU, PARNA HISTORICO DO MONTE PASCOAL)	RUA 04, QUADRA C, LOTE 31 , NOVO PRADO, CEP: 45980-000	PRADO	BA	Ativo Internet
BAL3000034	4.052,55	10	RESERVA EXTRATIVISTA DE CANAVIEIRAS	RUA GENERAL PEDERNEIRAS, 410 - CENTRO, CANAVIEIRAS - BA	CANAVIEIRAS	BA	Ativo Internet
BAL3000035	4.052,55	4	PARQUE NACIONAL DA SERRA DAS LONTRAS	RODOVIA ILHÉUS-ITABUNA, KM 22, CEPLAC/SUEBA-CEP: 45653-919, REFERÊNCIA: CORREDOR À DIREITA DA AG. BANCO BRASIL,	ILHÉUS	BA	Ativo Satélite
BAL3000208	5.071,44	6	UNIDADE AVANÇADA DE ADMINISTRAÇÃO E FINANÇAS 4 - SALVADOR-BA	Rua Frederico Simões, 125 / Sala 802 Edifício Liz Empresarial - Caminho das Árvores	SALVADOR	BA	Ativo Terrestre
BAL3000241	4.052,56	2	NGI JUAZEIRO (APA do Boqueirão da Onça/ PARNA do Boqueirão da Onça/ APA da Ararinha Azul/ Refúgio da Vida Silvestre da Ararinha Azul)	Unidade Técnica de 2º Nível do IBAMA em Juazeiro, IBAMA, RODOVIA Juazeiro-Sobradinho, BR-210, S/n, DISF, Juazeiro.	JUAZEIRO	BA	Ativo Satélite
CEL3000015	4.078,07	4	ESTAÇÃO ECOLÓGICA DE AIUABA	ESTRADA AIUABA - ANTONINA DO NORTE RODOVIA CE 176 - KM 495 - SITIO VOLTA	AIUABA	CE	Ativo Satélite
CEL3000016	4.078,07	2	FLORESTA NACIONAL DE ARARIPE-APODI	ROD. CE 055 - RODOVIA CRATO-EXU - KM 12	CRATO	CE	Ativo Terrestre
CEL3000017	3.301,49	10	PARQUE NACIONAL DE JERICOACOARA	RUA OCEANO ATLÂNTICO, S/N - B. JERICOACOARA	JERICOACOARA	CE	Ativo Satélite
CEL3000018	4.078,07	2	PARQUE NACIONAL DE UBAJARA	RODOVIA DA CONFIANÇA - CE 187 - HORTO FLORESTAL	UBAJARA	CE	Ativo Terrestre
CEL3000019	4.078,07	2	ÁREA DE PROTEÇÃO AMBIENTAL SERRA DA IBIAPABA	ROD. CE 187 KM 02 - RODOVIA DA CONFIANÇA - SÍTIO INGÁ - ZONA RURAL, CEP: 62300-000	VIÇOSA DO CEARÁ	CE	Ativo Terrestre
CEL3000020	4.078,07	2	AREA DE PROTEÇÃO AMBIENTAL CHAPADA DO ARARIPE	PRAÇA JOAQUIM FERNANDES TELES, S/N – PIMENTA	CRATO	CE	Ativo Terrestre
CEL3000021	4.078,07	2	RESERVA EXTRATIVISTA PRAINHA DO CANTO VERDE (RESEX BATOQUE)	RUA JOÃO T. FERREIRA, N° 208, BEBERIBE	BEBERIBE	CE	Ativo Terrestre
CEL3000022	4.078,07	2	FLORESTA NACIONAL DE SOBRAL – (ÁREA DE PROTEÇÃO AMBIENTAL DA MERUOCA)	3°46'28,80" S / 40°31'38" W	SOBRAL	CE	Ativo Terrestre
DFL3000056	4.052,55	2	FLORESTA NACIONAL DE BRASÍLIA – (APA DA BACIA DO RIO DESCOBERTO)	BR 070 - KM 0,5, COM A DF 001 (A APROX 500M DO FINAL DA ESTRUTURAL)	TAGUATINGA NORTE	DF	Ativo Terrestre
DFL3000058	13.759,64	20	PARQUE NACIONAL DE BRASÍLIA - (CEMAVE / CECAT / CECAV /CPB / APA DO PLANALTO CENTRAL / REBIO CONTAGEM)	BR040 - SMU - PARQUE NACIONAL DE BRASILIA	BRASÍLIA	DF	Ativo Terrestre
DFL3000060	54.368,69	150	ICMBIO - INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE / SEDE	EQSW 103/104 - BLOCO C – TERREO – SETOR SUDOESTE	BRASÍLIA	DF	Ativo Terrestre
ESL3000011	4.016,97	10	RESERVA BIOLÓGICA DO CÓRREGO GRANDE	ROD. BR 101 - VINDO DE VITÓRIA, NA DIVISA ENTRE ES E BA ENTRAR À DIRETA, ESTRADA DE TERRA PICADÃO DA BAHIA, ANDAR 16 KM -	CONCEIÇÃO DA BARRA	ES	Ativo Satélite
ESL3000012	4.016,97	10	FLORESTA NACIONAL DE PACOTUBA	ROD. JOÃO DOMINGOS ZAGO - KM 2,5 - DISTRITO DE PACOTUBA	CACHOEIRO DO ITAPEMIRIM	ES	Ativo Satélite
ESL3000013	4.016,97	10	PARQUE NACIONAL DO CAPARAÓ	PORTARIA DE PEDRA MENINA	DORES DO RIO PRETO	ES	Ativo Satélite
ESL3000014	4.016,97	2	FLORESTA NACIONAL DE GOYTACAZES	ROD. BR 101 - KM 153	LINHARES	ES	Ativo Terrestre
ESL3000015	4.016,97	10	TAMAR - BASE EM REGÊNCIA	Avenida Caboclo Bernardo - Rua do Cajueiro s/nº Centro Ecológico de Regência (Próximo ao Campo de Futebol)	LINHARES	ES	Ativo Satélite

LEVANTAMENTO DE DESPESAS COM A MANUTEÇÃO DOS CIRCUITOS MPLS - CONTRATADOS JUNTO A TELEBRAS

ESL3000016	4.016,97	10	RESERVA BIOLÓGICA DO CÓRREGO DO VEADO	ESTRADA PINHEIROS – PEDRO CANÁRIO, SAINDO DE PINHEIROS A RESERVA FICA A 10KM DA CIDADE	PINHEIROS	ES	Ativo Satélite
ESL3000017	4.016,97	10	FLORESTA NACIONAL DE RIO PRETO	ROD. BR 101 - KM 27 - À DIREITA, 12 KM EM DIREÇÃO AO CÓRREGO DO ARTHUR	SÃO MATEUS	ES	Ativo Satélite
ESL3000018	4.016,97	10	RESERVA BIOLÓGICA DE SOORETAMA	ROD. ES 358 - DISTRITO DE JUNCADO	SOORETAMA	ES	Ativo Satélite
ESL3000019	4.016,97	10	RESERVA BIOLÓGICA AUGUSTO RUSCHI	ESTRADA INTERMUNICIPAL SANTA TERESA À NOVA LOMBARDIA - KM 08	SANTA TEREZA	ES	Ativo Satélite
ESL3000078	4.858,20	6	Centro Nacional de Pesquisa e Conservação de Tartarugas Marinhas e da Biodiversidade Marinha do Leste (TAMAR/ Vitoria- ES)	Av Nossa Senhora dos Navegantes - Nº 451 - Enseada do Suá - Vitória - ES - Ed. Petro Tower - Sala 1601.	VITÓRIA	ES	Ativo Terrestre
ESL3000079	4.016,97	10	REBIO Comboios - ES	Rodovia ES 440 KM 47 - Estrada Bebedouro Regência - Município de Linhares	LINHARES	ES	Ativo Satélite
ESL3000084	4.016,97	10	BASE AVANÇADA DO CENTRO TAMAR GURIRI	Avenida Oceano Atlântico - s/nº - Guriri, CEP: 29946-550	SÃO MATEUS	ES	Ativo Satélite
GOL3000012	4.065,12	4	PARQUE NACIONAL DA CHAPADA DOS VEADEIROS	RODOVIA GO 239 - KM 39 - VILA SÃO JORGE, CEP: 73.770-000	ALTO PARAÍSO DE GOIAS	GO	Ativo Satélite
GOL3000013	4.065,12	4	ÁREA DE PROTEÇÃO AMBIENTAL MEANDROS DO RIO ARAGUAIA	AV. SALUSTRINO MARTINS PINHEIRO, QD. 04 , LT. 01, POVOADO LUIZ	SÃO MIGUEL DO ARAGUAIA	GO	Ativo Satélite
GOL3000014	4.065,12	2	ÁREA DE PROTEÇÃO AMBIENTAL DAS NASCENTES DO RIO VERMELHO – (FLONA DA MATA GRANDE / RVS DAS VEREDAS DO OESTE BAIANO / RESEX DE RECANTO DAS ARARAS DE TERRA RONCA)	AV. CASTELO BRANCO - QUADRA 31 LOTE 10/11 - CENTRO, CEP: 73.970-000	MAMBAI	GO	Ativo Terrestre
GOL3000015	9.008,15	10	RAN - CENTRO DE CONSERVAÇÃO E MANEJO DE RÉPTEIS E ANFÍBIOS – (UNIDADE AVANÇADA DE ADMINISTRAÇÃO E FINANÇAS GOIÂNIA / RESEX LAGO DO CEDRO)	RUA 229 NR 95 SETOR LESTE UNIVERSITÁRIO, CEP: 74.605-090	GOIÂNIA	GO	Ativo Terrestre
GOL3000016	4.065,12	10	FLORESTA NACIONAL DE SILVÂNIA	ESTRADA SILVÂNIA - LEOPOLDO DE BULHÕES, KM 07 – ZONA RURAL, CEP: 75.180-000, Caixa Postal 21	SILVANIA	GO	Ativo Satélite
GOL3000017	4.065,12	2	RESERVA EXTRATIVISTA LAGO DO CEDRO	RUA JOSÉ JOAQUIM DE SANTANA, QUADRA 11, LOTE 09 – CENTRO, CEP: 76.710-000	ARUANÃ	GO	Ativo Terrestre
GOL3000127	4.065,01	4	Parque Nacional das Emas	RODOVIA GO 206 - KM 9, S/N	CHAPADÃO DO CÉU	GO	Ativo Satélite
GOL3000132	4.560,81	6	COORDENAÇÃO REGIONAL 10	3º PAVIMENTO, DECIMA PRIMEIRA AVENIDA, QUADRA 94, LOTES 4,6 E 8, SETOR LESTE UNIVERSITÁRIO, CEP: 74605-060	GOIÂNIA	GO	Ativo Terrestre
MAL3000013	4.160,32	4	RESERVA BIOLÓGICA DO GURUPI	ROD. BR 222 - KM 12 - DISTRITO DE PEQUIÁ	AÇAILÂNDIA	MA	Ativo Satélite
MAL3000014	4.160,32	4	RESERVA BIOLÓGICA DO GURUPI - (BASE AVANÇADA)	UTM ZONA 23M, 296062,603 LESTE E 9557522,911 NORTE - DISTANTE 140KM DA SEDE ADMINISTRATIVA DA RESERVA BIOLÓGICA	AÇAILÂNDIA	MA	Ativo Satélite
MAL3000016	4.160,32	2	CNPT – CENTRO NACIONAL DE PESQUISA E CONSERVAÇÃO DA SÓCIO-BIODIVERSIDADE ASSOCIADA A POVOS E COMUNIDADES TRADICIONAIS – (RESEX CHAPADA LIMPA / RESEX CURURUPU / RESEX QUILOMBO FREXAL)	RUA DAS HORTAS, N° 223 – CENTRO	SÃO LUIS	MA	Ativo Terrestre
MAL3000017	4.160,32	4	PARQUE NACIONAL DOS LENÇÓIS MARANHENSES	RUA PRINCIPAL DO CANTINHO - POVOADO DO CANTINHO – BARREIRINHAS	BARREIRINHAS	MA	Ativo Satélite
MAL3000090	4.160,34	4	PARQUE NACIONAL DA CHAPADA DAS MESAS	Rua Tancredo Neves, número 681, - Bairro Nova Carolina	CAROLINA	MA	Ativo Satélite
MGL3000033	4.040,34	10		RUA VALE VERDE, S/N - ZONA RURAL	ALTO CAPARAÓ	MG	Ativo Satélite
MGL3000034	3.263,76	4	PARQUE NACIONAL GRANDE SERTÃO VEREDAS	RUA GUIMARÃES ROSA, 149 - CENTRO	CHAPADA GAUCHA	MG	Ativo Satélite
MGL3000035	4.040,34	10	NGI CIPÓ PEDREIRA - PARQUE NACIONAL DA SERRA DA CIPÓ/ APA MORRO DA PEDREIRA	ROD. MG 10 KM 97, DISTRITO DE SERRA DO CIPÓ, SANTANA DO RIACHO, CEP: 35847-000, CAIXA POSTAL 21	JABOTICATUBAS	MG	Ativo Satélite
MGL3000036	4.040,34	4	ÁREA DE PROTEÇÃO AMBIENTAL CAVERNAS DO PERUAÇU (PARNA CAVERNAS DO PERUAÇU)	ROD. MGT 135 - KM 155 - PRAÇA PRINCIPAL - DISTRITO DE FABIÃO I	JANUÁRIA	MG	Ativo Satélite
MGL3000037	4.040,34	2	FLORESTA NACIONAL DE PASSA QUATRO	ESTRADA DO TABUÃO, S/N - BAIRROTABUÃO - VINDO DE SÃO PAULO CEP: 37460-000	PASSA QUATRO	MG	Ativo Terrestre
MGL3000038	4.040,34	4	FLORESTA NACIONAL DE RITÁPOLIS	FAZENDA DO POMBAL - ROD. BR 494 - KM 4 (ENTRONCAMENTO À DIREITA) - ZONA RURAL	SÃO JOÃO DEL REI	MG	Ativo Satélite
MGL3000039	4.040,34	4	PARQUE NACIONAL DA SERRA DA CANASTRA	AV. PRESISENTE TANCREDO NEVES, 498, CENTRO, CEP: 37928-000	SÃO ROQUE DE MINAS	MG	Ativo Satélite
MGL3000040	4.040,34	4	ESTAÇÃO ECOLÓGICA DE PIRAPITINGA (Base de Campo em Ilha das Marias)	RUA ENGENHERIO JULIO AUGUSTO Nº 03 Bairro DNER CEP: 39.205-000	TRÊS MARIAS	MG	Ativo Satélite
MGL3000041	4.040,34	4	PARQUE NACIONAL DAS SEMPRE-VIVAS	BECO DA PACIÊNCIA, CASA - 166, CENTRO DIAMANTINA	DIAMANTINA	MG	Ativo Satélite
MGL3000042	4.040,34	2	AREA DE PROTEÇÃO AMBIENTAL CHAPADA DO ARARIPE	ROD. BR 354 - KM 48 HORTO FLORESTAL - CENTRO	ITAMONTE	MG	Ativo Terrestre
MGL3000043	4.040,34	4	RESERVA BIOLÓGICA DA MATA ESCURA	Está localizada a 7 km da cidade de Jequitinhonha/MG, zona rural, comunidade Nova Araçatuba, coordenadas 16°23'50.50"S e 40°58'34.04"O.	JEQUITINHONHA	MG	Ativo Satélite
MGL3000045	4.040,34	2	PARQUE NACIONAL SERRA DO ROLA MOÇA	AV. MONTREAL, S/N°, B. JARDIM CANADÁ, MUNICÍPIO DE NOVA LIMA, CEP: 34000-000	NOVA LIMA	MG	Ativo Terrestre
MGL3000046	4.040,34	6	ÁREA DE PROTEÇÃO AMBIENTAL CARSTE DA LAGOA SANTA - (PFE/ RAN / COORDENAÇÃO REGIONAL 11)	ALAMEDA DRA. WILMA EDELWEISS DOS SANTOS, 115 - B. LUNDCEIA CEP: 33400-000	LAGOA SANTA	MG	Ativo Terrestre
MGL3000047	4.040,34	2	FLORESTA NACIONAL DE PARAOPEBA	RUA BARÃO ANTÔNIO CÂNDIDO, 357 - CENTRO	PARAOPEBA	MG	Ativo Terrestre
MGL3000048	4.040,34	4	RESERVA DE DESENVOLVIMENTO SUSTENTÁVEL NASCENTES GERAIZEIRAS	PRAÇA BENEDITO VALADARES, NÚMERO 29, CENTRO	RIO PARDO DE MINAS	MG	Ativo Satélite

LEVANTAMENTO DE DESPESAS COM A MANUTEÇÃO DOS CIRCUITOS MPLS - CONTRATADOS JUNTO A TELEBRAS

MGL3000327	4.040,33	10	Parque Nacional da Serra do Gandarela	Rua Afonso Pena s/n - Centro (Sede da Secretaria de Meio Ambiente de Rio Acima)	RIO ACIMA	MG	Ativo Internet
MGL3000330	4.040,36	4	Centro de Visitantes Cavernas do Peruaçu	Acesso pela rodovia BR135 Km155 - Praça principal s/nº - Bairro Fabião I - Januária. (O centro fica a 5 km da sede do Parque pela estrada municipal de Januária) Coordenada Geográfica: 15°9'23.6 S e 44° 13' 53.1 W	JANUÁRIA	MG	Ativo Satélite
MSL3000010	4.065,13	4	PARQUE NACIONAL DA SERRA DA BODOQUENA	RUA OLÍVIO JACQUES, 795 - VILA DONÁRIA	BONITO	MS	Ativo Satélite
MTL3000015	4.105,17	4	ESTAÇÃO ECOLÓGICA DE TAIAMÃ (Zonal rural)	COORDENADAS GEOGRÁFICAS: 16° 50' 34,31" S - 57° 35' 03,70" O, CEP: 78.200-000	CÁCERES	MT	Ativo Satélite
MTL3000016	4.105,17	2	ESTAÇÃO ECOLÓGICA DE TAIAMÃ – (Escritório de apoio)	AVENIDA GETULIO VARGAS, S/N – B. COC, centro, ao lado da Empaer,	CÁCERES	MT	Ativo Terrestre
MTL3000017	4.105,17	4	PARQUE NACIONAL DO PANTANAL MATOGROSSENSE	SAINDO DE POCONÉ SEGUE PELA ESTRADA TRANSPANTANEIRA ATÉ O PORTO JOFRE NO FINAL DA ESTRADA. PEGA UM BARCO 5 HORAS DE VIAGEM ATÉ A REGIÃO DA FOZ DO RIO CUIABÁ COM O RIO PARAGUAI	POCONÉ	MT	Ativo Satélite
MTL3000018	4.105,17	4	ESTAÇÃO ECOLÓGICA DA SERRA DAS ARARAS	ROD MT-343, KM 69 COMUNIDADE SALOBRA GRANDE	PORTO ESTRELA	MT	Ativo Satélite
MTL3000019	4.702,56	6	PARQUE NACIONAL DA CHAPADA DOS GUIMARÃES (CNPT / CECAV)	CERCA DE 50 KM PELA RODOVIA EMANUEL PINHEIRO, SENTIDO CUIABÁ-CHAPADA VÉU DE NOIVA	CHAPADA DOS GUIMARAES	MT	Ativo Terrestre
MTL3000021	4.105,17	2	PARQUE NACIONAL DO JURUENA	AVENIDA LUDOVICO DA RIVA NETO, N° 2364	ALTA FLORESTA	MT	Ativo Terrestre
PAL3000017	3.301,49	4	ESTAÇÃO ECOLOGICA DO JARI (base avançada)	LOCALIZADA À 87 KM AO NORTE DA CIDADE DE MONTE DOURADO - PA COM ACESSO RODOVIÁRIO VIA ESTRADA DE TERRA VIA MONTE DOURADO, SAÍDA NO SENTIDO PONTE MARIA E VILA DO BANANAL,	ALMEIRIM	PA	Ativo Satélite
PAL3000018	3.301,49	4	NÚCLEO DE GESTÃO INTEGRADA DE TROMBETAS – (REBIO DO RIO TROMBETAS / FLONA DE SARACÁ-TAQUERÁ)	PRAÇA DA FEIRINHA, S/N - PORTO TROMBETAS	ORIXIMINÁ	PA	Ativo Satélite
PAL3000019	4.078,07	2	NÚCLEO DE GESTÃO INTEGRADA DE BRAGANÇA – (RESEX MARINHA TRACUATEUA / RESEX MARINHA CAIPE TAPERAÇU / RESEX ARAI-PEROBA / RESEX GURUPI PIRIA)	AV. NAZEAZENO FERREIRA S/N, ENTRE VIGÁRIO MOTA E 07 DE SETEMBRO	BRAGANÇA	PA	Ativo Terrestre
PAL3000020	4.078,07	2	NÚCLEO DE GESTÃO INTEGRADA DE CURUÇA – (RESEX MARINHA SÃO JOÃO DA PONTA / RESEX MARINHA MÃE GRANDE DE CURUÇA / RESEX MARINHA DE MARACANÃ / RESEX MARINHA DE CHOCOARÉ-MATO GROSSO)	RUA GENERAL .GURJÃO, 748 – CENTRO	CURUÇA	PA	Ativo Terrestre
PAL3000021	3.301,49	4	ESTAÇÃO ECOLOGICA DO JARI	RUA 80, 109 BAIRRO MONTE DOURADO	MONTE DOURADO	PA	Ativo Satélite
PAL3000023	4.078,07	4	NÚCLEO DE GESTÃO INTEGRADA DE GURUPÁ	AVENIDA SÃO BENEDITO, N° 160-A, CENTRO	GURUPÁ	PA	Ativo Satélite
PAL3000024	4.078,07	10	PARQUE NACIONAL DA AMAZÔNIA – (FLONA AMANÃ)	AV. MARECHAL RONDON, S/N - B. BOM JARDIM	ITAITUBA	PA	Ativo Internet
PAL3000025	4.078,07	4	FLORESTA NACIONAL DE CARAJÁS - (REBIO TAPIRAPÉ / APA DO IGUARAPÉ GELADO)	RUA J, 202 - B. UNIÃO	PARAUEPEBAS	PA	Ativo Satélite
PAL3000026	3.301,49	10	FLORESTA NACIONAL DE TAPAJÓS – (BASE AVANÇADA)	ROD. BR 163 - ROD. SANTARÉM-CUIABÁ - KM 84	BELTERRA	PA	Ativo Satélite
PAL3000027	4.583,60	10	NÚCLEO DE GESTÃO INTEGRADA DE SANTARÉM - (FLORESTA NACIONAL DE TAPAJÓS / RESEX TAPAJÓS ARAPIUNS / RESEX RENASCER / FLONA MULATA / PROCUADORIA / COORDENAÇÃO REGIONAL 03)	AV. TAPAJÓS N° 2201 – LAGUINHO, CEP: 68040-000	SANTARÉM	PA	Ativo Internet
PAL3000029	3.301,49	4	FLORESTA NACIONAL DE CAXIUANÃ	RUA 30 DE NOVEMBRO, 2738 - B. CIDADE NOVA	CAXIUANÃ	PA	Ativo Satélite
PAL3000030	3.301,49	4	RESERVA BIOLÓGICA DO RIO TROMBETAS – (BASE AVANÇADA)	PARTINDO DE PORTO TROMBETAS, PELO RIO TROMBETAS, APROXIMADAMENTE 55 KM RIO ACIMA, ESTÁ LOCALIZADA A SEDE DA RESERVA BIOLÓGICA - COORDENADAS UTM: X:516479 - Y:9848579 - OBTER AUTORIZAÇÃO PRÉVIA DE ENTRADA, NA BASE DA RESERVA QUE FICA NA SEDE DA FLONA SARAC	ORIXIMINÁ	PA	Ativo Satélite
PAL3000031	4.078,07	4	FLORESTA NACIONAL DE CARAJÁS – (FLONA ITACAIÚNAS / FLONA TAPIRAPÉ)	RUA GUAMÁ, NO. 23 - CARAJÁS	PARAUPEBAS	PA	Ativo Satélite
PAL3000032	9.616,24	10	CEPNOR - CENTRO DE PESQUISA E GESTÃO DE RECURSOS PESQUEIROS DO LITORAL NORTE	AV. PRES. TANCREDO NEVES, N° 2501 - CAMPUS UFRA /B. MONTESE	BELÉM	PA	Ativo Terrestre
PAL3000033	3.301,49	2	PARQUE NACIONAL DA SERRA DO PARDO	RUA CORONEL JOSÉ PORFÍRIO S/N°, ESPLANADA DO XINGU, CEP: 68372-040	ALTAMIRA	PA	Ativo Internet
PAL3000034	5.838,94	6	COORDENAÇÃO REGIONAL 04 / PROCURADORIA	AV. JULIO CESAR, 7060 – VALDECANS, CEP: 66617-420	BELÉM	PA	Ativo Terrestre
PAL3000035	3.301,49	2	RESERVA EXTRATIVISTA MARINHA DE SOURE	TERCEIRA RUA, S/N B. SÃO PEDRO	SOURE	PA	Ativo Satélite
PAL3000091	5.692,69	4	NÚCLEO DE GESTÃO INTEGRADA DE BREVES – (RESEX TERRA GRANDE PRACUÚBA / RESEX MAPUÁ / RESEX ARIOCA / RESEX GURUPÁ-MELGAÇO / RVS ITATUPÃ-BAQUIÁ / FLONA CAXIUANÃ)	RUA 30 DE NOVENBRO S/N - CIDADE NOVA	BREVES	PA	Ativo Satélite
PAL3000092	4.078,07	4	RESERVA EXTRATIVISTA VERDE PARA SEMPRE	Rua Professor Simpliciana Farias, número 1535, - Porto de Moz.	Porto de Moz	PA	Ativo Satélite

LEVANTAMENTO DE DESPESAS COM A MANUTEÇÃO DOS CIRCUITOS MPLS - CONTRATADOS JUNTO A TELEBRAS

PAL3000100	4.048,06	4	BASE AVANÇADA DA UNIDADE ESPECIAL AVANÇADA	RUA ITAITUBA, S/N, BELA VISTA, NOVO PROGRESSO - PA, (DENTRO DA SEDE DO IBAMA). COORDENADA GEOGRÁFICA: 55° 24' 56,94" O e 07° 01' 34,28' S.	NOVO PROGRESSO	PA	Ativo Satélite
PAL3000101	4.078,07	10	PARQUE NACIONAL DA AMAZÔNIA – (FLONA AMANÃ)	AV. MARECHAL RONDON, S/N - Bairro BOM JARDIM - BOA ESPERANÇA	ITAITUBA	PA	Ativo Internet
PBL3000010	4.078,07	4	RESERVA BIOLÓGICA GUARIBAS	ROD. PB 071 - KM 01 - ESTRADA DE JACARAÚ - ZONA RURAL	MAMANGUAPE	PB	Ativo Satélite
PBL3000011	4.078,07	4	ÁREA DE PROTEÇÃO AMBIENTAL BARRA DO RIO MAMANGUAPE - (ARIE MANGUEZAIS DA FOZ DO RIO MAMANGUAPE)	Rua da Vitória, S/N° Bonfim Rio Tinto/PB - (ao lado da CAGEPA, bem perto do SESI)	RIO TINTO	PB	Ativo Satélite
PBL3000012	4.583,60	6	CEMAVE - CENTRO NACIONAL DE PESQUISA PARA CONSERVAÇÃO DAS AVES SILVESTRES	ESTRADA DE CABEDELO, S/N - BR-230 KM 10	CABEDELO	PB	Ativo Terrestre
PBL3000014	10.813,86	10	FLORESTA NACIONAL DE RESTINGA DE CABEDELO (UNIDADE AVANÇADA DE ADMINISTRAÇÃO E FINANÇAS DE CABEDELO / COORDENAÇÃO REGIONAL 06)	ESTRADA DE CABEDELO, S/N - BR-230 KM 10 - Bairro: Amazônia Park	CABEDELO	PB	Ativo Terrestre
PEL3000020	3.301,49	4	ICMBio NORONHA - NGI DE FERNANDO DE NORONHA	RUA EURICO CAVALCANTI DE ALBUQUERQUE Nº 174 BAIRRO BOLDRO SEDEO ADMINISTRATIVO DE FERNANDO DE NORONHA	FERNANDO DE NORONHA	PE	Ativo Satélite
PEL3000021	4.078,07	4	RESERVA BIOLÓGICA DE SALTINHO	RODOVIA PE 60, KM 60, TREVO DA ENTRADA DE TAMANDARÉ	TAMANDARÉ	PE	Ativo Satélite
PEL3000022	4.078,07	4	RESERVA BIOLÓGICA SERRA NEGRA	RUA SANTA ISABEL,S/NR	IBIMIRIM	PE	Ativo Satélite
PEL3000023	4.078,07	4	FLORESTA NACIONAL DE NEGREIROS	SITIO NEGREIROS – ZONA RURAL DO MUNICIPIO DE SERRITA	SERRITA	PE	Ativo Satélite
PEL3000025	5.224,31	6	CEPENE - CENTRO DE PESQUISA E GESTÃO DE RECURSOS PESQUEIROS DO LITORAL NORDESTE (NGI COSTA DOS CORAIS)	RUA SAMUEL HARDMAN, S/N - CENTRO, CEP: 55578-000	TAMANDARÉ	PE	Ativo Terrestre
PEL3000135	4.077,99	4	CEPENE - Base Avançada	ESTRADA DO FORTE ORANGE, S/N° CX POSTAL 01	ITAMARACA	PE	Ativo Satélite
PIL3000013	4.319,66	4	APA DELTA DO PARNAÍBA (BASE) PROJETO PEIXE-BOI NO PIAUÍ	AVENIDA HERMÍNIO CAETANO, S/N - CENTRO	CAJUEIRO DA PRAIA	PI	Ativo Satélite
PIL3000014	4.319,66	4	PARQUE NACIONAL DA SERRA DAS CONFUSÕES	RUA JOÃO DIAS, 398 - CENTRO	CARACOL	PI	Ativo Satélite
PIL3000015	4.319,66	10	PARQUE NACIONAL DE SETE CIDADES	sete	PIRACURUCA	PI	Ativo Satélite
PIL3000016	4.319,66	4	PARQUE NACIONAL DA SERRA DA CAPIVARA	RUA DOUTOR LUIZ PAIXÃO,188 – B.: MILONGA	SÃO RAIMUNDO NONATO	PI	Ativo Satélite
PIL3000017	4.319,66	4	FLORESTA NACIONAL DE PALMARES	BR – 343, KM 327	ALTOS	PI	Ativo Satélite
PIL3000018	5.224,31	6	APA DELTA DO PARNAIBA / RESEX MARINHA DELTA DO PARNAIBA / CMA DO PIAUI (COORDENAÇÃO REGIONAL 05)	RUA MERVAL VERAS, N° 80 - B. DO CARMO	PARNAÍBA	PI	Ativo Terrestre
PIL3000019	4.319,66	4	PARQUE NACIONAL DAS NASCENTES DO RIO PARNAÍBA	AV. NOSSA SENHORA DA CONCEIÇÃO, ALÇA OESTE, N° 45, B. NOVA CORRENTE – CORRENTE PI	CORRENTE	PI	Ativo Satélite
PRL3000022	4.065,13	4	FLORESTA NACIONAL DE ASSUNGUI	ROD. BR 277 - SENTIDO CURITIBA - PONTA GROSSA, CHEGANDO EM CAMPO LARGO	CAMPO LARGO	PR	Ativo Satélite
PRL3000023	4.065,13	4	FLORESTA NACIONAL DE IRATI	ROD. BR 153 - KM 325 - (TRECHO IRATI-IMBITUVA)	FERNANDES PINHEIRO	PR	Ativo Satélite
PRL3000024	4.065,13	4	PARQUE NACIONAL DO SUPERAGUI	BARRA DE SUPERAGUI - ILHA DE SUPERAGUI	GUARAQUEÇABA	PR	Ativo Satélite
PRL3000025	9.008,16	10	PARQUE NACIONAL DO IGUAÇU – (UNIDADE AVANÇADA DE ADMINISTRAÇÃO E FINANÇAS DE FOZ DO IGUAÇU)	BR-469 KM 22,5 - SEDE ADMINISTRATIVA DO PARQUE-CX. P. 05	FOZ DO IGUAÇU	PR	Ativo Terrestre
PRL3000026	4.065,13	2	PARQUE NACIONAL DE ILHA GRANDE II	RUA BARÃO DO RIO BRANCO, 787 - B. VILA VELHA	GUAIRA	PR	Ativo Terrestre
PRL3000027	4.065,13	2	FLORESTA NACIONAL DE PIRAÍ DO SUL	ESTRADA DO CERNE, KM 152 - B. MACHADINHO	PIRAÍ DO SUL	PR	Ativo Terrestre
PRL3000028	4.065,13	2	PARQUE NACIONAL DE CAMPOS GERAIS – (REBIO DAS ARAUCÁRIAS)	Rua Jaime Pinto Rosas nº 81 Bairro Jardim Carvalho	PONTA GROSSA	PR	Ativo Terrestre
PRL3000029	4.065,13	2	REFÚGIO DE VIDA SILVESTRE DOS CAMPOS DE PALMAS – (ESEC DA MATA PRETA / PARNA DAS ARAUCÁRIAS)	RUA DOUTOR BEVILÁQUA, 863 (SOBRELOJA) - CENTRO, ENTRE AS RUAS MARECHAL DEODORO E AV. CLEVELÂNDIA	PALMAS	PR	Ativo Terrestre
PRL3000030	4.065,13	2	PARQUE NACIONAL DE ILHA GRANDE	AVENIDA RIO DE JANEIRO , N° 4870, ZONA II, CEP: 87501-370	UMUARAMA	PR	Ativo Terrestre
PRL3000031	4.065,13	2	ÁREA DE PROTEÇÃO AMBIENTAL DE GUARAQUEÇABA – (ESEC DE GUARAQUEÇABA)	RUA PAULA MIRANDA, N°10	GUARAQUEÇABA	PR	Ativo Terrestre
PRL3000033	4.065,13	2	PARQUE NACIONAL DE SAINT-HILAIRE/LANGE	AV. PARANAGUÁ, 729 - BALNEÁRIO FLAMINGO	MATINHOS	PR	Ativo Terrestre
PRL3000034	4.065,13	10	RESERVA BIOLÓGICA DAS PEROBAS	AV. RIO DE JANEIRO, N° 308	TUNEIRAS DO OESTE	PR	Ativo Satélite
RJL3000044	4.065,13	2	ÁREA DE PROTEÇÃO AMBIENTAL DE PETRÓPOLIS	ESTRADA UNIÃO E INDÚSTRIA, 9.722 - ITAIPAVA	ITAIPAVA	RJ	Ativo Terrestre
RJL3000045	4.065,13	4	PARQUE NACIONAL DE ITATIAIA	ESTRADA DO PARQUE NACIONAL (BR 485), KM 8,5 - SEDE ADMINISTRATIVA / CAIXA POSTAL 83657	ITATIAIA	RJ	Ativo Satélite
RJL3000047	4.065,13	2	PARQUE NACIONAL DA RESTINGA DE JURUBATIBA	Avenida Atlântica, s/n° Lagomar – Macaé – RJ – CEP 27966-080	MACAÉ	RJ	Ativo Terrestre
RJL3000048	4.065,13	4	RESERVA BIOLÓGICA DO TINGUÁ	ESTRADA DO COMÉRCIO, n º 3400 ,TINGUÁ	NOVA IGUAÇU	RJ	Ativo Satélite
RJL3000049	4.065,13	2	ÁREA DE PROTEÇÃO AMBIENTAL DE CAIRUÇU	RUA 8, N° 3 - B. PORTAL DAS ARTES	PARATI	RJ	Ativo Terrestre
RJL3000050	4.065,13	2	ESTAÇÃO ECOLÓGICA DE TAMOIOS	ROD. BR 101, KM 531,5 - MAMBUCABA / PARATI	PARATI	RJ	Ativo Terrestre
RJL3000051	4.065,13	4	RESERVA BIOLÓGICA UNIÃO	ROD. BR 101 - KM 185 - B. ROCHA LEÃO	RIO DAS OSTRAS	RJ	Ativo Satélite
RJL3000052	4.065,13	2	FLORESTA NACIONAL MÁRIO XAVIER	ANTIGA ESTRADA RIO-SÃO PAULO - KM 51	SEROPÉDICA	RJ	Ativo Terrestre
RJL3000053	4.065,13	2	RESERVA EXTRATIVISTA MARINHA ARRAIAL DO CABO – (CMA)	RUA MARECHAL FLORIANO PEIXOTO S/N	ARRAIAL DO CABO	RJ	Ativo Terrestre
RJL3000054	4.065,13	4	NÚCLEO DE GESTÃO INTEGRADA GUAPI-MIRIM GUANABARA - (APA DE GUAPI-MIRIM / ESEC DA GUANABARA)	RODOVIA BR 493, KM 12,8 - VALE DAS PEDRINHAS	GUAPIMIRM	RJ	Ativo Satélite
RJL3000055	4.560,81	6	PARQUE NACIONAL DE SERRA DOS ÓRGÃOS	AVENIDA ROTARIANA - PARQUE NACIONAL DA SERRA DOS ORGÃOS	TERESÓPOLIS	RJ	Ativo Terrestre

LEVANTAMENTO DE DESPESAS COM A MANUTEÇÃO DOS CIRCUITOS MPLS - CONTRATADOS JUNTO A TELEBRAS

RJL3000056	8.736,63	10	UNIDADE AVANÇADA DE ADMINISTRAÇÃO E FINANÇAS DO RIO DE JANEIRO, PROCURADORIA, MONA CAGARRAS (COORDENAÇÃO REGIONAL 08)	ESTRADA VELHA DA TIJUCA, N° 77. PRÉDIO ANEXO	RIO DE JANEIRO	RJ	Ativo Terrestre
RJL3000057	4.065,13	2	ÁREA DE RELEVANTE INTERESSE ECOLÓGICO DA FLORESTA DA CICUTA	RUA 18-A, N° 68 - VILA SANTA CECÍLIA, CEP: 27260-380	VOLTA REDONDA	RJ	Ativo Terrestre
RJL3000058	4.560,81	6	UNIDADE AVANÇADA DE ADMINISTRAÇÃO E FINANÇAS DE TERESÓPOLIS	AV. ROTARIANA - PARQUE NACIONAL DA SERRA DOS ÓRGÃOS (140 M do local atual)	TERESÓPOLIS	RJ	Ativo Terrestre
RNL3000008	4.078,07	2	FLORESTA NACIONAL DO AÇU	RUA POETA RENATO CALDAS, S/N	AÇU	RN	Ativo Terrestre
RNL3000009	4.078,07	4	RESERVA BIOLÓGICA DO ATOL DAS ROCAS	ÁGUAS JURISDICIONAIS BRASILEIRAS	NATAL	RN	Ativo Satélite
RNL3000010	4.078,07	4	ESTAÇÃO ECOLÓGICA DO SERIDÓ	ROD. BR 427 - KM 128 - ZONA RURAL	SERRA NEGRA DO NORTE	RN	Ativo Satélite
RNL3000011	4.078,07	2	FLORESTA NACIONAL DE NÍSIA FLORESTA	ESTRADA DO TIMBÓ, S/N - ZONA RURAL	NISIA FLORESTA	RN	Ativo Terrestre
RNL3000062	4.078,07	2	REBIO ATOL DAS ROCAS	Rua Alexandrino de Alencar, 1399 - Tirol -	NATAL	RN	Ativo Terrestre
RNL3000064	4.016,51	2	PARQUE NACIONAL FURNA FEIA	Rua Dr. Almir de Almeida Castro - nº 400 - Centro Sala 802 Edifício Liz Empresarial - Caminho das Árvores	MOSSORÓ	RN	Ativo Terrestre
ROL3000012	4.016,95	4	PARQUE NACIONAL DA SERRA DE PACAAS NOVOS	AVENIDA TANCREDO NEVES, SETOR 2 - CENTRO	CAMPO NOVO DE RONDONIA	RO	Ativo Satélite
ROL3000013	4.016,95	2	RESERVA BIOLÓGICA DO JARÚ + NGI COSTA MARQUES	RUA SÃO CRISTOVÃO, 903, JARDIM PRESIDENCIAL	JI-PARANÁ	RO	Ativo Terrestre
ROL3000014	4.016,92	4	RESERVA EXTRATIVISTA DO LAGO DO CUNIÃ – (BASE AVANÇADA)	LAGO DO CUNIÃ – MARGEM ESQUERDA - COMUNIDADE. SILVA LOPES E ARAÚJO, ZONA RURAL	PORTO VELHO	RO	Ativo Satélite
ROL3000015	4.016,92	4	ESTAÇÃO ECOLÓGICA DE CUNIÃ	ROD. BR 319 - KM 120 - SENTIDO PORTO VELHO - HUMAITÁ, ZONA RURAL	PORTO VELHO	RO	Ativo Satélite
ROL3000016	4.016,92	4	RESERVA BIOLÓGICA DO GUAPORÉ – (BASE AVANÇADA)	A MARGEM DIREITA DO RIO GUAPORÉ	COSTA MARQUES	RO	Ativo Satélite
ROL3000017	4.016,92	4	FLORESTA NACIONAL DE JAMARI	ROD. RO 452 - KM 7,5 - ZONA RURAL	ITAPUÃ DO OESTE	RO	Ativo Satélite
ROL3000018	15.300,00	20	COORDENAÇAO REGIONAL 01 - (FLORESTA NACIONAL BOM FUTURO / PARQUE NACIONAL MAPINGUARI / PARQUE NACIONAL CAMPOS AMAZÔNICOS / FLORESTA NACIONAL JACUNDÁ / FLONA JAMIRI / ESTAÇÃO ECOLÓGICA CUNIÃ / RESERVA EXTRATIVISTA LAGO DO CUNIÃ / NGI HUMAITA - FLONA JATUARANA /PARNA LAGO DO JARI, FLONA BALATA TUFARI)	AV. LAURO SODRÉ 6500, BAIRO AEROPORTO CEP: 76803-260	PORTO VELHO	RO	Ativo Terrestre
ROL3000020	4.016,92	6	NÚCLEO DE GESTÃO INTEGRADA DE GUAJARÁ-MIRIM SEDE	Av. dos Seringueiros 1343, Bairro 10 de abril	GUAJARÁ-MIRIM	RO	Ativo Terrestre
ROL3000023	4.016,92	4	BASE DE FISCALIZAÇÃO BOCA DO JARU DA REBIO JARU	LINHA 612, S/N, DISTRITO DE SANTA ROSA, COORDENADAS: LAT. 10° 04' 07.20" S LOG. 61° 58' 17.86" W,	VALE DO PARAISO	RO	Ativo Satélite
ROL3000055	4.016,92	4	RESERVA EXTRATIVISTA do Rio Preto - Pompeu	As margens do Rio Ouro, Final da Estrada do Palheta, às margens do Rio Ouro Preto. Coordenadas Geograficas: 10º55'03,17" 065º02'34,46"	GUAJARÁ-MIRIM	RO	Ativo Satélite
ROL3000056	4.016,92	4	BASE DE APOIO DA RESERVA EXTRATIVISTA RIO CAUTÁRIO	Margens da direita do Rio Cautário no fim da linha 52 da BR Federal 429 em Rondônia, na frente da Comunidade Laranjal. Coordenação geográfica: 11°52'37.02"S;64° 8'15.19"W	COSTA MARQUES	RO	Ativo Satélite
ROL3000058	4.016,89	4	BASE AVANÇADA DA RESEX BARREIRO DAS ANTAS	Avenida dos Seringueiros 1343, Bairro 10 de Abril (Endereço da Sede).	GUAJARÁ-MIRIM	RO	Ativo Satélite
ROL3000060	4.016,97	4	RESERVA BIOLÓGICA DO GUAPORÉ – (BASE AVANÇADA)	PORTO MURTINHO, ZONA RURAL	SÃO FRANCISCO DO GUAPORÉ	RO	Ativo Satélite
RRL3000009	4.016,95	4	PARQUE NACIONAL DO VIRUÁ	Endereço: BR-174, Km 322, Zona Rural, Caracaraí/RR. CEP 69.360-000	CARACARAÍ	RR	Ativo Satélite
RRL3000010	3.240,39	10	ESTAÇÃO ECOLÓGICA DE MARACÁ	NA ESTRADA QUE VAI PARA ALTO ALEGRE, VIRAR À DIREITA NA SUB-ESTAÇÃO DE ENERGIA NA LOCALIDADE DE SUCUBA, EM DIREÇÃO DA COMUNIDADE INDÍGENA DO BOQUEIRÃO DO IGARAPÉ GRANDE	ALTO ALEGRE	RR	Ativo Satélite
RRL3000011	4.016,95	10	NÚCLEO DE GESTÃO INTEGRADA DE RORAIMA – (ESEC MARACÁ / FLONA RORAIMA)	RUA ALFREDO CRUZ, 283, CENTRO, CEP: 69301-140	BOA VISTA	RR	Ativo Satélite
RRL3000012	3.240,39	10	PARQUE NACIONAL DO MONTE RORAIMA	AV. PANAMERICANA, S/N (AO LADO DO MINISTÉRIO DA AGRICULTURA) - CENTRO	PACARAIMA	RR	Ativo Satélite
RRL3000013	4.016,95	2	NÚCLEO DE GESTÃO INTEGRADA CARACARAÍ	AVENIDA BEM-QUERER, 2337, CENTRO, BAIRRO SÃO FRANCISCO- CEP 69360-000	CARACARAÍ	RR	Ativo Terrestre
RSL3000022	4.078,07	4	FLORESTA NACIONAL DE CANELA	RUA OTAVIANO DO AMARAL PIRES, 5000/ULISSES DE ABREU	CANELA	RS	Ativo Satélite
RSL3000023	4.078,07	10	PARQUE NACIONAL DE APARADOS DA SERRA – (PARNA DE SERRA GERAL)	RODOVIA RS-429, KM 18, CEP: 95480-000	CAMBARÁ DO SUL	RS	Ativo Satélite
RSL3000024	4.078,07	10	PARQUE NACIONAL DA LAGOA DO PEIXE	PRAÇA PREFEITO LUIZ MARTINS, 30 - CENTRO	MOSTARDAS	RS	Ativo Satélite
RSL3000025	4.078,07	10	FLORESTA NACIONAL DE PASSO FUNDO	AV. PRESIDENTE VARGAS, S/N	MATO CASTALHANO	RS	Ativo Satélite
RSL3000026	4.078,07	4	ESTAÇÃO ECOLÓGICA DE ARACURI-ESMERALDA	ESTRADA BANHADO SECO, 550-INTERIOR - 2° DISTRITO - BOM RETIRO - ACESSO PELA BR 285	MUITOS CAPÕES	RS	Ativo Satélite
RSL3000027	4.078,07	4	ESTAÇÃO ECOLÓGICA DO TAIM	ROD. BR 471 - KM 492	RIO GRANDE	RS	Ativo Satélite
RSL3000028	4.078,07	4	FLORESTA NACIONAL DE SÃO FRANCISCO DE PAULA	ROD. RS 484 - KM 06 - ESTRADA DE MORRINHOS, CEP: 95.400-000	SÃO FRANCISCO DE PAULA	RS	Ativo Satélite
RSL3000029	4.078,07	4	REFÚGIO DA VIDA SILVESTRE DA ILHA DOS LOBOS	TRAV. FRANCISCO TEIXEIRA, 16; CENTRO	TORRES	RS	Ativo Satélite
RSL3000185	4.388,68	4	Base do CEPSUL em Rio Grande - RS	RUA MARIA ARAÚJO Nº 470 BAIRRO CASSINO - RS, CEP: 96200-190	RIO GRANDE	RS	Ativo Satélite

LEVANTAMENTO DE DESPESAS COM A MANUTEÇÃO DOS CIRCUITOS MPLS - CONTRATADOS JUNTO A TELEBRAS

RSL3000188	4.078,07	2	AREA DE PROTEÇÃO AMBIENTAL CHAPADA DE IBIRATUIPÃ	Rua 13 de Maio, 410 - sala 702	SANTANA DO LIVRAMENTO	RS	Ativo Terrestre
SCL3000018	4.016,95	4	FLORESTA NACIONAL DE CAÇADOR	ROD. SC 451 - KM 159 - DISTRITO DE TAQUARA VERDE	CAÇADOR	SC	Ativo Satélite
SCL3000019	4.016,95	4	FLORESTA NACIONAL DE CHAPECÓ	ESTRADA CHAPECÓ-SÃO CARLOS - CERCA DE 13 KM DEPOIS DA FAZENDA ZANDAVALI- SC283(ESTRADA ESTADUAL)	GUATAMBU	SC	Ativo Satélite
SCL3000020	4.016,95	4	FLORESTA NACIONAL DE IBIRAMA	ESTRADA GERAL DO RIBEIRÃO TAQUARAS, S/N	IBIRAMA	SC	Ativo Satélite
SCL3000021	4.016,95	4	FLORESTA NACIONAL DE TRÊS BARRAS	ROD. BR 280 - KM 224	TRES BARRAS	SC	Ativo Satélite
SCL3000022	4.016,95	2	PARQUE NACIONAL DE SÃO JOAQUIM	AV. FELICISSIMO RODRIGUES SOBRINHO, 1542	URUBICI	SC	Ativo Terrestre
SCL3000023	4.016,95	2	PARQUE NACIONAL DA SERRA DO ITAJAÍ	RUA PROGRESSO, 167 - B. PROGRESSO	BLUMENAU	SC	Ativo Terrestre
SCL3000024	8.503,15	10	ESTAÇÃO ECOLÓGICA DE CARIJÓS - (APA ANHATOMIRIM / REBIO ARVOREDO / COORDENAÇÃO REGIONAL 09 / CMA / CEMAVE / CNPT)	ROD. MAURÍCIO SIROTSKY SOBRINHO, S/N - KM 2, CEP: 88053-701	FLORIANÓPOLIS	SC	Ativo Terrestre
SCL3000025	4.016,95	2	RESERVA EXTRATIVISTA DE PIRAJUBAÉ	JOÃO CÂNCIO JAQUES, 1375 - COSTEIRA DO PIRAJUBAÉ	FLORIANÓPOLIS	SC	Ativo Terrestre
SCL3000026	4.475,99	6	CEPSUL - CENTRO DE PESQUISA E GESTÃO DE RECURSOS PESQUEIROS DO LITORAL SUDESTE E SUL	AV. MINISTRO VICTOR KONDER, N.° 374	ITAJAÍ	SC	Ativo Terrestre
SCL3000027	4.016,95	10	ÁREA DE PROTEÇÃO AMBIENTAL BALEIA FRANCA	AVENIDA SANTA CATARINA, 1465 - B. PAS LEME	IMBITUBA	SC	Ativo Satélite
SEL3000007	4.078,07	10	FLORESTA NACIONAL DE IBURA	ROD. BR 101, KM 85	NOSSA SENHORA DO SOCORRO	SE	Ativo Internet
SEL3000009	4.078,07	4	PARQUE NACIONAL SERRA DE ITABAIANA	ROD. BR 235 - KM 34 - ENTRAR NA GURARITA DO IBAMA E ANDAR 2,5KM PELA ESTRADA DE TERRA (ESTRADA DO POÇO DAS MOÇAS)	AREIA BRANCA	SE	Ativo Satélite
SEL3000010	4.078,07	4	RESERVA BIOLÓGICA DE SANTA ISABEL - (TAMAR - BASE PIRAMBU)	EM ARACAJÚ, PEGAR UMA BALSA PARA BARRA DOS COQUEIROS E VIAJAR 27 KM ATÉ A CIDADE DE PIRAMBU. A RESEX FICA NA PRAIA DE PIRAMBÚ, VISINHA AO TERMINAL TURÍSTICO	PIRAMBU	SE	Ativo Satélite
SPL3000043	3.240,36	2	RESERVA EXTRATIVISTA DO MANDIRA	RUA JOSÉ ANTONIO DE CAMPOS, 297 - 2° ANDAR - SALA 22	REGISTRO	SP	Ativo Terrestre
SPL3000044	3.240,36	4	FLORESTA NACIONAL CAPÃO BONITO	ROD. SP 258 (ROD. FRANCISCO ALVES NEGRÃO) - KM 241	CAPÃO BONITO	SP	Ativo Satélite
SPL3000045	3.240,36	2	FLORESTA NACIONAL DE LORENA	AV. MAJOR ERMENEGILDO ANTÔNIO AQUINO, S/N - B. COATINGA - HORTO	LORENA	SP	Ativo Terrestre
SPL3000046	8.001,48	6	CENAP - CENTRO NACIONAL DE PESQUISA PARA A CONSERVAÇÃO DOS PREDADORES NATURAIS – (UNIDADE AVANÇADA DE ADMINISTRAÇÃO E FINANÇAS ATIBAIA)	ESTRADA MUNICIPAL HISAICHI TAKEBAIYASHI S/N° - B. DA USINA - ÁREA URBANA DE ATIBAIA	ATIBAIA	SP	Ativo Internet
SPL3000048	19.030,11	40	ACADEBIO	ESTRADA VICINAL IPÊ, 265 - KM 19,5 - FAZENDA IPANEMA	IPERÓ	SP	Ativo Terrestre
SPL3000049	3.240,36	2	ÁREA DE PROTEÇÃO AMBIENTAL CANANÉIA-IGUAPE-PERUÍBE - (ARIE ILHA DO AMEIXAL)	RUA DA SAUDADE, 350 - CANTO DO MORRO	IGUAPE	SP	Ativo Terrestre
SPL3000050	15.300,00	20	CEPTA - CENTRO DE PESQUISA E GESTÃO DE RECURSOS PESQUEIROS CONTINENTAIS	ROD EUBERTO NEMESIO PEREIRA DE GODOY KM 6,5 - B. CACHOEIRA DE EMAS	PIRASSUNUNGA	SP	Ativo Terrestre
SPL3000051	3.240,36	1	PARQUE NACIONAL DA SERRA DA BOCAINA	RODOVIA ESTADUAL FRANCISCA MENDES RIBEIRO - SP 221 – CENTRO	SAO JOSÉ DO BARREIRO	SP	Ativo Satélite
SPL3000052	4.858,20	6	ESTAÇÃO ECOLÓGICA TUPINAMBÁS	AVENIDA MANOEL HIPOLITO DO REGO Nº 1.907 - BAIRRO ARRASTÃO CEP:11605-136	SÃO SEBASTIÃO	SP	Ativo Terrestre
SPL3000053	4.858,20	6	ÁREA DE PROTEÇÃO AMBIENTAL DA BACIA DO RIO PARAIBA DO SUL	AV. OLIVIO GOMES, 100 – SANTANA PQ. DA CIDADE – ANEXO À CASA DE CAFÉ	SÃO JOSÉ DOS CAMPOS	SP	Ativo Terrestre
SPL3000054	3.240,36	2	ESTAÇÃO ECOLÓGICA DE TUPINIQUINS - (ARIE DAS ILHAS DA QUEIMADA GRANDE E PEQUENA)	RUA DON SEBASTIÃO LEME, 135 - VILA IVOTY	ITANHAÉM	SP	Ativo Terrestre
SPL3000055	3.240,36	2	ESTAÇÃO ECOLÓGICA MICO-LEÃO-PRETO	RUA BOIADEIRA NORTE NR 3-27 VILA SANTA ROSA	PRESIDENTE EPITÁCIO	SP	Ativo Terrestre
SPL3000477	4.858,20	6	CMA - CENTRO MAMÍFEROS AQUÁTICOSCMA - CENTRO MAMÍFEROS AQUÁTICOS	Edifício VISTAMAR, Rua Alexandre Herculano nº 197, Bairro Gonzaga, CEP: 11050-031	SANTOS	SP	Ativo Terrestre
TOL3000010	4.065,13	4	ESTAÇÃO ECOLÓGICA SERRA GERAL DO TOCANTINS – (APA DA SERRA DE TABATINGA)	AV. BEIRA RIO, QUADRA 2 NÚMERO 6 - CENTRO	RIO DA CONCEIÇÃO	TO	Ativo Satélite
TOL3000011	4.065,13	4	PARQUE NACIONAL DO ARAGUAIA	AV. TANCREDO NEVES, 494 - SETOR JARDIM PRIMAVERA	PIUM	TO	Ativo Satélite

VALOR TOTAL MENSAL	**R$ 1.109.952,21**
BANDA TOTAL CONTRATADA (Mbps)	**1351**
QUANTIDADE DE CIRCUITOS INSTALADOS	**241**
CUSTO MÉDIO MENSAL DE MPLS POR CIRCUITO	**R$ 4.605,61**

Anexo II - Nota Técnica 25 - Caderno de testes - POC FW RAN GOIANIA.pdf

Central IT – Governança Corporativa
Instituto Chico Mendes de Conservação da Biodiversidade
Contrato 18/2017

NOTA TÉCNICA N. 025/2021/CentralIT Governança Corporativa

Assunto: POC - Proof of Concept (Implantação de Firewall)

1- Objetivo

Esta Prova de Conceito - POC teve como objetivo avaliar tecnicamente a solução de segurança de redes do Instituto Chico Mendes de Conservação da Biodiversidade – ICMBio, com o propósito de reestruturar toda a rede de comunicação desta autarquia. O equipamento atualmente instalado (fornecedor: Check Point) apresenta segurança nas soluções de internet e VPN que inclui: *firewall*, proteção contra-ataques a redes, aplicações e gerenciamento centralizado de vários *firewalls*.

Para avaliação da gerência centralizada do firewall na sede do ICMBio em Brasília, foi instalado um equipamento de mesmo fornecedor (firewall Check Point, modelo 1470/1490) no Centro Nacional de Pesquisa e Conservação de Répteis e Anfíbios (RAN/ICMBio) em Goiânia-GO, em parceria com a empresa de telecomunicações Telefônica Brasil S.A (VIVO), sem custos à administração pública.

2- Informações e Contatos

ICMBio – SEDE	
Contato	Márcio Gomes
Cargo	Administrativo
E-mail	marcio.gomes.terceirizado@icmbio.gov.br
Telefone	(61) 98567-2860
Contato	Rodrigo Lopes
Cargo	Chefe de Serviço - SISUP
E-mail	rodrigo.lopes@icmbio.gov.br
Telefone	(61) 99266-4450

CentralIT	
Contato	Janilson Sousa
Cargo	Gerente
E-mail	Janilson.sousa@centrailit.com.br
Telefone	(61) 99936-6379

ICMBio – RAN GOIANIA	
Contato	Regenildo
Telefone	(62) 99802-6780

VIVO	
Contato	Abílio Neto
Cargo	VIVO

Telefone	(61) 99987-7767

L8	
Contato	Allan Follmann
Cargo	L8
Telefone	(41) 9649-1409

3- Estrutura Atual

REDE MPLS VIA TERRESTRE

Abaixo, segue o atual diagrama do link MPLS via terrestre que interliga a rede do RAN à rede do ICMBio na sede.

➢ Localidade: Centro Nacional de Pesquisa e Conservação de Répteis e Anfíbios (RAN/ICMBio);

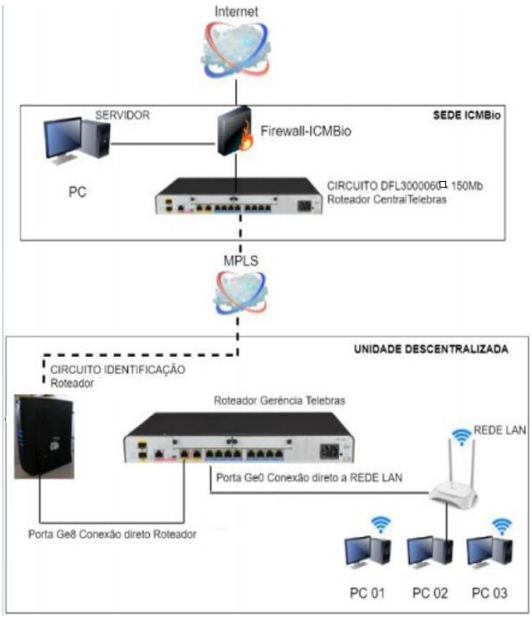
➢ Identificação do Circuito: GOL3000015 / Link: 10Mb;

➢ Custo Mensal Link MPLS: R$ 9.273,89;

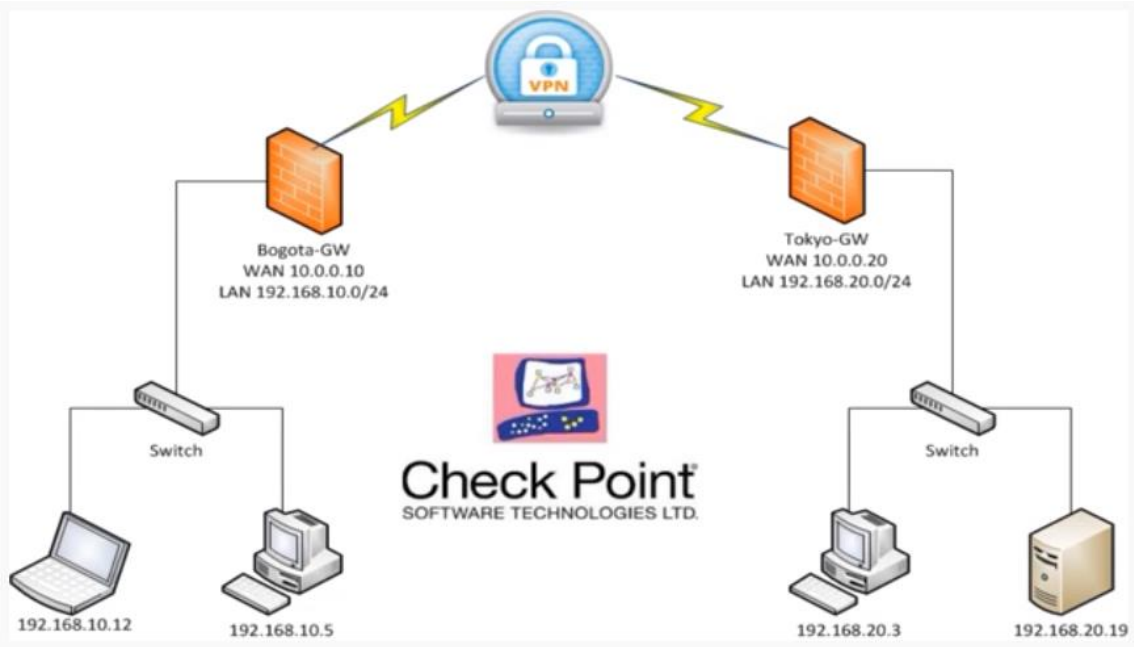
➢ Quantidade de Equipamentos: 30 Ativos (Desktop/impressoras/voips/switch/Wifi/roteador);

➢ Faixa de Range: 10.62.208.0/24 e Gateway: 10.62.208.1.

A estrutura de rede nesta unidade é formada por identificação do circuito, com um roteador terrestre e um roteador de gerência, ambos de responsabilidade da contratada Telebrás (atual fornecedora do serviço de internet do ICMBio), além da rede LAN (HUB/SWITCH e Roteador WIFI) pertencente ao ICMBio.



4- Estrutura de rede do RAN com a solução Check Point implantada



5- Migração da solução

5.1 Equipamentos Instalados:

O equipamento modem foi instalado e configurado pela empresa VIVO. Após fixação do endereço WAN, foi iniciado pela empresa L8 (representante Check Point) as configurações do equipamento firewall 1470/1490.

ITEM	DESCRIÇÃO-OBSERVAÇÃO	EVIDÊNCIA
01	1- Modem vivo instalado e configurado IP-DINÂMICO na interface WAN. 2- Firewall Check Point modelo 1470/1490 Appliance instalado e configurado em modo BRIDGE no RANGE 10.62.209.0/24 fora do projeto MPLS do ICMBio-SEDE, não gerando conflito de endereçamento.	

5.2 Teste com endereçamento:

Dia 15 de junho de 2021: Após a confirmação das empresas sobre as configurações dos equipamentos da VIVO e Check Point, foram iniciados os testes de endereçamento de rede LAN.

ITEM	DESCRIÇÃO-OBSERVAÇÃO	EVIDÊNCIA
01	1- Verificado as configurações de endereçamento LAN fornecido pelo serviço de DHCP do Firewall Check Point. O endereço utilizado está dentro da faixa de range de distribuição, entre 10.62.209.20/24 até 10.62.209.254/24 com Gateway 10.62.209.1 e DNS 10.197.32.131.	

5.3 Teste de ROTA:

No mesmo dia, após a confirmação da empresa sobre as configurações e conexões de VPN entre Firewalls Check Point, foi iniciado os testes de rota.

ITEM	DESCRIÇÃO-OBSERVAÇÃO	EVIDÊNCIA
01	1- Verificado a conexão de rota após configurações e testes com conexão VPN entre Firewalls do Check Point executados pela empresa L8. O Tempo de resposta entre RAN de Goiânia e ICMBio sede, é de 53ms sem perda de pacotes.	

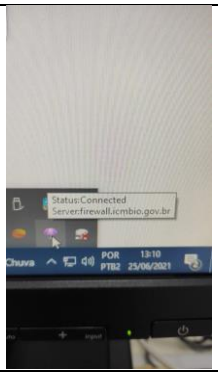
5.4 Teste de Voip:

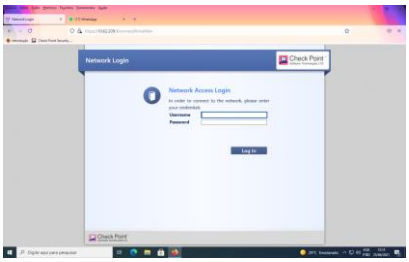
Ainda no dia 15 de julho, conforme testes executados nos item 5.2 e 5.3, foram iniciados os testes com VoIP da Marca Polycom.

ITEM	DESCRIÇÃO-OBSERVAÇÃO	EVIDÊNCIA
01	1- Após inicialização do Voip ramal 9959, foi verificado a normalidade do telefone.	

5.5 Autenticação Check Point:

Dia 25 de junho de 2021: Conforme testes executados nos item 5.2 e 5.3, foram iniciados os testes de navegação com autenticação Check Point e filtro de conteúdo.

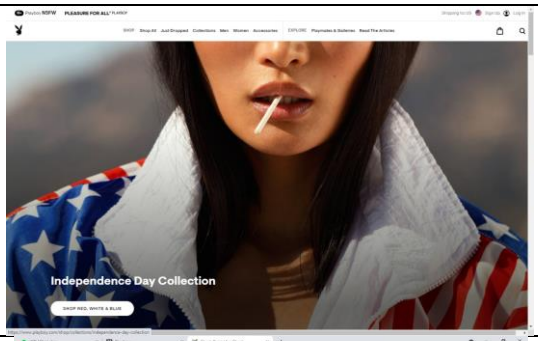
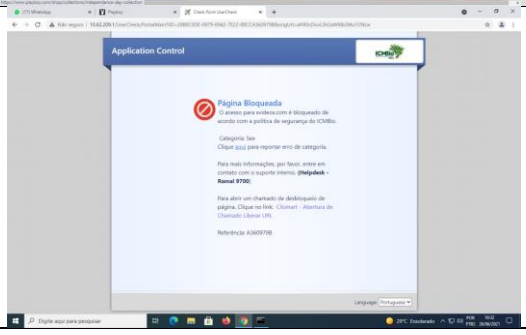
ITEM	DESCRIÇÃO-OBSERVAÇÃO	EVIDÊNCIA
01	1- Conforme coluna de evidência, foi verificado a conexão e autenticação com Check Point.	

5.6 Autenticação Check Point com Filtro de Conteúdo:

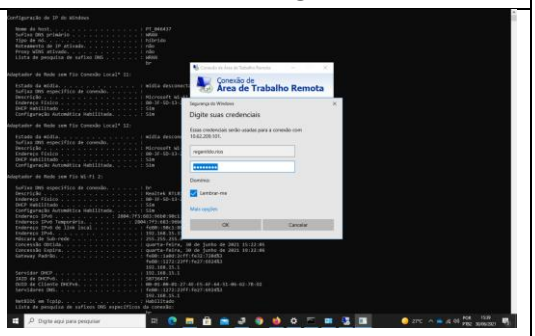
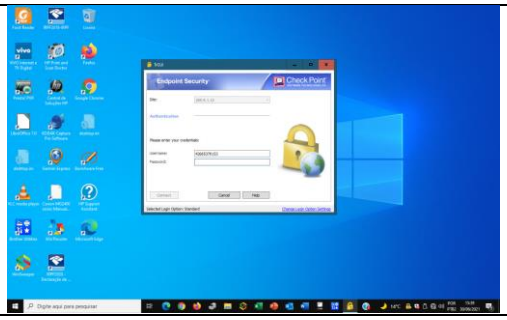
No mesmo dia, conforme testes executados nos item 5.5, foi verificado a ausência do filtro de conteúdo, quando informado aos responsáveis.

<u>Dia 26 de junho de 2021:</u> Testado páginas de conteúdo proibido.

ITEM	DESCRIÇÃO-OBSERVAÇÃO	EVIDÊNCIA
01	1- Para validar o teste de filtro de conteúdo, no dia 25/06/21 a página playboy estava com acesso liberado, no dia seguinte após contato com empresa responsável pelo Check Point, foi acessado o site www.playboy.com.br com resposta imediata de bloqueio de página.	 

5.7 Autenticação Via VPN:

Dia 30 de junho de 2021: Iniciado os testes de acesso remoto via VPN; solicitado a migração das regras e políticas de segurança aplicadas na rede MPLS do RAN Goiânia para a solução Check Point. Após migração, o acesso remoto via VPN com conexão Check Point ocorreu com sucesso.

ITEM	DESCRIÇÃO-OBSERVAÇÃO	EVIDÊNCIA
01	1- Migração para o Check Point das regras e políticas de segurança aplicadas na rede MPLS do RAN Goiânia.	 

6- Dificuldades Encontradas/ Sugestão para melhoria

O IP-WAN (DINÂMICO) do link instalado pela operadora VIVO muda sempre que o modem é inicializado, atribuindo um novo endereço IP aleatoriamente. Quando isso ocorre, é necessário fechar nova conexão por VPN para aplicação das políticas de segurança e configurações (IP-WAN) no firewall Check Point.

Para correção dessa dificuldade, sugere-se a adoção de endereço IP estático (IP fixo) com a operadora do serviço de internet, atribuindo esse IP manualmente ao dispositivo da operadora uma única vez, e configurado para ser usado como bridge

junto às políticas de segurança e configurações da conexão (IP-WAN) do firewall Check Point.

7 - Considerações finais

Após a realização dos testes, foi verificado que o módulo funcionou de acordo com o esperado, possibilitando a replicação das políticas de segurança aplicadas na sede e tornando a Unidade de Conservação independente da sede, quanto ao acesso à internet.

Foi identificado que a configuração de um IP fixo para o modem da operadora garante com que as integrações via VPN funcionem com melhor performance.

CENTRAL IT
Janilson Santos
Gerente de Contratos

Janilson de Sousa Santos
Central IT

Anexo III - Resposta_Checkpoint.pdf

RE: Consulta ao fabricante sobre a participação de outros fabricantes no processo licitatório

Daniel Matos <dmatos@checkpoint.com>

Seg, 30/08/2021 10:31

Para: Felipe Finger Santiago <felipe.santiago@icmbio.gov.br>

Prezado Felipe, bom dia!

Segue abaixo nosso posicionamento quanto essa questao da incompatibilidade de comunicacao e justificativa da vantajosidade:

O ambiente NGTX/NGTP existente no Datacenter do ICMbio hoje composto de cluster 6900 e gerência centralizada versão 80.40 da Checkpoint.

O conceito de se ter uma gerência centralizada é redução dos recursos necessários para administrar o ambiente de segurança, permitindo a criação de regras e aplicação para todos os firewalls de maneira mais rápida e uniforme, reduzindo as falhas, assim como a atualização de software dos firewalls.

Além da redução de recursos uma gerência centralizada gera uma administração mais rápida e precisa da solução de segurança, com a emissão de relatórios centralizados, consolidados troubleshooting e correções, quando necessárias.

A adição deste preâmbulo se faz necessário para dizer que a adição de outro(s) fabricante(s) nesse ambiente para atender os escritórios remotos, se torna inviável, conforme destacaremos abaixo:

Cada fabricante possui a sua gerência exclusiva, dito isso, o uso de mais de um fabricante no ambiente, impossibilita o uso da gerência centralizada, sendo necessário uma plataforma de gerência para cada fabricante na rede.

Dessa forma, as aplicações das regras, por exemplo, teriam que ser feitas manualmente nesses equipamentos remotos ou através de outra(s) gerência(s), tornando o trabalho muito mais oneroso e crítico, isso também se aplica as atualizações dos firewalls.

A administração se torna mais crítica, pois, além das aplicações das regras ou atualizações, em caso de troubleshooting, os dados dos relatórios não seriam mais consolidados e customizados, já que teriam que utilizar várias gerências para obter as informações necessárias para a resolução de problemas, o que muitas vezes torna impossível a visão completa dos dados necessários para a solução de problemas.

Agora falando da implementação da solução, o projeto do ICMbio prevê o Firewall do Datacenter (Core) e gerência centralizada, integrado as unidades remotas através da utilização de firewalls menores, cada unidade remota utilizando dois links de Internet, através de operadoras locais.

Nesse formato, o projeto traz um aumento da segurança da rede e redução de custos, já que utilizará links de internet, em detrimento ao uso dos atuais links MPLS que são utilizados pelo Icmbio, que possuem custo muito elevado.

Cada firewall instalado nas unidades remotas, utilizará um recurso chamado ISP Redundancy responsável por gerenciar até dois links de internet em modo load sharing (onde ambos são utilizados em conjunto) ou modo ativo/backup, onde um link assume quando o outro para de responder (baseado em testes de ICMP para hosts remotos e conectividade da interface). Esta mesma feature possibilita fazer também a redundância de VPN, caso pare de responder um link, a VPN pode ser fechada pelo outro, independente do link padrão de saída da internet.

Sendo assim, não seria possível colocar firewalls de outros fabricantes, já que não teria a possibilidade de implementar o ISP Redundancy nesse equipamento.

Qq duvida estamos a disposicao.

Att,

Daniel Matos
Account Manager – Brazil
Check Point Software Technologies Ltd.
Cell:+55 61 99166-2361

From: Felipe Finger Santiago <felipe.santiago@icmbio.gov.br>
Sent: Monday, August 30, 2021 8:56 AM
To: Daniel Matos <dmatos@checkpoint.com>
Subject: Consulta ao fabricante sobre a participação de outros fabricantes no processo licitatório

Prezado, Daniel!

Solicitamos um posicionamento da fabricante Check Point sobre a possibilidade de outros fornecedores participarem do processo licitatório para a aquisição de novos firewalls para as Unidades Descentralizadas do ICMBio, haja vista que o Instituto possui hoje em sua sede o Firewall cujo modelo é o Check Point R80.40 incluindo todo o licenciamento de aplicação e software de gerenciamento.

- Há alguma incompatibilidade de comunicação de equipamentos de outros fabricantes com o Modelo Check Point R80.40? Se sim, quais funcionalidades ficariam comprometidas?
- Poderia nos relatar os prós e os contras de se fazer uma indicação por marca (Check Point) nesse processo licitatório?

Esse questionamento se deve ao fato de possibilitar a ampla concorrência desse processo licitatório para que um maior número de empresas de diversos fabricantes possam participar.

Atenciosamente,

FELIPE FINGER SANTIAGO
Analista em TI

Instituto Chico Mendes de Conservação da Biodiversidade
Coordenação de Tecnologia da Informação e Comunicação - COTEC
COTEC/CGATI/DIPLAN

Telefone: (61) 2028-9700
E-mail: felipe.santiago@icmbio.gov.br
http://www.icmbio.gov.br

Anexo IV - Proposta Comercial - L8 Group.pdf

Re: Solicitação de Cotação de Preços

Luciano Fernandes <luciano.fernandes@l8group.net>
Seg, 20/09/2021 11:22

Para: COTEC <cotec@icmbio.gov.br>
Cc: Jaime Heleno Correa de Lisboa <jaime.lisboa@icmbio.gov.br>

1 anexos (426 KB)
L8 - Proposta Comercial Firewall Escritórios Remotos - 20.09.2021 - Rev.02.pdf;

Bom dia Felipe
Segue novamente a proposta atualizada, peço que desconsidere as anteriores, pois não possuem validade.

Att

Luciano Fernandes
luciano.fernandes@l8group.net | +55 51 98156 0095
+55 51 4042 1788 | 0800 932 0000 ramal 6888
www.l8group.net

On Thu, 16 Sept 2021 at 16:19, Luciano Fernandes <luciano.fernandes@l8group.net> wrote:

> Felipe
> Segue a proposta atualizada.
>
> Att
>
> **Luciano Fernandes**
> luciano.fernandes@l8group.net | +55 51 98156 0095
> +55 51 4042 1788 | 0800 932 0000 ramal 6888
> www.l8group.net
>
> On Thu, 16 Sept 2021 at 14:37, Luciano Fernandes <luciano.fernandes@l8group.net> wrote:
>
> > Felipe, boa tarde.
> > Segue a proposta comercial
> > Qualquer dúvida estou à disposição.
> >
> > Att
> >
> > **Luciano Fernandes**
> > luciano.fernandes@l8group.net | +55 51 98156 0095
> > +55 51 4042 1788 | 0800 932 0000 ramal 6888
> > www.l8group.net
> >
> > On Thu, 16 Sept 2021 at 13:50, Luciano Fernandes <luciano.fernandes@l8group.net> wrote:
> >
> > > Felipe
> > > Pode desconsiderar o email anterior, agora eu li melhor e entendi, está considerado sim.
> > >
> > > Att
> > >
> > > **Luciano Fernandes**

luciano.fernandes@l8group.net | +55 51 98156 0095
+55 51 4042 1788 | 0800 932 0000 ramal 6888
www.l8group.net

On Thu, 16 Sept 2021 at 13:47, Luciano Fernandes <luciano.fernandes@l8group.net> wrote:

Prezado Felipe, boa tarde.

Na especificação vocês não estão considerando o suporte nível 1 e 2 do integrador, vocês farão a contratação desses serviços, como hoje vocês possuem do core?

Att

Luciano Fernandes
luciano.fernandes@l8group.net | +55 51 98156 0095
+55 51 4042 1788 | 0800 932 0000 ramal 6888
www.l8group.net

On Thu, 9 Sept 2021 at 14:09, COTEC <cotec@icmbio.gov.br> wrote:

Prezado(a) fornecedor(a),

Tendo em vista o estudo de viabilidade de contratação da expansão de solução integradora de Firewall NEXT GENERATION composta de hardware e software de segurança da informação do tipo UTM (Unified Threat Management) para interligar de forma segura, a rede central do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) a suas Unidades Descentralizadas, solicitamos o envio de proposta comercial para o fornecimento dos itens e quantitativos constantes do quadro a seguir:

Cabe ressaltar que o ICMBio possui hoje um cluster 6900 com uma gerência centralizada versão 80.40 da Checkpoint e que será exigido para todos os itens a **garantia de suporte técnico com reposição de peças e componentes pelo período de 60 meses**, garantida a atualização de todos os softwares e licenciamentos necessários.

Todos os itens serão entregues na sede do ICMBio em Brasília.

As especificações mínimas por item, constam elencadas a seguir:

ESPECIFICAÇÕES TÉCNICAS DO LOTE 01

ESPECIFICAÇÕES TÉCNICAS GERAIS PARA O LOTE 01

A solução deverá ser composta de hardware e software licenciado do mesmo fabricante;

Tendo em vista o fato de que o projeto trata-se de expansão de solução de segurança, onde os equipamentos e softwares fornecidos serão gerenciados de forma centralizada, todos os itens deverão ser totalmente compatíveis com o módulo de gerenciamento do ICMBio (Security Management R80) devendo:

possuir recurso automatizado de atualização de políticas por meio de consulta ao módulo de gerência centralizado;

possuir recurso para disponibilização de logs em Log Server Dedicado;

ser compatível com serviço SNMP;

garantir comunicação entre os appliances de segurança e o módulo de gerência através de meio criptografado.

Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 01 - MÓDULO DE SEGURANÇA TIPO 01

Desempenho requerido de Next Generation Firewall: 600 Mbps.

Desempenho requerido de Threat Prevention: 340 Mbps.

Desempenho requerido de VPN: 950 Mbps.

Desempenho requerido de IPS: 650 Mbps.

Deverá suportar 10.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 02 - MÓDULO DE SEGURANÇA TIPO 02

Desempenho requerido de Next Generation Firewall: 800 Mbps.

Desempenho requerido de Threat Prevention: 450 Mbps.

Desempenho requerido de VPN: 1.2 Gbps.

Desempenho requerido de IPS: 850 Mbps.

Deverá suportar 14.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 03 - MÓDULO DE SEGURANÇA TIPO 03

Desempenho requerido de Next Generation Firewall: 950 Mbps.

Desempenho requerido de Threat Prevention: 500 Mbps.

Desempenho requerido de VPN: 1.8 Gbps.

Desempenho requerido de IPS: 1 Gbps.

Deverá suportar 15.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 8 (oito) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 04 - MÓDULO DE SEGURANÇA TIPO 04

Desempenho requerido de Next Generation Firewall: 3.0 Gbps.

Desempenho requerido de Threat Prevention: 1.5 Gbps.

Desempenho requerido de VPN: 3 Gbps.

Desempenho requerido de IPS: 3.2 Gbps.

Deverá suportar 50.000 novas conexões por segundo.

Deverá suportar 2.200.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 16 (dezesseis) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

Deverá possuir 1 (uma) interface dedicada para WAN sendo do tipo RJ45 ou Fibra.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá possuir 1 (uma) interface DSL.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS EXIGIDAS PARA OS ITENS 01, 02, 03 E 04 - (MÓDULOS DE SEGURANÇA)

Funcionalidade de Firewall

A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

O hardware e o software que executam as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

Realizar upgrade via interface WEB;

Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: suporte a, no mínimo, VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, DHCP Relay, DHCP Server;

Deve suportar os seguintes tipos de NAT: Nat dinâmico (Many-to-1), NAT estático (1-to-1), NAT de Origem, NAT de Destino;

Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

A solução deve possuir aplicativo para Smartphones da própria solução para integrar ao dispositivo remoto e criar visibilidade e monitoramento das principais ameaças, conectividade e também receber notificações de ameaças ou qualquer outra falha no gateway de segurança;

Enviar logs para sistemas de monitoramento externos, simultaneamente;

Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos:

transparente;

mode sniffer (monitoramento e análise o tráfego de rede);

camada 2 (L2); e

camada 3 (L3).

A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

Funcionalidade de IPS

Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance.

Para os appliances em plantas sem conexão a Internet deve ser possível realizar a atualização manual importando o pacote de

atualização.

Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta a scanning de portas CIFS, Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS-SQLServer, IKE aggressive Exchange;

Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

Em cada proteção de segurança, deve estar incluso informações como: categoria, tipo de impacto na ferramenta, severidade e tipo de ação que a mesma irá executar;

A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas;

Deve ser possível criar regras de exceção no IPS para que a engine não faça a inspeção de um tráfego específico por proteção, origem, destino, serviço ou porta;

Deve ser possível visualizar a lista de proteções disponíveis no appliance com os detalhes.

Funcionalidade de controle de aplicação Web e URL

A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking;

Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool;

Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por:

Usuário do Active Directory;

IP;

Rede.

Deve ser possível configurar com apenas um clique o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

Deve ser possível limitar o consumo de banda de aplicações.

Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp e etc;

Na própria interface de gerência web deve ser possível realizar a recategorização de uma URL.

A base de aplicações deve ser superior a 4500 aplicações já categorizada na base de administração da solução.

Deve ser possível customizar e também definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

Aceitar e informar;

Bloquear e informar;

Perguntar.

Identificação de Usuários

A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

A solução deve identificar usuários das seguintes fontes:

Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

Autenticação via navegador - para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

Identificação do usuário registrado no Microsoft Active Directory - deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando.

Funcionalidades de Anti-Vírus e Anti-Malware

A solução deve incluir ferramenta própria ou solução de terceiros para mitigar / bloquear a comunicação entre os hosts infectados com bot e operador remoto.

A solução deve bloquear arquivos potencialmente maliciosos infectados com vírus.

A solução de proteção contra vírus e bot devem compartilhar a mesma política para facilitar o gerenciamento.

A solução de proteção contra vírus e bot devem incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas.

As proteções devem ser ativadas baseadas em critério de nível de confiança, ações da proteção e impacto de performance.

Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta.

Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

Deve ser possível criar regras de exceção para que a engine não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

Inspecionar tipos de arquivos conhecidos que contém malware;

Inspecionar todos os tipos de arquivos;

Inspecionar tipos de arquivos de famílias específicas.

Deve bloquear acesso a URLs com malware.

Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado.

Funcionalidades de VPN Site to Site

A solução deve prover acesso seguro criptografado entre dois sites através da Internet.

A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros.

A solução deve suportar autenticação com senha ou certificado.

Deve suportar criptografia AES 128 e 256;

Deve possuir mecanismo para monitorar a saúde do túnel remoto.

Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

A solução deve suportar DPD (Dead Peer Detection) para minimizar a quantidade de mensagens trocadas para verificar a disponibilidade do Peer.

A solução deve suportar CA para configuração das VPNs.

MÓDULO DE GERENCIAMENTO CENTRALIZADO – ITEM 05

A solução de gerenciamento e administração centralizada nas dependências da instituição deve sofrer um upgrade para suportar 200 dispositivos conectados;

O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

Suportar backup das configurações e rollback de configuração para a última configuração salva;

Suportar validação de regras antes da aplicação;

Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;

SERVIÇO DE ARMAZENAMENTO DE LOGS DEDICADO - ITEM 06

Deve ser contemplado nesse projeto solução dedicada para armazenamento de logs de todos os dispositivos conectados na gerência centralizada;

A solução de log server pode ser entregue através de appliance físico do próprio fabricante ou através de software que será instalada no ambiente de virtualização da própria instituição que está contratando os serviços e equipamentos desse edital;

Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;

Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;

Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware) e URLs que passaram pela solução;

Deve ser possível exportar os logs em CSV;

Deve possibilitar a geração de relatórios de eventos no formato PDF;

Possibilitar rotação do log;

Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

Deve permitir a criação de relatórios personalizados;

Suportar enviar os relatórios de forma automática via PDF;

A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

Deve consolidar logs e relatórios de todos os dispositivos administrados;

Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

Permitir que os relatórios possam ser salvos, enviados e impressos;

Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;

Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

Visualizar a quantidade de tráfego utilizado de aplicações e navegação;

Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;

Permitir a visualização de gráficos e mapa de ameaças;

Possuir mecanismo para que logs antigos sejam removidos automaticamente;

Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

Atenciosamente,

FELIPE FINGER SANTIAGO
Analista em TI

Instituto Chico Mendes de Conservação da Biodiversidade
Coordenação de Tecnologia da Informação e Comunicação - COTEC
COTEC/CGATI/DIPLAN

Telefone: (61) 2028-9700
E-mail: felipe.santiago@icmbio.gov.br
http://www.icmbio.gov.br

BUSINESS**PROPOSAL**

Curitiba, 20 de setembro de 2021.

Prezado Sr.

Jaime Heleno Correa de Lisboa

Segue nossa Proposta Comercial para o objeto descrito abaixo.

FATURAMENTO

Razão Social:	L8 GROUP S.A.
Materiais - CNPJ:	19.952.299/0001-02
Serviços - CNPJ:	19.952.299/0002-93
D-U-N-S:	914725411

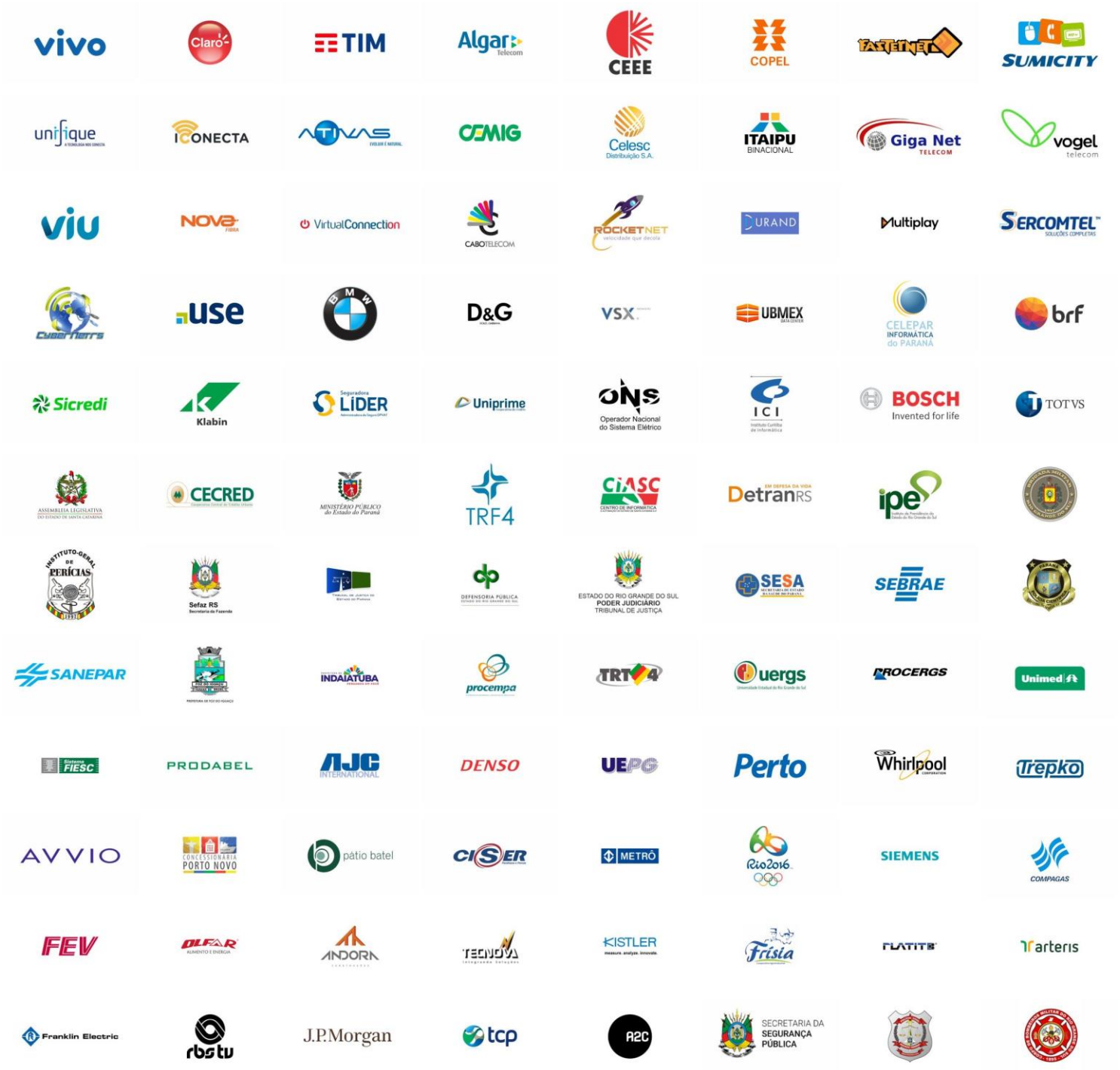
Atenciosamente,

Luciano Fernandes
luciano.fernandes@l8group.net | +55 51 98156-0095
+55 41 3908 8438 | 0800 718 7819
www.l8group.net

Composição da Solução					
Lote	Item	Descrição	Quant	Valor Unit	Valor Total
1	1	Modelo de Segurança Tipo 1 (Compatibilidade de Appliance – redes com até 30 usuários)	40	R$ 14.446,27	R$ 577.850,80
	2	Modelo de Segurança Tipo 2 (Compatibilidade de Appliance – redes com de 30 até 70 usuários)	100	R$ 18.438,38	R$ 1.843.838,00
	3	Modelo de Segurança Tipo 3 (Compatibilidade de Appliance – redes com de 70 até 150 usuários)	50	R$ 25.446,26	R$ 1.272.313,00
	4	Modelo de Segurança Tipo 4 (Compatibilidade de Appliance – redes acima de 70 até 150 usuários)	10	R$ 70.115,04	R$ 701.150,40
	5	Upgrade de Licenciamento Security Manager R80 – Modelo de Gerenciamento de até 200 firewalls	1	R$ 891.237,73	R$ 891.237,73
	6	Log Server R80 – Licenciamento para Implementação de Serviço de Armazenamento de logs dedicados.	1	R$ 137.850,35	R$ 137.850,35

Valor total do Investimento: R$ 5.424.240,28

PRINCIPAIS CLIENTES



ENDEREÇOS

CURITIBA - PR

RUA JOSÉ IZIDORO BIAZETTO ,1210
2º ANDAR | (LAB)
+55 41 2106 6888

SÃO PAULO - SP

AVENIDA BRIGADEIRO FARIA LIMA, 3729
5º ANDAR
+55 11 4933 2768

BRASÍLIA - DF

COMERCIAL SUL QUADRA 09 BLOCO C
TORRE C | 10º ANDAR
+55 61 4042 5088

CURITIBA - PR

RUA PADRE ANCHIETA, 2540
8º ANDAR | (FINANCE)
+55 41 3908 8438

BELO HORIZONTE - MG

AVENIDA DO CONTORNO, 6594
17º ANDAR
+55 31 4042 1568

PORTO ALEGRE - RS

AVENIDA CARLOS GOMES, 700
8º ANDAR
+55 51 4042 1788

SÃO JOSÉ DOS PINHAIS - PR

AV. ROCHA POMBO, 2561 - MÓD 5B
(WAREHOUSE)
+55 41 3134 8226

RIO DE JANEIRO - RJ

AVENIDA RIO BRANCO, 115
19º ANDAR
+55 21 4042 0958

POMPANO BEACH - FL

PARK CENTRAL BLVD SOUTH, 1310
+1 954 951 8025

Anexo V - Proposta Comercial - NTSEC.pdf

Re: Solicitação de Cotação de Preços

Vinicius Oliveira <vinicius@ntsec.com.br>
Qui, 16/09/2021 18:02

Para: COTEC <cotec@icmbio.gov.br>
Cc: Daniel Zapelini <daniel.zapelini@ntsec.com.br>

1 anexos (282 KB)
Proposta Comercial - NTSec - ICMBio.pdf;

Prezados,

segue proposta comercial para o projeto em questão.

Fico a disposição para qualquer esclarecimento.

Obrigado.

Att,

Em qui., 9 de set. de 2021 às 14:14, COTEC <cotec@icmbio.gov.br> escreveu:

> Prezado(a) fornecedor(a),
>
> Tendo em vista o estudo de viabilidade de contratação da expansão de solução integradora de Firewall NEXT GENERATION composta de hardware e software de segurança da informação do tipo UTM (Unified Threat Management) para interligar de forma segura, a rede central do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) a suas Unidades Descentralizadas, solicitamos o envio de proposta comercial para o fornecimento dos itens e quantitativos constantes do quadro a seguir:
>
> Cabe ressaltar que o ICMBio possui hoje um cluster 6900 com uma gerência centralizada versão 80.40 da Checkpoint e que será exigido para todos os itens a **garantia de suporte técnico com reposição de peças e componentes pelo período de 60 meses**, garantida a atualização de todos os softwares e licenciamentos necessários.
> Todos os itens serão entregues na sede do ICMBio em Brasília.
> As especificações mínimas por item, constam elencadas a seguir:

ESPECIFICAÇÕES TÉCNICAS DO LOTE 01

ESPECIFICAÇÕES TÉCNICAS GERAIS PARA O LOTE 01

A solução deverá ser composta de hardware e software licenciado do mesmo fabricante;

Tendo em vista o fato de que o projeto trata-se de expansão de solução de segurança, onde os equipamentos e softwares fornecidos serão gerenciados de forma centralizada, todos os itens deverão ser totalmente compatíveis com o módulo de gerenciamento do ICMBio (Security Management R80) devendo:

possuir recurso automatizado de atualização de políticas por meio de consulta ao módulo de gerência centralizado;

possuir recurso para disponibilização de logs em Log Server Dedicado;

ser compatível com serviço SNMP;

garantir comunicação entre os appliances de segurança e o módulo de gerência através de meio criptografado.

Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 01 - MÓDULO DE SEGURANÇA TIPO 01

Desempenho requerido de Next Generation Firewall: 600 Mbps.

Desempenho requerido de Threat Prevention: 340 Mbps.

Desempenho requerido de VPN: 950 Mbps.

Desempenho requerido de IPS: 650 Mbps.

Deverá suportar 10.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 02 - MÓDULO DE SEGURANÇA TIPO 02

Desempenho requerido de Next Generation Firewall: 800 Mbps.

Desempenho requerido de Threat Prevention: 450 Mbps.

Desempenho requerido de VPN: 1.2 Gbps.

Desempenho requerido de IPS: 850 Mbps.

Deverá suportar 14.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 03 - MÓDULO DE SEGURANÇA TIPO 03

Desempenho requerido de Next Generation Firewall: 950 Mbps.

Desempenho requerido de Threat Prevention: 500 Mbps.

Desempenho requerido de VPN: 1.8 Gbps.

Desempenho requerido de IPS: 1 Gbps.

Deverá suportar 15.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 8 (oito) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 04 - MÓDULO DE SEGURANÇA TIPO 04

Desempenho requerido de Next Generation Firewall: 3.0 Gbps.

Desempenho requerido de Threat Prevention: 1.5 Gbps.

Desempenho requerido de VPN: 3 Gbps.

Desempenho requerido de IPS: 3.2 Gbps.

Deverá suportar 50.000 novas conexões por segundo.

Deverá suportar 2.200.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 16 (dezesseis) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

Deverá possuir 1 (uma) interface dedicada para WAN sendo do tipo RJ45 ou Fibra.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá possuir 1 (uma) interface DSL.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS EXIGIDAS PARA OS ITENS 01, 02, 03 E 04 - (MÓDULOS DE SEGURANÇA)

Funcionalidade de Firewall

A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

O hardware e o software que executam as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

Realizar upgrade via interface WEB;

Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: suporte a, no mínimo, VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, DHCP Relay, DHCP Server;

Deve suportar os seguintes tipos de NAT: Nat dinâmico (Many-to-1), NAT estático (1-to-1), NAT de Origem, NAT de Destino;

Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

A solução deve possuir aplicativo para Smartphones da própria solução para integrar ao dispositivo remoto e criar visibilidade e monitoramento das principais ameaças, conectividade e também receber notificações de ameaças ou qualquer outra falha no gateway de segurança;

Enviar logs para sistemas de monitoramento externos, simultaneamente;

Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos:

transparente;

mode sniffer (monitoramento e análise o tráfego de rede);

camada 2 (L2); e

camada 3 (L3).

A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

Funcionalidade de IPS

Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance.

Para os appliances em plantas sem conexão a Internet deve ser possível realizar a atualização manual importando o pacote de atualização.

Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta a scanning de portas CIFS, Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS-SQLServer, IKE aggressive Exchange;

Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

Em cada proteção de segurança, deve estar incluso informações como: categoria, tipo de impacto na ferramenta, severidade e tipo de ação que a mesma irá executar;

A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas;

Deve ser possível criar regras de exceção no IPS para que a engine não faça a inspeção de um tráfego específico por proteção, origem, destino, serviço ou porta;

Deve ser possível visualizar a lista de proteções disponíveis no appliance com os detalhes.

Funcionalidade de controle de aplicação Web e URL

A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking;

Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool;

Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por:

Usuário do Active Directory;

IP;

Rede.

Deve ser possível configurar com apenas um clique o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

Deve ser possível limitar o consumo de banda de aplicações.

Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp e etc;

Na própria interface de gerência web deve ser possível realizar a recategorização de uma URL.

A base de aplicações deve ser superior a 4500 aplicações já categorizada na base de administração da solução.

Deve ser possível customizar e também definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

Aceitar e informar;

Bloquear e informar;

Perguntar.

Identificação de Usuários

A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

A solução deve identificar usuários das seguintes fontes:

Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

Autenticação via navegador - para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

Identificação do usuário registrado no Microsoft Active Directory - deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando.

Funcionalidades de Anti-Vírus e Anti-Malware

A solução deve incluir ferramenta própria ou solução de terceiros para mitigar / bloquear a comunicação entre os hosts infectados com bot e operador remoto.

A solução deve bloquear arquivos potencialmente maliciosos infectados com vírus.

A solução de proteção contra vírus e bot devem compartilhar a mesma política para facilitar o gerenciamento.

A solução de proteção contra vírus e bot devem incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas.

As proteções devem ser ativadas baseadas em critério de nível de confiança, ações da proteção e impacto de performance.

Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta.

Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

Deve ser possível criar regras de exceção para que a engine não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

Inspecionar tipos de arquivos conhecidos que contém malware;

Inspecionar todos os tipos de arquivos;

Inspecionar tipos de arquivos de famílias específicas.

Deve bloquear acesso a URLs com malware.

Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado.

Funcionalidades de VPN Site to Site

A solução deve prover acesso seguro criptografado entre dois sites através da Internet.

A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros.

A solução deve suportar autenticação com senha ou certificado.

Deve suportar criptografia AES 128 e 256;

Deve possuir mecanismo para monitorar a saúde do túnel remoto.

Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

A solução deve suportar DPD (Dead Peer Detection) para minimizar a quantidade de mensagens trocadas para verificar a disponibilidade do Peer.

A solução deve suportar CA para configuração das VPNs.

MÓDULO DE GERENCIAMENTO CENTRALIZADO – ITEM 05

A solução de gerenciamento e administração centralizada nas dependências da instituição deve sofrer um upgrade para suportar 200 dispositivos conectados;

O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

Suportar backup das configurações e rollback de configuração para a última configuração salva;

Suportar validação de regras antes da aplicação;

Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;

SERVIÇO DE ARMAZENAMENTO DE LOGS DEDICADO - ITEM 06

Deve ser contemplado nesse projeto solução dedicada para armazenamento de logs de todos os dispositivos conectados na gerência centralizada;

A solução de log server pode ser entregue através de appliance físico do próprio fabricante ou através de software que será instalada no ambiente de virtualização da própria instituição que está contratando os serviços e equipamentos desse edital;

Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;

Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;

Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware) e URLs que passaram pela solução;

Deve ser possível exportar os logs em CSV;

Deve possibilitar a geração de relatórios de eventos no formato PDF;

Possibilitar rotação do log;

Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

Deve permitir a criação de relatórios personalizados;

Suportar enviar os relatórios de forma automática via PDF;

A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

Deve consolidar logs e relatórios de todos os dispositivos administrados;

Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

Permitir que os relatórios possam ser salvos, enviados e impressos;

Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;

Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

- Visualizar a quantidade de tráfego utilizado de aplicações e navegação;
- Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;

Permitir a visualização de gráficos e mapa de ameaças;

Possuir mecanismo para que logs antigos sejam removidos automaticamente;

Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

Atenciosamente,

FELIPE FINGER SANTIAGO
Analista em TI

Instituto Chico Mendes de Conservação da Biodiversidade
Coordenação de Tecnologia da Informação e Comunicação - COTEC
COTEC/CGATI/DIPLAN

Telefone: (61) 2028-9700
E-mail: felipe.santiago@icmbio.gov.br
http://www.icmbio.gov.br

PROPOSTA COMERCIAL

ICMBIO

Contratação da expansão de solução integradora de Firewall NEXT GENERATION composta de hardware e software de segurança da informação do tipo UTM (Unified Threat Management) para interligar de forma segura, a rede central do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) a suas Unidades Descentralizadas

+55 61 32483829
licitacao@ntsec.com.br | www.ntsec.com

SCN QD. 05 Torre Norte Sala 617. Ed Brasília Shopping
Asa Norte – Brasília/DF CEP: 70715-900

Brasília-DF, 16 de setembro de 2021.

Ao
ICMBio

Prezados,

É com grande satisfação que encaminhamos **Proposta de Preços Estimativa** na área de Tecnologia da Informação e comunicação - TIC, para atendimento do ICMBio
.

Agradecemos a oportunidade e a confiança depositada na **NTSec | Network Security** e esperamos poder estreitar ainda mais o nosso relacionamento.

Em caso de dúvida ou questionamento, entre em contato conosco. Estamos à disposição para atendê-lo.

Atenciosamente,

Vinicius Oliveira
Gerente Comercial
(61) 3248-3829

+55 61 32483829
licitacao@ntsec.com.br | www.ntsec.com

SCN QD. 05 Torre Norte Sala 617. Ed Brasília Shopping
Asa Norte – Brasília/DF CEP: 70715-900

1. TERMO DE CONFIDENCIALIDADE.

Todas as informações, contidas ou reveladas neste documento, a partir daqui referenciadas apenas como 'Informações confidenciais', são de propriedade da NTSec | Network Security. Estas informações confidenciais são compartilhadas para fins de avaliação da Proposta Comercial para o projeto em questão. A aceitação deste material implica que essas informações confidenciais serão usadas somente com esta finalidade, e que as mesmas serão mantidas em sigilo, não serão reproduzidas, reveladas a terceiros ou usadas, totalmente ou parcialmente, sem permissão expressa e por escrito da NTSec | Network Security.

2. NTSEC | NETWORK SECURITY.

Somos uma empresa de Segurança da Informação reconhecida por proteger com eficácia negócios empresariais há mais de 12 anos. Nos preocupamos com o sigilo das informações de nossos clientes, e proporcionamos as mais adequadas e atuais soluções de segurança do mercado, visando garantir a segurança e o resguardo das informações para que, com a empresa protegida você possa focar no crescimento de seus negócios com tranquilidade.

O rápido desenvolvimento dos meios de comunicação e de novas tecnologias trouxeram muitas possibilidades e grandes desafios para as instituições. Ao passo que, a possibilidade de profissionais desempenharem suas atividades a qualquer hora e em qualquer lugar, resguardar as informações e garantir a segurança dos acessos tornou-se um grande desafio na era da internet.

Levamos em consideração a importância de se ter uma estrutura de informática segura e viável a todos que a utilizam. Portanto, entendemos o funcionamento tecnológico mundial e possibilitamos a nossos clientes a execução de projetos que utilizem padrões de segurança, tendo como resultado, a excelência nos serviços sob os pilares da confidencialidade, integridade e disponibilidade da informação.

+55 61 32483829
licitacao@ntsec.com.br | www.ntsec.com

SCN QD. 05 Torre Norte Sala 617. Ed Brasília Shopping
Asa Norte – Brasília/DF CEP: 70715-900

3. ONDE ESTAMOS.

Matriz:
- Brasília - DF

Filiais:
- Fortaleza - CE
- Cuiabá - MT
- São Paulo - SP

Presença:
- Curitiba - PR
- Florianópolis - SC
- Rio de Janeiro - RJ

4. TRANSPARÊNCIA LEVADA A SÉRIO.

A **NTSEC** é uma empresa certificada no programa de transparência **CERTGOV**, que comprova a nossa intenção de construir, não apenas ambientes seguros de tecnologia, mas também um país melhor! O programa **CERTGOV** comprova a nossa integridade e conformidade com as normativas exigidas para fornecimento aos mercados públicos e privados.

+55 61 32483829
licitacao@ntsec.com.br | www.ntsec.com

SCN QD. 05 Torre Norte Sala 617. Ed Brasília Shopping
Asa Norte – Brasília/DF CEP: 70715-900

5. PROPOSTA DE PREÇOS ESTIMATIVA.

5.1 Objeto da proposta.

Contratação da expansão de solução integradora de Firewall NEXT GENERATION composta de hardware e software de segurança da informação do tipo UTM (Unified Threat Management) para interligar de forma segura, a rede central do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) a suas Unidades Descentralizadas.

5.2 Investimento.

COMPOSIÇÃO DA SOLUÇÃO						
Lote	**Item**	**Descricao**	**UNIDADE**	**Quant.**	**Valor Unit R$**	**Valor Total R$**
1	1	Modelo de Segurança Tipo 1 (Compatibilidade de Appliance – redes com até 30 usuários)	UN.	40	R$ 15.513,31	R$ 620.532,40
	2	Modelo de Segurança Tipo 2 (Compatibilidade de Appliance – redes com de 30 até 70 usuários)	UN.	100	R$ 21.088,11	R$ 2.108.811,00
	3	Modelo de Segurança Tipo 3 (Compatibilidade de Appliance – redes com de 70 até 150 usuários)	UN.	50	R$ 27.423,70	R$ 1.371.185,00
	4	Modelo de Segurança Tipo 4 (Compatibilidade de Appliance – redes acima de 70 até 150 usuários)	UN.	10	R$ 76.493,24	R$ 764.932,40
	5	Upgrade de Licenciamento Security Manager R80 – Modelo de Gerenciamento de até 200 firewalls	UN.	1	R$ 973.155,53	R$ 973.155,53
	6	Log Server R80 – Licenciamento para Implementação de Serviço de Armazenamento de logs dedicados.	UN.	1	R$ 139.144,99	R$ 139.144,99
Total						**R$ 5.977.761,32**

Valor total da proposta: R$ 5.977.761,32 (Cinco milhões, novecentos e setenta e sete mil, setecentos e sessenta e um reais e trinta e dois centavos).

+55 61 32483829
licitacao@ntsec.com.br | www.ntsec.com
SCN QD. 05 Torre Norte Sala 617. Ed Brasília Shopping
Asa Norte – Brasília/DF CEP: 70715-900

Nos valores acima estão compreendidos além do lucro, encargos sociais, taxas e seguros, fretes e quaisquer despesas de responsabilidade do proponente, que direta ou indiretamente, decorram da execução do objeto licitado, na forma e condições previstas no edital e seus anexos.

Declaramos estar de acordo com todas as condições estipuladas no edital e seus anexos.

6. DADOS DA EMPRESA.

Razão Social: NTSEC SOLUÇÕES EM TELEINFORMÁTICA LTDA.			
CNPJ: 09.137.728/0001-34		**Inscrição Estadual:** 07.494.369/001-70	
Endereço: SCN Quadra 05 Bloco A Nº 50 Torre Norte Sala 617 Edifício Brasília Shopping - Asa Norte			
CEP: 70.715-900	**Cidade:** Brasília	**UF:** D.F.	**Telefone:** (61) 3248-3829
Nome do Banco: Banco do Brasil 001		**Agência:** 0452-9	**Conta Corrente:** 500700-3
E-mail: licitacao@ntsec.com.br		**Home Page:** www.ntsec.com.br	

Vinicius Oliveira
Gerente Comercial
(61) 3248-3829

+55 61 32483829
licitacao@ntsec.com.br | www.ntsec.com
SCN QD. 05 Torre Norte Sala 617. Ed Brasília Shopping
Asa Norte – Brasília/DF CEP: 70715-900

Anexo VI - Proposta Comercial - APTUM.pdf

Re: Solicitação de Cotação de Preços

Felipe Nagaishi - Aptum Tecnologia & Outsourcing <felipe@aptum.com.br>
Seg, 27/09/2021 11:31
Para: COTEC <cotec@icmbio.gov.br>

1 anexos (665 KB)
PR_ICMBIOcp___V3.pdf;

Segue proposta com data atualizada!

Respeitosamente,

APTUM
Felipe Nagaishi
DIVISÃO DE OPERAÇÕES
+55 (65) 99942-9955
+55 (65) 2127-7922
Av. Hist. Rubens de Mendonça, 1836
Ed. Work Center | Sala 906
Bosque da Saúde | 78.050-000
Cuiabá - MT
Central de Serviços 24x7
+55 0800 002 7886
aptum.com.br

De: COTEC <cotec@icmbio.gov.br>
Data: quinta-feira, 9 de setembro de 2021 13:13
Para: Felipe Nagaishi - Aptum Tecnologia & Outsourcing <felipe@aptum.com.br>
Assunto: Solicitação de Cotação de Preços

Prezado(a) fornecedor(a),

Tendo em vista o estudo de viabilidade de contratação da expansão de solução integradora de Firewall NEXT GENERATION composta de hardware e software de segurança da informação do tipo UTM (Unified Threat Management) para interligar de forma segura, a rede central do Instituto Chico Mendes de Conservação da Biodiversidade (ICMBio) a suas Unidades Descentralizadas, solicitamos o envio de proposta comercial para o fornecimento dos itens e quantitativos constantes do quadro a seguir:

COMPOSIÇÃO DA SOLUÇÃO				
LOTE	**ITEM**	**DESCRIÇÃO**	**UNIDADE**	**QUANT.**
01	01	Módulo de segurança tipo 01 (compatibilidade do Appliance - redes com até 30 usuários)	UN.	40
	02	Módulo de segurança tipo 02 (compatibilidade do Appliance - redes de 30 até 70 usuários)	UN.	100
	03	Módulo de segurança tipo 03 (compatibilidade do Appliance - redes de 70 até 150 usuários)	UN.	50
	04	Módulo de segurança tipo 04 (compatibilidade do Appliance - redes acima de 150 usuários)	UN.	10
	05	Upgrade de Licenciamento Security Management R80 - Módulo de gerenciamento de até 200 firewalls	UN.	1
	06	Log Server Dedicado R80 - Licenciamento para implementação de serviço de armazenamento de logs dedicado	UN.	1

Cabe ressaltar que o ICMBio possui hoje um cluster 6900 com uma gerência centralizada versão 80.40 da Checkpoint e que será exigido para todos os itens a **garantia de suporte técnico com reposição de peças e componentes pelo período de 60 meses**, garantida a atualização de todos os softwares e licenciamentos necessários.

Todos os itens serão entregues na sede do ICMBio em Brasília.

As especificações mínimas por item, constam elencadas a seguir:

ESPECIFICAÇÕES TÉCNICAS DO LOTE 01

ESPECIFICAÇÕES TÉCNICAS GERAIS PARA O LOTE 01

A solução deverá ser composta de hardware e software licenciado do mesmo fabricante;

Tendo em vista o fato de que o projeto trata-se de expansão de solução de segurança, onde os equipamentos e softwares fornecidos serão gerenciados de forma centralizada, todos os itens deverão ser totalmente compatíveis com o módulo de gerenciamento do ICMBio (Security Management R80) devendo:

possuir recurso automatizado de atualização de políticas por meio de consulta ao módulo de gerência centralizado;

possuir recurso para disponibilização de logs em Log Server Dedicado;

ser compatível com serviço SNMP;

garantir comunicação entre os appliances de segurança e o módulo de gerência através de meio criptografado.

Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 01 - MÓDULO DE SEGURANÇA TIPO 01

Desempenho requerido de Next Generation Firewall: 600 Mbps.

Desempenho requerido de Threat Prevention: 340 Mbps.

Desempenho requerido de VPN: 950 Mbps.

Desempenho requerido de IPS: 650 Mbps.

Deverá suportar 10.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 02 - MÓDULO DE SEGURANÇA TIPO 02

Desempenho requerido de Next Generation Firewall: 800 Mbps.

Desempenho requerido de Threat Prevention: 450 Mbps.

Desempenho requerido de VPN: 1.2 Gbps.

Desempenho requerido de IPS: 850 Mbps.

Deverá suportar 14.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 5 (cinco) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 03 - MÓDULO DE SEGURANÇA TIPO 03

Desempenho requerido de Next Generation Firewall: 950 Mbps.

Desempenho requerido de Threat Prevention: 500 Mbps.

Desempenho requerido de VPN: 1.8 Gbps.

Desempenho requerido de IPS: 1 Gbps.

Deverá suportar 15.000 novas conexões por segundo.

Deverá suportar 500.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 8 (oito) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS ESPECÍFICAS DO ITEM 04 - MÓDULO DE SEGURANÇA TIPO 04

Desempenho requerido de Next Generation Firewall: 3.0 Gbps.

Desempenho requerido de Threat Prevention: 1.5 Gbps.

Desempenho requerido de VPN: 3 Gbps.

Desempenho requerido de IPS: 3.2 Gbps.

Deverá suportar 50.000 novas conexões por segundo.

Deverá suportar 2.200.000 conexões simultâneas.

Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

Deverá suportar Policy-based routing.

Deverá possuir pelo menos 16 (dezesseis) interfaces 10/100/1000Base-T RJ-45.

Deverá possuir 1 (uma) interface dedicada para DMZ sendo do tipo RJ45 ou Fibra.

Deverá possuir 1 (uma) interface dedicada para WAN sendo do tipo RJ45 ou Fibra.

Deverá possuir 1 (uma) interface USB.

Deverá possuir 1 (uma) interface console serial do tipo RJ-45 e micro USB.

Deverá possuir 1 (uma) interface DSL.

Deverá suportar modem 3G/4G.

Deverá disponibilizar serviço de alertas configuráveis de acordo com as políticas de segurança implementadas.

ESPECIFICAÇÕES TÉCNICAS MÍNIMAS EXIGIDAS PARA OS ITENS 01, 02, 03 E 04 - (MÓDULOS DE SEGURANÇA)

Funcionalidade de Firewall

A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

O hardware e o software que executam as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

Realizar upgrade via interface WEB;

Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades: suporte a, no mínimo, VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, DHCP Relay, DHCP Server;

Deve suportar os seguintes tipos de NAT: Nat dinâmico (Many-to-1), NAT estático (1-to-1), NAT de Origem, NAT de Destino;

Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

A solução deve possuir aplicativo para Smartphones da própria solução para integrar ao dispositivo remoto e criar visibilidade e monitoramento das principais ameaças, conectividade e também receber notificações de ameaças ou qualquer outra falha no gateway de segurança;

Enviar logs para sistemas de monitoramento externos, simultaneamente;

Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos:

transparente;

mode sniffer (monitoramento e análise o tráfego de rede);

camada 2 (L2); e

camada 3 (L3).

A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

Funcionalidade de IPS

Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance.

Para os appliances em plantas sem conexão a Internet deve ser possível realizar a atualização manual importando o pacote de atualização.

Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta a scanning de portas CIFS, Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS-SQLServer, IKE aggressive Exchange;

Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

Em cada proteção de segurança, deve estar incluso informações como: categoria, tipo de impacto na ferramenta, severidade e tipo de ação que a mesma irá executar;

A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas;

Deve ser possível criar regras de exceção no IPS para que a engine não faça a inspeção de um tráfego específico por proteção, origem, destino, serviço ou porta;

Deve ser possível visualizar a lista de proteções disponíveis no appliance com os detalhes.

Funcionalidade de controle de aplicação Web e URL

A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking;

Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool;

Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por:

Usuário do Active Directory;

IP;

Rede.

Deve ser possível configurar com apenas um clique o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

Deve ser possível limitar o consumo de banda de aplicações.

Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp e etc;

Na própria interface de gerência web deve ser possível realizar a recategorização de uma URL.

A base de aplicações deve ser superior a 4500 aplicações já categorizada na base de administração da solução.

Deve ser possível customizar e também definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

Aceitar e informar;

Bloquear e informar;

Perguntar.

Identificação de Usuários

A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

A solução deve identificar usuários das seguintes fontes:

Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

Autenticação via navegador - para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

Identificação do usuário registrado no Microsoft Active Directory - deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando.

Funcionalidades de Anti-Vírus e Anti-Malware

A solução deve incluir ferramenta própria ou solução de terceiros para mitigar / bloquear a comunicação entre os hosts infectados com bot e operador remoto.

A solução deve bloquear arquivos potencialmente maliciosos infectados com vírus.

A solução de proteção contra vírus e bot devem compartilhar a mesma política para facilitar o gerenciamento.

A solução de proteção contra vírus e bot devem incluir um modo de solução de problemas, que define o uso de perfil de detectar, apenas com um clique, sem modificar as proteções individuais já criadas e customizadas.

As proteções devem ser ativadas baseadas em critério de nível de confiança, ações da proteção e impacto de performance.

Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta.

Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

Deve ser possível criar regras de exceção para que a engine não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

Inspecionar tipos de arquivos conhecidos que contém malware;

Inspecionar todos os tipos de arquivos;

Inspecionar tipos de arquivos de famílias específicas.

Deve bloquear acesso a URLs com malware.

Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado.

Funcionalidades de VPN Site to Site

A solução deve prover acesso seguro criptografado entre dois sites através da Internet.

A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros.

A solução deve suportar autenticação com senha ou certificado.

Deve suportar criptografia AES 128 e 256;

Deve possuir mecanismo para monitorar a saúde do túnel remoto.

Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.

A solução deve suportar DPD (Dead Peer Detection) para minimizar a quantidade de mensagens trocadas para verificar a disponibilidade do Peer.

A solução deve suportar CA para configuração das VPNs.

MÓDULO DE GERENCIAMENTO CENTRALIZADO – ITEM 05

A solução de gerenciamento e administração centralizada nas dependências da instituição deve sofrer um upgrade para suportar 200 dispositivos conectados;

O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

Suportar backup das configurações e rollback de configuração para a última configuração salva;

Suportar validação de regras antes da aplicação;

Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory e Radius;

SERVIÇO DE ARMAZENAMENTO DE LOGS DEDICADO - ITEM 06

Deve ser contemplado nesse projeto solução dedicada para armazenamento de logs de todos os dispositivos conectados na gerência centralizada;

A solução de log server pode ser entregue através de appliance físico do próprio fabricante ou através de software que será instalada no ambiente de virtualização da própria instituição que está contratando os serviços e equipamentos desse edital;

Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a sua maior capacidade suportada ou ilimitada;

Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores.

Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;

Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware) e URLs que passaram pela solução;

Deve ser possível exportar os logs em CSV;

Deve possibilitar a geração de relatórios de eventos no formato PDF;

Possibilitar rotação do log;

Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

Deve permitir a criação de relatórios personalizados;

Suportar enviar os relatórios de forma automática via PDF;

A solução de gerenciamento deverá ser entregue como appliance virtual e deve ser compatível/homologado para VMware ESXi versão 5 e superior.

Deve consolidar logs e relatórios de todos os dispositivos administrados;

Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

Permitir que os relatórios possam ser salvos, enviados e impressos;

Deve incluir uma ferramenta do próprio fabricante ou de outro, desde que não seja software livre, ou em composição com terceiros, para correlacionar os eventos de segurança das funcionalidades adquiridas de todos os equipamentos e softwares ofertados;

Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

- Visualizar a quantidade de tráfego utilizado de aplicações e navegação;
- Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

Permitir o download de assinaturas, atualizações e firmwares para distribuição centralizada aos dispositivos de segurança integrados a mesma;

Permitir a visualização de gráficos e mapa de ameaças;

Possuir mecanismo para que logs antigos sejam removidos automaticamente;

Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências.

Atenciosamente,

FELIPE FINGER SANTIAGO

Analista em TI

Instituto Chico Mendes de Conservação da Biodiversidade

Coordenação de Tecnologia da Informação e Comunicação - COTEC

COTEC/CGATI/DIPLAN

Telefone: (61) 2028-9700

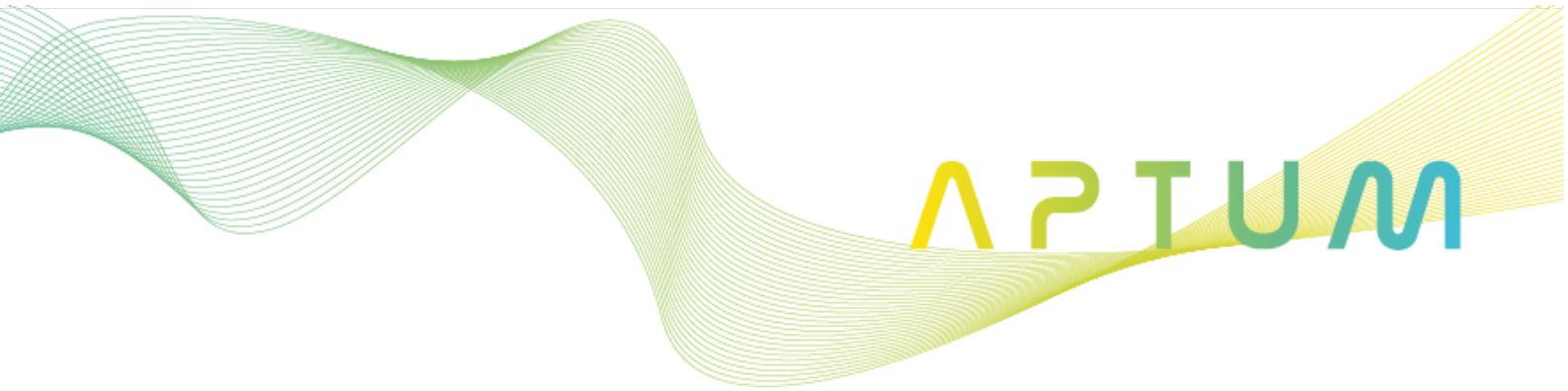
E-mail: felipe.santiago@icmbio.gov.br

http://www.icmbio.gov.br

PROPOSTA TÉCNICA E COMERCIAL

CYBER SECURITY

AQUISIÇÃO SUBSCRIÇÃO DE SERVIÇO DE SUPORTE E ATUALIZAÇÕES DA SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO (CHECK POINT®) PARA O INSTITUTO CHICO MENDES DE CONSERVAÇÃO DA BIODIVERSIDADE - ICMBIO



1. Sobre a Empresa

A **APTUM** foi fundada em 2014 por engenheiros especializados em Service Providers e desde então, a Aptum vem agregando valores aos seus clientes levando inovação tecnológica, conhecimento e suporte às operações.

Especialista em Tecnologia e no mercado de TI, a Aptum possui um amplo catálogo de serviços com soluções que abrangem desde o planejamento, execução, manutenção e monitoramento.

Oferecemos aos nossos clientes muito mais do que soluções tecnológicas: entregamos inteligência e qualidade, comprovados em projetos de alta complexidade para empresas líderes em seus segmentos.

IDENTIFICAÇÃO DO PROPONENTE

Razão Social: IMPERIAL COMÉRCIO E SERVIÇOS TECNOLÓGICOS LTDA.	
CNPJ: 18.858.496/0001-02	I. E.: 13528446-5
Optante pelo SIMPLES? Sim ( ) Não (x)	
Endereço: AV. Historiador Rubens de Mendonça n° 1836, Ed. Work Center, sala 303.	
Bairro: Jardim Aclimação	Cidade: Cuiabá
CEP: 78.050-280	E-mail: licitacoes@aptum.com.br
Telefone: (65) 2127-7922	Fax 2:(65) 9 98165-0093
Banco da licitante: Sicredi (748)	Conta Bancária da licitante: 40318-1
N. da Agência: 0810	
Representante: Fernando Jacó de Souza	
E-mail: licitacoes@aptum.com.br; Fernando.jaco@aptum.com.br;comercial@aptum.com.br	

+55 0800 00 APTUM
Av. Hist. Rubens de Mendonça, 1836
Ed. Work Center | Sala 905
Bosque da Saúde | 78.050-000
Cuiabá - MT

Nossos Parceiros de Produtos:

2. Objeto da Proposta

Fornecimento de produtos Cyber Segurança da fabricante líder CHECKPOINT com fornecimento de Mão de obra qualificada e certificada pelo fabricante por um período de **60 meses** de acordo com termo de referência do ICMBIO.

+55 0800 00 APTUM
Av. Hist. Rubens de Mendonça, 1836
Ed. Work Center | Sala 905
Bosque da Saúde | 78.050-000
Cuiabá - MT

3. Descritivo Técnico

Lote	Item	Descricao	UNIDADE	Quant.	Valor Unit R$	Valor Total R$
1	1	Modelo de Segurança Tipo 1 (Compatibilidade de Appliance – redes com até 30 usuários)	UN.	40	R$ 16.488,88	R$ 659.555,20
	2	Modelo de Segurança Tipo 2 (Compatibilidade de Appliance – redes com de 30 até 70 usuários)	UN.	100	R$ 22.602,66	R$ 2.260.266,00
	3	Modelo de Segurança Tipo 3 (Compatibilidade de Appliance – redes com de 70 até 150 usuários)	UN.	50	R$ 28.913,67	R$ 1.445.683,50
	4	Modelo de Segurança Tipo 4 (Compatibilidade de Appliance – redes acima de 70 até 150 usuários)	UN.	10	R$ 80.345,65	R$ 803.456,50
	5	Upgrade de Licenciamento Security Manager R80 – Modelo de Gerenciamento de até 200 firewalls	UN.	1	R$ 1.032.486,65	R$ 1.032.486,65
	6	Log Server R80 – Licenciamento para Implementação de Serviço de Armazenamento de logs dedicados.	UN.	1	R$ 147.990,40	R$ 147.990,40
						R$ 6.349.438,25

4. Pagamento

a) Moeda corrente
Real

b) Prazo de entrega
60 dias

c) Validade da Proposta
90 dias

d) Forma de Pagamento
À vista.

e) Garantia e atualizações
36 meses.

5. Declarações

Declaramos que nos valores da proposta estão incluídas todas as despesas com tributos, encargos fiscais, sociais, trabalhistas, previdenciários, comerciais e, ainda, acondicionamento dos

+55 0800 00 APTUM
Av. Hist. Rubens de Mendonça, 1836
Ed. Work Center | Sala 905
Bosque da Saúde | 78.050-000
Cuiabá - MT

equipamentos, encargos previdenciários, trabalhistas, Frete, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens/serviços.

Declaramos ainda que todos os problemas técnicos terão solução tipo "NBD"

Atenciosamente,

Felipe Nagaishi de Oliveira **Divisão Operações** **Aptum Tecnologia**	

Termo de Aceite de Proposta:
segunda-feira, 27 de setembro de 2021

_____
Cliente

+55 0800 00 APTUM
Av. Hist. Rubens de Mendonça, 1836
Ed. Work Center | Sala 905
Bosque da Saúde | 78.050-000
Cuiabá - MT

Anexo VII - Pesquisa de Preço NOBREAK 1.5kva senoidal RESUMIDA.pdf

Painel de Preços | MINISTÉRIO DA ECONOMIA

MÉDIA	MEDIANA	MENOR
R$ 1.094,58	**R$ 884,50**	**R$ 564**

FILTROS APLICADOS

Descrição Complementar	Ano da Compra	Modalidade da Compra
12 of 499384	**2021, 2020**	**Pregão**

Quantidade total de registros: 14

Registros apresentados: 1 a 14

Identificação da Compra	Número do Item	Modalidade	Código do CATMAT	Descrição do Item	Descrição Complementar	Unidade de Fornecimento	Quantidade Ofertada	Valor Unitário	Fornecedor	Órgão	UASG	Data da Compra
00043/2020	00013	Pregão	64653	ACUMULADOR TENSÃO		UNIDADE	280	R$564	HS COMERCIO, LOCACAO E MANUTENCAO DE EQUIPAMENTOS DE INFORMATICA LTDA	COMANDO DA MARINHA	788820 - CENTRO DE INTENDENCIA DA MARINHA EM MANAUS	26/01/2021
00043/2020	00014	Pregão	64653	ACUMULADOR TENSÃO		UNIDADE	93	R$564	HS COMERCIO, LOCACAO E MANUTENCAO DE EQUIPAMENTOS DE INFORMATICA LTDA	COMANDO DA MARINHA	788820 - CENTRO DE INTENDENCIA DA MARINHA EM MANAUS	26/01/2021
00012/2021	00002	Pregão	361658	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	18	R$647,84	A C S DE OLIVEIRA MATERIAL DE INFORMATICA E PAPELARIA EIRELI	COMANDO DO EXERCITO	160242 - BASE ADMINISTRATIVA DO COMPLEXO DE SAÚDE RJ	19/07/2021
00008/2020	00008	Pregão	361658	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	2	R$668,25	EGC COMERCIO E ATACADISTA DE INFORMATICA E ELETROELETRONICOS EIRELI	ESTADO DE SAO PAULO	927856 - SERVICO AUTONOMO MUNICIPAL DE SAUDE IBITINGA	08/12/2020
00054/2020	00023	Pregão	361658	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	20	R$799	IDEAL INFORMATICA EIRELI	COMANDO DO EXERCITO	160026 - COMANDO DA 22ª BRIGADA DE INFANTARIA DE SELVA	14/07/2021

00010/2020	00003	Pregão	41629	ESTABILIZADOR TENSÃO		UNIDADE	3	R$837,9966	SISTEMICA SOLUCOES CORPORATIVAS EIRELI	UNIVERSIDADE FEDERAL DE ALAGOAS	153037 - UNIVERSIDADE FEDERAL DE ALAGOAS	19/11/2020
00004/2019	00003	Pregão	357692	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	539	R$869,99	ARIANE MENDES ROCHA 06147679546	DEPARTAMENTO DE POLICIA FEDERAL	200352 - SUPERINTENDENCIA REGIONAL NO ESTADO DO ES	30/12/2020
00003/2021	00008	Pregão	64653	ACUMULADOR TENSÃO		UNIDADE	15	R$899	VIA NOVITA LTDA	ESTADO DO PARANA	987989 - PREFEITURA MUNICIPAL DE VERA CRUZ DO OESTE	08/03/2021
00022/2020	00001	Pregão	361658	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	40	R$930	INFOPLEM INFORMATICA LTDA	MINISTERIO DA EDUCACAO	152005 - MEC-INES-INST.NAC.DE EDUCACAO DE SURDOS/RJ	18/12/2020
00022/2020	00002	Pregão	41629	ESTABILIZADOR TENSÃO		UNIDADE	10	R$1056	ITEC INFORMATICA E TECNOLOGIA LTDA	FUNDACAO FACULDADE FED.CIENCIAS MEDICAS POA	154032 - UNIVERSIDADE FED. DE CIENCIAS DA SAUDE/RS	10/12/2020
00009/2020	00019	Pregão	325954	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	40	R$1200	CR ENERGIA E INFORMATICA EIRELI	COMANDO DO EXERCITO	160545 - HOSPITAL DA G. S. GABRIEL DA CACHOEIRA	10/02/2021
00037/2020	00010	Pregão	361658	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	10	R$1465	HS COMERCIO, LOCACAO E MANUTENCAO DE EQUIPAMENTOS DE INFORMATICA LTDA	COMANDO DA AERONAUTICA	120641 - BASE AÉREA DE PORTOVELHO	11/12/2020
00004/2019	00002	Pregão	325954	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	131	R$1573	ITEC INFORMATICA E TECNOLOGIA LTDA	DEPARTAMENTO DE POLICIA FEDERAL	200352 - SUPERINTENDENCIA REGIONAL NO ESTADO DO ES	30/12/2020
00003/2021	00013	Pregão	361658	FONTE ALIMENTAÇÃO ININTERRUPTA		UNIDADE	1	R$3250	GUARD SISTEMAS DE SEGURANCA LTDA	ESTADO DE GOIAS	989265 - PREFEITURA M.DE BELA VISTA DE GOIÁS	28/06/2021

Anexo VIII - Pesquisa de Preço NOBREAK 1.5kva senoidal COMPLETA.pdf

MÉDIA	MEDIANA	MENOR
R$ 1.094,58	**R$ 884,50**	**R$ 564**

Quantidade total de registros: 14
Registros apresentados: 1 a 14

FILTROS APLICADOS

Descrição Complementar	Ano da Compra	Modalidade da Compra
12 of 499384	**2021, 2020**	**Pregão**

RESULTADO 1

DADOS DA COMPRA

Identificação da Compra: 00043/2020
Número do Item: 00013
Objeto da Compra: Pregão Eletrônico - Aquisição de material e equipamentos de informática para o comando do 9¨ Distrito Naval e suas Organizações Militares subordinadas
Quantidade Ofertada: 280
Valor Proposto Unitário: R$ 714,84
Valor Unitário do Item: R$ 564
Código do CATMAT: 64653
Descrição do Item: ACUMULADOR TENSÃO, SISTEMA NO - BREAK ACIMA 3 KVA
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: TS SHARA
Data do Resultado: 26/01/2021

DADOS DO FORNECEDOR

Nome do Fornecedor: HS COMERCIO, LOCACAO E MANUTENCAO DE EQUIPAMENTOS DE INFORMATICA LTDA
CNPJ/CPF: 24802687000147
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 788820 - CENTRO DE INTENDENCIA DA MARINHA EM MANAUS
Órgão: COMANDO DA MARINHA
Órgão Superior: MINISTERIO DEFESA

RESULTADO 2

DADOS DA COMPRA

Identificação da Compra: 00043/2020
Número do Item: 00014
Objeto da Compra: Pregão Eletrônico - Aquisição de material e equipamentos de informática para o comando do 9¨ Distrito Naval e suas Organizações Militares subordinadas
Quantidade Ofertada: 93
Valor Proposto Unitário: R$ 714,84
Valor Unitário do Item: R$ 564
Código do CATMAT: 64653
Descrição do Item: ACUMULADOR TENSÃO, SISTEMA NO - BREAK ACIMA 3 KVA
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: TS SHARA
Data do Resultado: 26/01/2021

DADOS DO FORNECEDOR

Nome do Fornecedor: HS COMERCIO, LOCACAO E MANUTENCAO DE EQUIPAMENTOS DE INFORMATICA LTDA
CNPJ/CPF: 24802687000147
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 788820 - CENTRO DE INTENDENCIA DA MARINHA EM MANAUS
Órgão: COMANDO DA MARINHA
Órgão Superior: MINISTERIO DEFESA

RESULTADO 3

DADOS DA COMPRA

Identificação da Compra: 00012/2021
Número do Item: 00002
Objeto da Compra: Pregão Eletrônico - Material Permanente de Informática para atender a demanda da Base Adm Cmpl Sau RJ.
Quantidade Ofertada: 18
Valor Proposto Unitário: R$ 647,84
Valor Unitário do Item: R$ 647,84
Código do CATMAT: 361658
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, TIPO:ON LINE INTERATIVO / MICROPROCESSADOR RISC/FLASH /, TENSÃO ENTRADA:TRIVOLT AUTOMÁTICO 115/127/220 V, TENSÃO SAÍDA:115 V, CARACTERÍSTICAS ADICIONAIS:CARREGA BATERIAS COM CHAVES DESLIGADAS; DC-START, TIPO ONDA:SENOIDAL MODIFICADA, SOFTWARE:"CHECK" DE PARTIDA AUTO DIAGNOTICA FUNÇÕES NOBREAK, BATERIA:"SWITCH CHARGER" RECARREGADOR CHAVEADO, VARIAÇÃO ENTRADA:115V (80 A 145) 220V (175 A 255), CAPACIDADE NOMINAL:1,4 KVA, COMPONENTES:DISPLAY DIGITAL INTELIGENTE;CONECTOR TIPO ENGATE R
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: TS SHARA
Data do Resultado: 19/07/2021

DADOS DO FORNECEDOR

Nome do Fornecedor: A C S DE OLIVEIRA MATERIAL DE INFORMATICA E PAPELARIA EIRELI
CNPJ/CPF: 31884913000141
Porte do Fornecedor: Micro Empresa

DADOS DO ÓRGÃO

Número da UASG: 160242 - BASE ADMINISTRATIVA DO COMPLEXO DE SAÚDE RJ
Órgão: COMANDO DO EXERCITO
Órgão Superior: MINISTERIO DEFESA

RESULTADO 4

DADOS DA COMPRA

Identificação da Compra: 00008/2020
Número do Item: 00008
Objeto da Compra: Pregão Eletrônico - Aquisição de equipamentos e material permanente para o Centro de Atenção Psicossocial, conforme especificações contidas no Anexo I do Edital.
Quantidade Ofertada: 2
Valor Proposto Unitário: R$ 714,0643
Valor Unitário do Item: R$ 668,25
Código do CATMAT: 361658
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, TIPO:ON LINE INTERATIVO / MICROPROCESSADOR RISC/FLASH /, TENSÃO ENTRADA:TRIVOLT AUTOMÁTICO 115/127/220 V, TENSÃO SAÍDA:115 V, CARACTERÍSTICAS ADICIONAIS:CARREGA BATERIAS COM CHAVES DESLIGADAS; DC-START, TIPO ONDA:SENOIDAL MODIFICADA, SOFTWARE:"CHECK" DE PARTIDA AUTO DIAGNOTICA FUNÇÕES NOBREAK, BATERIA:"SWITCH CHARGER" RECARREGADOR CHAVEADO, VARIAÇÃO ENTRADA:115V (80 A 145) 220V (175 A 255), CAPACIDADE NOMINAL:1,4 KVA, COMPONENTES:DISPLAY DIGITAL INTELIGENTE;CONECTOR TIPO ENGATE R
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISPP
Marca: RAGTECH
Data do Resultado: 08/12/2020

DADOS DO FORNECEDOR

Nome do Fornecedor: EGC COMERCIO E ATACADISTA DE INFORMATICA E ELETROELETRONICOS EIRELI
CNPJ/CPF: 31768037000198
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 927856 - SERVICO AUTONOMO MUNICIPAL DE SAUDE IBITINGA
Órgão: ESTADO DE SAO PAULO
Órgão Superior: REPUBLICA FEDERATIVA DO BRASIL

RESULTADO 5

DADOS DA COMPRA

Identificação da Compra: 00054/2020
Número do Item: 00023
Objeto da Compra: Pregão Eletrônico - Aquisição de material e suprimentos de informática.
Quantidade Ofertada: 20
Valor Proposto Unitário: R$ 995
Valor Unitário do Item: R$ 799
Código do CATMAT: 361658
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, TIPO:ON LINE INTERATIVO / MICROPROCESSADOR RISC/FLASH /, TENSÃO ENTRADA:TRIVOLT AUTOMÁTICO 115/127/220 V, TENSÃO SAÍDA:115 V, CARACTERÍSTICAS ADICIONAIS:CARREGA BATERIAS COM CHAVES DESLIGADAS; DC-START, TIPO ONDA:SENOIDAL MODIFICADA, SOFTWARE:"CHECK" DE PARTIDA AUTO DIAGNOTICA FUNÇÕES NOBREAK, BATERIA:"SWITCH CHARGER" RECARREGADOR CHAVEADO, VARIAÇÃO ENTRADA:115V (80 A 145) 220V (175 A 255), CAPACIDADE NOMINAL:1,4 KVA, COMPONENTES:DISPLAY DIGITAL INTELIGENTE;CONECTOR TIPO ENGATE R
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: SMS
Data do Resultado: 14/07/2021

DADOS DO FORNECEDOR

Nome do Fornecedor: IDEAL INFORMATICA EIRELI
CNPJ/CPF: 23811891000161
Porte do Fornecedor: Micro Empresa

DADOS DO ÓRGÃO

Número da UASG: 160026 - COMANDO DA 22ª BRIGADA DE INFANTARIA DE SELVA
Órgão: COMANDO DO EXERCITO
Órgão Superior: MINISTERIO DEFESA

RESULTADO 6

DADOS DA COMPRA

Identificação da Compra: 00010/2020
Número do Item: 00003
Objeto da Compra: Pregão Eletrônico - Aquisição de materiais e equipamentos para o Laboratório de Microbiologia, Imunologia e Parasitologia para o curso de medicina do Campus Arapiraca.
Quantidade Ofertada: 3
Valor Proposto Unitário: R$ 1.065,54
Valor Unitário do Item: R$ 837,9966
Código do CATMAT: 41629
Descrição do Item: ESTABILIZADOR TENSÃO, ESTABILIZADOR - TENSAO
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISPP
Marca: KVA
Data do Resultado: 19/11/2020

DADOS DO FORNECEDOR

Nome do Fornecedor: SISTEMICA SOLUCOES CORPORATIVAS EIRELI
CNPJ/CPF: 24284710000159
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 153037 - UNIVERSIDADE FEDERAL DE ALAGOAS
Órgão: UNIVERSIDADE FEDERAL DE ALAGOAS
Órgão Superior: MINISTERIO DA EDUCACAO

RESULTADO 7

DADOS DA COMPRA

Identificação da Compra: 00004/2019
Número do Item: 00003
Objeto da Compra: Pregão Eletrônico - Aquisição de bens e materiais de informática para atender as necessidades da SR/PF/ES e demais órgãos participantes, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.
Quantidade Ofertada: 539
Valor Proposto Unitário: R$ 925,81
Valor Unitário do Item: R$ 869,99
Código do CATMAT: 357692
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, TIPO:MICROPROCESSADO, TENSÃO ENTRADA:BIVOLT AUTOMÁTICO 115 - 127/220 V, TIPO ESTABILIZADOR INTERNO:4 ESTÁGIOS REGULAÇÃO, TIPO ALARME:AUDIOVISUAL INTERMITENTE, CARACTERÍSTICAS ADICIONAIS:CHAVE LIGA/DESLIGA TEMPORIZADA, FUNÇÃO MUTE DO ALA, FREQUÊNCIA:60 HZ, TIPO ONDA:SENOIDAL PURA, BATERIA:12V/7AH, VARIAÇÃO ENTRADA:115V(86 A 138) E 220V(170 A 260) PER, APLICAÇÃO:SETOR DE INFORMÁTICA, CAPACIDADE NOMINAL:1,4 KVA
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: RAGTECH
Data do Resultado: 30/12/2020

DADOS DO FORNECEDOR

Nome do Fornecedor: ARIANE MENDES ROCHA 06147679546
CNPJ/CPF: 32924197000141
Porte do Fornecedor: Micro Empresa

DADOS DO ÓRGÃO

Número da UASG: 200352 - SUPERINTENDENCIA REGIONAL NO ESTADO DO ES
Órgão: DEPARTAMENTO DE POLICIA FEDERAL
Órgão Superior: MINISTERIO DA JUSTICA

RESULTADO 8

DADOS DA COMPRA

Identificação da Compra: 00003/2021
Número do Item: 00008
Objeto da Compra: Pregão Eletrônico - Aquisição de equipamentos de informática e materiais de processamento de dados para atender todas as secretarias do Município de Vera Cruz do Oeste.
Quantidade Ofertada: 15
Valor Proposto Unitário: R$ 1.253
Valor Unitário do Item: R$ 899
Código do CATMAT: 64653
Descrição do Item: ACUMULADOR TENSÃO, SISTEMA NO - BREAK ACIMA 3 KVA
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: APC
Data do Resultado: 08/03/2021

DADOS DO FORNECEDOR

Nome do Fornecedor: VIA NOVITA LTDA
CNPJ/CPF: 04447180000105
Porte do Fornecedor: Micro Empresa

DADOS DO ÓRGÃO

Número da UASG: 987989 - PREFEITURA MUNICIPAL DE VERA CRUZ DO OESTE
Órgão: ESTADO DO PARANA
Órgão Superior: REPUBLICA FEDERATIVA DO BRASIL

RESULTADO 9

DADOS DA COMPRA

Identificação da Compra: 00022/2020
Número do Item: 00001
Objeto da Compra: Pregão Eletrônico - Aquisição de bens comuns de informática (material permanente) visando atender a demanda na área de TI (Tecnologia da Informação), que serão utilizados nos diversos setores da instituição, conforme condições, quantidades e exigências estabelecidas em Edital e seus anexos.
Quantidade Ofertada: 40
Valor Proposto Unitário: R$ 1.013
Valor Unitário do Item: R$ 930
Código do CATMAT: 361658
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, TIPO:ON LINE INTERATIVO / MICROPROCESSADOR RISC/FLASH /, TENSÃO ENTRADA:TRIVOLT AUTOMÁTICO 115/127/220 V, TENSÃO SAÍDA:115 V, CARACTERÍSTICAS ADICIONAIS:CARREGA BATERIAS COM CHAVES DESLIGADAS; DC-START, TIPO ONDA:SENOIDAL MODIFICADA, SOFTWARE:"CHECK" DE PARTIDA AUTO DIAGNOTICA FUNÇÕES NOBREAK, BATERIA:"SWITCH CHARGER" RECARREGADOR CHAVEADO, VARIAÇÃO ENTRADA:115V (80 A 145) 220V (175 A 255), CAPACIDADE NOMINAL:1,4 KVA, COMPONENTES:DISPLAY DIGITAL INTELIGENTE;CONECTOR TIPO ENGATE R
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISPP
Marca: SMS
Data do Resultado: 18/12/2020

DADOS DO FORNECEDOR

Nome do Fornecedor: INFOPLEM INFORMATICA LTDA
CNPJ/CPF: 07042421000124
Porte do Fornecedor: Micro Empresa

DADOS DO ÓRGÃO

Número da UASG: 152005 - MEC-INES-INST.NAC.DE EDUCACAO DE SURDOS/RJ
Órgão: MINISTERIO DA EDUCACAO
Órgão Superior: MINISTERIO DA EDUCACAO

RESULTADO 10

DADOS DA COMPRA

Identificação da Compra: 00022/2020
Número do Item: 00002
Objeto da Compra: Pregão Eletrônico - Aquisição de materiais permanentes e equipamentos diversos, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.
Quantidade Ofertada: 10
Valor Proposto Unitário: R$ 2.000
Valor Unitário do Item: R$ 1056
Código do CATMAT: 41629
Descrição do Item: ESTABILIZADOR TENSÃO, ESTABILIZADOR - TENSAO
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISPP
Marca: TS SHARA
Data do Resultado: 10/12/2020

DADOS DO FORNECEDOR

Nome do Fornecedor: ITEC INFORMATICA E TECNOLOGIA LTDA
CNPJ/CPF: 13531571000102
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 154032 - UNIVERSIDADE FED. DE CIENCIAS DA SAUDE/RS
Órgão: FUNDACAO FACULDADE FED.CIENCIAS MEDICAS POA
Órgão Superior: MINISTERIO DA EDUCACAO

RESULTADO 11

DADOS DA COMPRA

Identificação da Compra: 00009/2020
Número do Item: 00019
Objeto da Compra: Pregão Eletrônico - Eventual Aquisição de Material de Informática e Comunicação em Proveito deste Hospital de Guarnição e Unidades Gestoras participantes.
Quantidade Ofertada: 40
Valor Proposto Unitário: R$ 1.605
Valor Unitário do Item: R$ 1200
Código do CATMAT: 325954
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, CAPACIDADE:2 KVA, TIPO:ON-LINE, TENSÃO ENTRADA:110/127 V, TIPO ALARME:LED INDICADOR FORNECIMENTO DE ENERGIA PELA REDE EL, CARACTERÍSTICAS ADICIONAIS:6 TOMADAS DE SAÍDA NEMA 5-15R; POTÊNCIA NOMINAL DE, FREQUÊNCIA:60 HZ, TIPO ONDA:SENOIDAL, SOFTWARE:COMPATÍVEL C/SISTEMAS DE GERENCIAMENTO DE ENERGIA, BATERIA:SELADA E COM RECARGA AUTOMÁTICA, FATOR POTÊNCIA:0,7
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: KVA
Data do Resultado: 10/02/2021

DADOS DO FORNECEDOR

Nome do Fornecedor: CR ENERGIA E INFORMATICA EIRELI
CNPJ/CPF: 25329167000121
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 160545 - HOSPITAL DA G. S. GABRIEL DA CACHOEIRA
Órgão: COMANDO DO EXERCITO
Órgão Superior: MINISTERIO DEFESA

RESULTADO 12

DADOS DA COMPRA

Identificação da Compra: 00037/2020
Número do Item: 00010
Objeto da Compra: Pregão Eletrônico - Aquisição de material de informática.
Quantidade Ofertada: 10
Valor Proposto Unitário: R$ 2.470,96
Valor Unitário do Item: R$ 1465
Código do CATMAT: 361658
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, TIPO:ON LINE INTERATIVO / MICROPROCESSADOR RISC/FLASH /, TENSÃO ENTRADA:TRIVOLT AUTOMÁTICO 115/127/220 V, TENSÃO SAÍDA:115 V, CARACTERÍSTICAS ADICIONAIS:CARREGA BATERIAS COM CHAVES DESLIGADAS; DC-START, TIPO ONDA:SENOIDAL MODIFICADA, SOFTWARE:"CHECK" DE PARTIDA AUTO DIAGNOTICA FUNÇÕES NOBREAK, BATERIA:"SWITCH CHARGER" RECARREGADOR CHAVEADO, VARIAÇÃO ENTRADA:115V (80 A 145) 220V (175 A 255), CAPACIDADE NOMINAL:1,4 KVA, COMPONENTES:DISPLAY DIGITAL INTELIGENTE;CONECTOR TIPO ENGATE R
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: D-LINK
Data do Resultado: 11/12/2020

DADOS DO FORNECEDOR

Nome do Fornecedor: HS COMERCIO, LOCACAO E MANUTENCAO DE EQUIPAMENTOS DE INFORMATICA LTDA
CNPJ/CPF: 24802687000147
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 120641 - BASE AÉREA DE PORTOVELHO
Órgão: COMANDO DA AERONAUTICA
Órgão Superior: MINISTERIO DEFESA

RESULTADO 13

DADOS DA COMPRA

Identificação da Compra: 00004/2019
Número do Item: 00002
Objeto da Compra: Pregão Eletrônico - Aquisição de bens e materiais de informática para atender as necessidades da SR/PF/ES e demais órgãos participantes, conforme condições, quantidades e exigências estabelecidas no Edital e seus anexos.
Quantidade Ofertada: 131
Valor Proposto Unitário: R$ 3.000
Valor Unitário do Item: R$ 1573
Código do CATMAT: 325954
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, CAPACIDADE:2 KVA, TIPO:ON-LINE, TENSÃO ENTRADA:110/127 V, TIPO ALARME:LED INDICADOR FORNECIMENTO DE ENERGIA PELA REDE EL, CARACTERÍSTICAS ADICIONAIS:6 TOMADAS DE SAÍDA NEMA 5-15R; POTÊNCIA NOMINAL DE, FREQUÊNCIA:60 HZ, TIPO ONDA:SENOIDAL, SOFTWARE:COMPATÍVEL C/SISTEMAS DE GERENCIAMENTO DE ENERGIA, BATERIA:SELADA E COM RECARGA AUTOMÁTICA, FATOR POTÊNCIA:0,7
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISRP
Marca: TS SHARA
Data do Resultado: 30/12/2020

DADOS DO FORNECEDOR

Nome do Fornecedor: ITEC INFORMATICA E TECNOLOGIA LTDA
CNPJ/CPF: 13531571000102
Porte do Fornecedor: Pequena Empresa

DADOS DO ÓRGÃO

Número da UASG: 200352 - SUPERINTENDENCIA REGIONAL NO ESTADO DO ES
Órgão: DEPARTAMENTO DE POLICIA FEDERAL
Órgão Superior: MINISTERIO DA JUSTICA

RESULTADO 14

DADOS DA COMPRA

Identificação da Compra: 00003/2021
Número do Item: 00013
Objeto da Compra: Pregão Eletrônico - Contratação de empresa especializada no fornecimento de equipamentos, instalação, configuração, manutenção e suporte técnico para implantar o Sistema de Vídeo Monitoramento Urbano de Vias Públicas no Município de Bela Vista de Goiás.
Quantidade Ofertada: 1
Valor Proposto Unitário: R$ 3.333,33
Valor Unitário do Item: R$ 3250
Código do CATMAT: 361658
Descrição do Item: FONTE ALIMENTAÇÃO ININTERRUPTA, TIPO:ON LINE INTERATIVO / MICROPROCESSADOR RISC/FLASH /, TENSÃO ENTRADA:TRIVOLT AUTOMÁTICO 115/127/220 V, TENSÃO SAÍDA:115 V, CARACTERÍSTICAS ADICIONAIS:CARREGA BATERIAS COM CHAVES DESLIGADAS; DC-START, TIPO ONDA:SENOIDAL MODIFICADA, SOFTWARE:"CHECK" DE PARTIDA AUTO DIAGNOTICA FUNÇÕES NOBREAK, BATERIA:"SWITCH CHARGER" RECARREGADOR CHAVEADO, VARIAÇÃO ENTRADA:115V (80 A 145) 220V (175 A 255), CAPACIDADE NOMINAL:1,4 KVA, COMPONENTES:DISPLAY DIGITAL INTELIGENTE;CONECTOR TIPO ENGATE R
Descrição Complementar:
Unidade de Fornecimento: UNIDADE
Modalidade da Compra: Pregão
Forma de Compra: SISPP
Marca: SMS
Data do Resultado: 28/06/2021

DADOS DO FORNECEDOR

Nome do Fornecedor: GUARD SISTEMAS DE SEGURANCA LTDA
CNPJ/CPF: 08683960000105
Porte do Fornecedor: Micro Empresa

DADOS DO ÓRGÃO

Número da UASG: 989265 - PREFEITURA M.DE BELA VISTA DE GOIÁS
Órgão: ESTADO DE GOIAS
Órgão Superior: REPUBLICA FEDERATIVA DO BRASIL