disponibilizados on-line, sempre que solicitado pela RFB, com os dados dos últimos 6 meses:

Relatórios de Disponibilidade: devem apresentar informações diária, semanal e mensal. Devem conter a análise de tendência quanto ao desempenho e à utilização dos recursos da rede.

Relatórios de Tráfego: relatórios diários que apresentam o tráfego de todos os circuitos, com suas séries históricas, fornecendo subsídios para analisar o desempenho e as tendências de aproveitamento dos recursos da rede. Estes relatórios devem estratificar a utilização dos circuitos de comunicação por tipo de tráfego (IP, portas, protocolos, classes de serviço) apresentando informações de banda utilizada e do volume de tráfego.

Relatório de Prazos: relatório mensal com listagem de todas as demandas abertas, as pendentes e as concluídas relativas à instalação, mudança de endereço, alteração de largura de banda de circuitos, com informações da data de abertura de cada demanda e dias gastos para conclusão do serviço.

Relatório de Acompanhamento dos Chamados: relatório diário com todas as informações relativas ao chamado como data, hora, identificação do elemento (circuito ou equipamento), descrição detalhada do chamado.

Relatórios de Chamados: relatório mensal de chamados abertos e encerrados.

Relatório de Acompanhamento de ANS: relatório mensal analítico de ANS, contendo para cada circuito/circuito as ocorrências de falhas, caso tenham existido e os valores mensais apurados para cada indicador referenciado no item Acordo de Níveis de Serviço;

Relatório de Tendências: relatório que tem como finalidade indicar os recursos de rede que estão saturados e/ou com indicação de problemas, apontando necessidade de expansão da rede.

Requisitos para Mudanças

A RFB poderá solicitar ao SERPRO, durante a vigência do Contrato, a inclusão, exclusão e alteração de endereços de Circuitos de comunicação e o aumento ou redução da largura de banda para o tráfego que atende aos Circuitos de comunicação, em função das necessidades administrativas e técnicas.

A inclusão de novos Circuitos de comunicação, bem como a alteração de endereço de Circuitos de comunicação existentes na Rede RFB se dará mediante solicitação formal da RFB ao SERPRO.

Para a inclusão e alteração de endereço a RFB deverá informar ao SERPRO o endereço completo (com CEP) onde será instalado o circuito, o nome e telefone do responsável para contato na localidade ou da Unidade jurisdicionante e código da UA.

Nos casos de alteração de endereço, o SERPRO deverá manter disponível o tráfego no Circuito de comunicação antigo até que o novo Circuito de comunicação seja ativado, de forma a não haver interrupção do serviço.

A exclusão de Circuito de comunicação se dará mediante solicitação formal da RFB ao SERPRO, informando a Unidade, o endereço e a data a partir da qual o serviço de conexão poderá ser desativado, cabendo ao SERPRO executar a desativação do circuito de comunicação e a retirada dos equipamentos relativos ao serviço de rede WAN, bem como a "baixa" do circuito de comunicação nos sistemas de gerenciamento e controle.

O aumento (upgrade) ou redução (downgrade) de largura de banda dos circuitos serão solicitados pela RFB após avaliação técnica da necessidade.

O SERPRO poderá propor o aumento ou redução de largura de banda dos circuitos, em decorrência de suas ações de gerenciamento proativo e avaliação técnica que justifique a proposição.

Para os casos de aumento de largura de banda devem ser esgotadas as possibilidades de redução do tráfego pelo uso de novas soluções ou de ações corretivas no ambiente de rede LAN ou de rede WAN, sempre considerando o custo/benefício das ações e soluções.

A RFB deverá disponibilizar a infraestrutura adequada e necessária para a implantação de novo Circuito de comunicação ou aumento da largura de banda de Circuito de comunicação existente, previamente à formulação da demanda ao SERPRO, garantindo, no mínimo:

a) rede elétrica estabilizada e aterramento de acordo com as normas ABNT e internas da RFB; e
b) disponibilização de rede interna, que consta de duto e cabo entre o distribuidor geral de telefonia (DGT) e o local de instalação dos equipamentos de comunicação (modem e roteador), bem como eventuais adaptações nas instalações físicas.

Em locais que exigem implementações distintas das elencadas no item anterior, o SERPRO deve comunicar por escrito à RFB para que tome as providências necessárias, antecipadamente à inclusão de novos pontos ou aumento de largura de banda da interconexão do Circuito de comunicação.

O custo de revisita pelas operadoras/concessionárias executantes da ativação dos circuitos, motivados por falta ou descumprimento técnico das condições de infraestrutura elétrica e lógica necessárias, serão repassados à RFB.

Os prazos para atendimento pelo SERPRO de inclusão e mudança de endereço dos Circuitos de comunicação e de aumento ou redução de largura de banda são os apresentados na tabela a seguir:

Tabela 1 – Prazo de atendimento

Circuito de comunicação	**Região**					
		Norte		**Nordeste**		**Sul, Sudeste e Centro-oeste**
		Interurbano	**Urbano**	**Interurbano**	**Urbano**	**Interurbano** / **Urbano**
Instalação		75 dias	60 dias	70 dias	55 dias	65 dias / 60 dias
Alteração de velocidade		75 dias	60 dias	70 dias	55 dias	65 dias / 60 dias
Mudança de endereço		75 dias	60 dias	70 dias	55 dias	65 dias / 60 dias

Os prazos acima estabelecidos serão válidos para as solicitações que estejam adequadas as faixas de velocidades estabelecidas na tabela abaixo. Tais faixas de velocidade poderão ser ampliadas em comum acordo com a RFB e o SERPRO.

Tabela 2 – Faixas de velocidades por Unidade Federativa

Link	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**	**UF**
512K	U	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
	I	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR

1M	U	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
	I	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
2M	U	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
	I	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
4M	U	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
	I	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
6M	U	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
	I	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
8M	U	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
	I	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
10M	U	SC	TO	AM	MT	PA	RO	DF	ES	MA	RJ	PI	MS	RR
	I	SC						DF	ES	MA	RJ			RR
20M	U	SC						DF	ES	MA	RJ			RR
	I	SC						DF	ES	MA	RJ			RR
30M	U	SC						DF	ES	MA	RJ			RR
	I	SC						DF	ES	MA	RJ			RR
50M	U	SC						DF	ES	MA	RJ			RR
	I	SC						DF	ES	MA	RJ			RR
70M	U	SC						DF	ES	MA	RJ			RR
	I	SC						DF	ES	MA	RJ			RR
100M	U	SC				PA		DF	ES	MA	RJ			RR
	I	SC						DF	ES	MA	RJ			RR

Link	UF	UF	UF	UF	UF	UF	UF	UF	UF	UF	UF	UF	UF	UF	UF
512K	U	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
	I	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
1M	U	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
	I	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
2M	U	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
	I	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
4M	U	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE

6M	I	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
	U	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
8M	I	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
	U	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
10M	I	CE	RS	GO	MG	PE	PR	SP	AC	AL	AP	BA	PB	RN	SE
	U	CE	RS	GO	MG	PE	PR	SP							
20M	I	CE	RS	GO	MG	PE	PR	SP							
	U	CE	RS	GO	MG	PE	PR	SP							
30M	I	CE	RS	GO	MG	PE	PR	SP				BA			
	U	CE	RS	GO	MG	PE	PR	SP							
50M	I	CE	RS	GO	MG	PE	PR	SP							
	U	CE	RS	GO	MG	PE	PR	SP							
70M	I	CE	RS	GO	MG	PE	PR	SP							
	U	CE	RS	GO	MG	PE	PR	SP							
100M	I	CE	RS	GO	MG	PE	PR	SP				BA			

Para velocidade que não consta na tabela de faixas de velocidades, o SERPRO deverá providenciar a instalação de uma combinação de circuitos com balanceamento de tráfego que resulte na velocidade demandada para suprir temporariamente a Unidade no prazo constante da tabela 1. No prazo máximo de 150 dias, o SERPRO deverá instalar um circuito único com a velocidade demandada. Caso a instalação não seja atendida em 150 dias, a RFB passará a pagar pela combinação de circuitos o valor do circuito único da velocidade demandada.

5.2 Características do Serviço de Segurança da Informação

O serviço de Segurança da Informação compreende os seguintes itens:

a) Sistema de firewall;

b) Tratamento de incidentes;

c) Gerenciamento e administração de política de filtro de conteúdo;

d) Análise de vulnerabilidades;

e) Testes de invasão;

f) Análise forense; e

g) Análise de conformidade.

Sistema de Firewall

Compreende a utilização de sistema de firewall com alta disponibilidade para tratamento da

segurança do tráfego de saída/entrada proveniente da Intranet e VPNs para acesso à Internet e desta para as Zonas Desmilitarizadas (ZDMs) da RFB. Compreende, ainda, a implementação de ZDMs compartilhadas para produção de serviço de publicação Internet.

Este item de serviço tem como requisito os seguintes componentes:

a) Sistema de firewall dedicado com alta disponibilidade e alto nível de capacidade/performance.

b) Sistema de gerência de firewall.

c) Console de gerenciamento de firewall.

d) Servidor de consolidação de logs.

e) Armazenamento em disco para dados de auditoria.

f) Analisador de protocolo (SNIFERs) para coleta e rastreamento de tráfego.

g) Administração contemplando criação de regras de NAT e PAT, criação e atualização de regras e políticas de segurança, monitoração dos acessos e filtros em conformidade com as necessidades de segurança para o ambiente computacional corporativo e compartilhado.

Resultados Esperados

Preservar os aspectos de Disponibilidade, Integridade por meio de filtragem de tráfego e a confidencialidade (para os casos onde se aplicam o uso de criptografia e VPNs criptografadas por sistemas de firewall) para o ambiente dos serviços/sistemas da RFB na internet e intranet.

Tratamento de incidentes (ambiente dedicado)

Compreende as atividades de detecção e bloqueio de tentativas de ataques e incidentes de segurança computacional no ambiente de rede ou VPN e nas zonas desmilitarizadas da RFB, abrangendo o ambiente dos serviços/sistemas da RFB na internet e intranet, realizado pelo GRA (Grupo de Resposta a Ataques) do SERPRO.

Fica o SERPRO autorizado a implementar medidas de controle e bloqueio de acessos, aos serviços WEB da RFB, dos endereços IP's caracterizados como origem de tentativas de ataque, acessos robotizados e abusivos. O modelo de definição dos paramentros e gestão dos bloqueios e controles efetuados, será descrito no documento: MODELO DE GESTÃO DE CONTROLE CONTRA ATAQUES E ACESSOS ROBOTIZADOS E ABUSIVOS À SERVIÇOS WEB RFB, editado pela RFB e SERPRO, conforme política de segurança vigente.

Este item de serviço tem como requisito os seguintes componentes:

a) Sensores de detecção de intrusão dedicado ao segmento de rede da RFB (IDS) ou Sensores de prevenção de intrusão dedicado ao segmento de rede da RFB (IPS);

b) Console de eventos de incidentes de segurança;

c) Servidor de Bancos de dados de coleta de eventos;

d) Servidor de consolidação de logs;

e) Servidor de e-mails para mensagens automáticas de IPS e IDS;

f) Armazenamento em disco para dados de auditoria deverá ser previsto para um

período de 03 (três) anos, podendo a RFB solicitar armazenamento de dados específicos por período superior;

g) Sistema customizável para emissão de relatórios e indicadores de tratamento de incidentes específico para os serviços da RFB;

h) Analisador de protocolo (SNIFFERs) para coleta e rastreamento de tráfego; e

i) Serviço de monitoração de alertas de segurança sobre os segmentos de rede e publicação contemplando a mitigação e aplicação de estratégias de resposta a Incidentes de Segurança Computacional visando o bloqueio e eliminação de tentativas de exploração de vulnerabilidades e padrões de ataque sobre o ambiente computacional.

Resultados Esperados

Realizar o Tratamento de incidentes adequado em todas as tentativas e incidentes detectados para o ambiente dos serviços/sistemas da RFB na internet e intranet;

Gerenciamento e administração de política de filtro de conteúdo.

Compreende as atividades de definição de uma política de tratamento e filtragem de conteúdo WEB, junto com a RFB e segundo suas necessidades. Após as definições de categorias, serão implementados controles de cache e Filtro de conteúdo no modelo centralizado e as categorias de acesso WEB definidas previamente, de forma a implementar a política de filtragem de todas as páginas WEB Internet acessadas pelos usuários da Intranet ou VPN da RFB.

Este item de serviço tem como requisito os seguintes componentes:

a) Servidores de Cache de acesso WEB Internet.

b) Servidores de Antivírus para tráfego de acesso WEB (HTTP).

c) Servidor de Bancos de dados de URLS classificadas atualizadas diariamente por assinatura de serviço de filtragem de conteúdo.

d) Balanceadores de tráfego para servidores de cache e filtro.

e) Console de monitoração de eventos de cache e filtro de conteúdo.

f) Banco de dados de URLS mais acessadas por cliente.

g) Bloqueio de todas as categorias de filtragem de conteúdo solicitadas pela RFB, segundo sua política de segurança, incluindo anti-spam para serviço de e-mail;

h) Informações a serem disponibilizadas, para a RFB quando solicitadas por esta, sobre os endereços mais acessados no mês, endereços (URLs) mais bloqueados no mês, usuários (endereços IP) mais bloqueados no mês.

Análise de vulnerabilidade

Compreende as atividades realizadas pelo GRA visando identificar vulnerabilidade em servidores, serviços e aplicações consideradas críticas, cuja exploração poderia comprometer a segurança da informação nos aspectos de confidencialidade, integridade e disponibilidade.

Este item de serviço tem como requisito os seguintes componentes:

a) Ferramentas de mapeamento de portas e protocolos TCP/IP definidos nos serviços

alvo (ex. nmap, fport, entre outras).

b) Ferramentas de varredura e detecção de vulnerabilidade: (ex. Nessus, Nikito, Internet scanner (ISS), entre outras).

Testes de invasão

Compreende a realização de testes remotos, por meio de programas e ferramentas de exploração de vulnerabilidades em servidores, serviços, aplicações e redes, visando à identificação de formas de acesso indevido que permitam a perpetração do ambiente computacional da RFB, possibilitando o comprometimento da segurança da informação nos aspectos de confidencialidade, disponibilidade e integridade.

Este item de serviço tem como requisito a utilização dos seguintes componentes:

a) Ferramentas de mapeamento de portas e protocolos TCP/IP definidos nos serviços alvo (ex. nmap, fport, entre outras).

b) Ferramentas de varredura e detecção de vulnerabilidade: (ex. Nessus, Nikito, Internet scanner (ISS), entre outras).

c) Ferramentas de varredura wireless (wardriving) por meio de ferramentas de mapeamento e scanner de vulnerabilidade, visando obter informações das redes, serviços e aplicações acessíveis através de Circuitoss wireless (AP- Access Point).

d) Aplicações de testes de engenharia social, visando obter privilégios de acesso físico e lógico ao ambientes computacionais.

e) Ferramentas de invasão e exploração de vulnerabilidades.

Análise de artefato, análise forense

A análise de artefato compreende a aplicação de técnica forense computacional, visando identificar o comportamento malicioso de artefato, para gerar controles e minimizar impactos no ambiente computacional.

A analise forense compreende a aplicação de técnica forense computacional, visando a identificação e extração de evidências que permitam a formulação de conclusões para determinar a causa de um incidente.

Este item de serviço tem como requisito a utilização dos seguintes componentes:

a) Ferramentas disponíveis no laboratório de análise forense.

b) Servidor de armazenamento de cópias forense.

c) Discos e demais componentes para cópias de segurança.

Análise de conformidade

Análise de segurança para identificar possíveis pontos de falhas e aspectos de não-conformidade com as normas e procedimentos estabelecidos.

Este item de serviço tem como requisito a utilização dos seguintes componentes:

a) Política, norma ou procedimento de segurança a ser analisado.

b) Equipe preparada e listas de procedimentos de análise elaborados.

c) Realização de visitas técnicas.

Relatórios Técnicos

Os relatórios deste anexo, técnicos ou gerenciais, serão entregues em prazo acordado, após solicitação formal da RFB.

Relatório do Sistema de Firewall

a) Relatório contendo dados do firewall, como nome, dados diários de consumo de CPU e memória, hora do consumo máximo de uso (pico), tempo que estava UP, tempo que ficou fora (DOWN); e

b) Relatório contendo dados do firewall referentes a endereços IPs, versão de software e regras, apresentadas em meio digital, baseado em critérios/condições previamente definidas.

Relatório de Tratamento de Incidentes

a) Relatório contendo dados sobre as tentativas de ataques e incidentes de segurança computacional detectados e bloqueados no ambiente de rede ou VPN e nas zonas desmilitarizadas da RFB, abrangendo o ambiente dos seus serviços/sistemas na internet e intranet, realizado pelo GRA (Grupo de Resposta a Ataques) do CONTRATADO;

b) Em caso de ataque ou incidente de segurança que obtiver êxito, além do relatório que que deve ser produzido conforme item anterior, devem ser gerados 3 (três) relatórios, dispostos da seguinte forma:

1) Relatório de Abertura de Incidente: deve ser entregue em até 48 horas após detecção do incidente de segurança, com informações preliminares e levantamento emergencial sobre o ataque, tipo de ataque, aplicação/serviço, sistema operacional e máquina atacada, data e hora da detecção do ataque e primeiras medidas tomadas para sanar o problema e recolocação do serviço ao estado normal de utilização, se possível. A partir do relato, o GRA deverá realizar a Análise forense do incidente conforme o subitem "*Análise de artefato, análise forense*" do item 6.1, a partir da anuência/autorização do cliente;

2) Relatório de Acompanhamento de Incidente: deverá ser entregue em até 5 (cinco) dias úteis após a entrega do relatório do item anterior, até o fechamento do incidente, com informações mais detalhadas sobre: o ataque, seu tipo; descrição, pormenorizada, das ações realizadas para corrigir os problemas encontrados a fim de evitar-se recorrência do problema;

3) Relatório de Fechamento de Incidente: deverá ser entregue em até 5 (cinco) dias úteis após a entrega do relatório do item anterior com informações detalhadas sobre as correções realizadas e medidas tomadas para evitar-se a recorrência do problema.

Relatório de Gerenciamento e administração de política de filtro de conteúdo

a) Relatório contendo dados do Filtro de Conteúdo, como nome, dados diários do consumo de CPU e memória, hora do consumo máximo de uso (pico), tempo que estava UP, tempo que ficou fora (DOWN), versão de software.

b) Relatório contendo dados do firewall referentes às regras aplicadas e levantamento por usuário, apresentadas em meio digital, para os sistemas de cache/filtro de

conteúdo, baseado em critérios/condições previamente definidas.

Relatório de Análise de Vulnerabilidades

a) Relatório, que deve ser entregue em 15 dias úteis a partir da formalização do pedido da análise, contendo as informações sobre as vulnerabilidades encontradas, suas causas e ações que devem ser tomadas para corrigi-las. Além disso, deve ser descrito o procedimento utilizado na análise, ferramentas utilizadas, resultado da análise (saída do comando executado), linha de comando executada com opções e/ou ações executadas que permitiram o resultado da análise (para redes/acessos externos/anexadas ou situações específicas, como o sistema SMV, por exemplo).

Relatório de Testes de Invasão

a) Relatório, que deve ser entregue em 15 dias úteis a partir da formalização do pedido do teste, contendo as informações sobre o teste de invasão realizado, descrevendo os problemas encontrados e ações que devem ser realizadas para corrigi-los. Além disso, deve ser descrito o procedimento utilizado no teste, ferramentas utilizadas, resultado do mesmo (saída do comando executado), linha de comando executada com opções e/ou ações executadas que permitiram o resultado do teste.

Relatório de Análise Forense

a) Relatório, que deve ser entregue em 20 dias úteis a partir da formalização do pedido da análise, contendo os resultados das análises de artefato e/ou análise forense.

Relatório de Análise de Conformidade

a) Relatório, que deve ser entregue em 10 dias úteis a partir da formalização do pedido da análise, contendo as informações sobre os pontos de falhas e aspectos de não-conformidade com as normas e procedimentos estabelecidos, juntamente com as devidas correções que devem ser realizadas para corrigir os desvios encontrados.

Relatórios Gerenciais

Relatório de Inclusão/ Modificação/ Exclusão de regras na segurança de rede Firewall

a) Relatório discriminando a quantidade total de regras criadas/ modificadas/ excluídas fora do prazo e a quantidade total regras criadas/ modificadas / excluídas no mês.

Relatório de bloqueios de endereço IP na segurança de rede Firewall

a) Relatório discriminando a quantidade total de IP bloqueados, a pedido da RFB, fora do prazo e a quantidade total IP bloqueados no mês.

Relatório de bloqueios de provedores Internet

a) Relatório discriminando a quantidade total de provedores Internet bloqueados, a pedido da RFB, fora do prazo e a quantidade total de provedores Internet bloqueados no mês.

Relatório de fixação de IP/NAT na segurança de rede Firewall

a) Relatório discriminando a quantidade total de IP/NAT fixados, a pedido da RFB, fora

do prazo e a quantidade total de IP/NAT fixados no mês.

Relatório de Inclusão/ Modificação/ Exclusão de endereços no "filtro de conteúdo"

a) Relatório discriminando a quantidade total de endereços alterados "filtro de conteúdo", a pedido da RFB, fora do prazo e a quantidade total de endereços alterados no "filtro de conteúdo" no mês.

Relatório de Criação de Domínios (DNS)

a) Relatório discriminando a quantidade de solicitações atendidas, a pedido da RFB, fora do prazo e a quantidade total de domínios criados no mês.

Relatório de Criação de Endereço IP

a) Relatório discriminando a quantidade total de endereços alterados no "filtro de conteúdo", a pedido da RFB, fora do prazo e a quantidade total de endereços alterados no "filtro de conteúdo" no mês.

Relatório de conexão de servidor WEB à Internet

a) Relatório discriminando a quantidade total de servidores WEB conectados à Internet, a pedido da RFB, fora do prazo e a quantidade total de servidores WEB conectados à Internet no mês.

Relatório de registros de DNS

a) Relatório discriminando a quantidade total de pedidos de registro de DNS, a pedido da RFB, fora do prazo e a quantidade total de pedidos de registro de DNS no mês.

5.3 Forma de Execução do Serviço

Central de Serviços da RFB

Para consultas e aberturas de chamados técnicos, durante 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, será utilizada a Central de Serviços da RFB.

Os chamados abertos na Central de Serviços serão referentes a todas as atividades de responsabilidade do SERPRO, englobando, mas não se limitando, à instalação, configuração, recuperação, alteração e remoção de equipamentos, à modificação/exclusão/inclusão de regras no firewall, aos bloqueios de endereço IP, aos bloqueios de provedores Internet, à fixação de IP/NAT na segurança de rede Firewall, à modificação/exclusão/inclusão de endereços no "filtro de conteúdo", à criação de domínios e endereços IP, à conexão de servidor WEB à Internet e ao registro de DNS. à configuração de roteadores, ao roteamento, endereçamento IP, SNMP, organização e atualização da gerência, de maneira a assegurar a integridade dos meios de comunicação fim-a-fim e a qualidade e desempenho do serviço de rede dentro dos limites estabelecidos.

Os registros dos chamados deverão conter todas as informações relativas ao chamado aberto, como tempo de início e fim de atendimento, identificação do elemento (equipamento, circuito de comunicação ou serviço) afetado, nome, telefone e e-mail do contato na RFB que foi posicionado acerca do reparo/restabelecimento do serviço, descrição detalhada da resolução do chamado com um código associado e responsabilidades.

Sistema de Controle de Demandas

Para consultas e aberturas de demandas, será utilizado o sistema informatizado de controle de demandas.

As demandas abertas neste sistema serão referentes a todas as atividades de responsabilidade do SERPRO, englobando, mas não se limitando, à instalação, à alteração de velocidade, à mudança de endereço de circuitos,

Os registros das demandas deverão conter todas as informações relativas à demanda aberta, como data de início e fim de atendimento, identificação do elemento (circuito de comunicação).

Todas as alterações necessárias ao perfeito funcionamento dos serviços contratados, que gerem ou não indisponibilidade, deverão ser previamente acordadas, por meio de autorização formal entre as partes, com no mínimo 02 (dois) dias úteis de antecedência.

O SERPRO deverá disponibilizar, sempre que solicitado, sua base de dados de chamados e demandas, conjuntamente com o modelo de dados, para que a RFB possa gerar relatórios com a finalidade de acompanhamento, averiguação ou auditoria.

Prazos para atendimento

	Indicador	Prazos
1	Prazo máximo para Incluir/ Modificar/ Excluir regras na segurança de rede Firewall	4 dias úteis
2	Prazo máximo para bloqueio de endereço IP na segurança de rede Firewall	4 dias úteis
3	Prazo para bloqueio de provedores Internet.	22 dias úteis
4	Prazo para fixação de IP/NAT na segurança de rede Firewall	4 dias úteis
5	Prazo máximo para Incluir/ Modificar/ Excluir endereços no "filtro de conteúdo"	4 dias úteis
6	Prazo de Criação de Domínios (DNS)	56 horas
7	Prazo para Criação de Endereço IP	12 dias úteis
8	Prazo para conexão de servidor WEB à Internet	4 dias úteis
9	Prazo para fazer registro de DNS	56 horas

5.4 Procedimento para Recebimento dos Serviços

O recebimento se dará pelo ateste de cumprimento dos níveis de serviço e da disponibilidade do serviço. O serviço será considerado executado a partir da análise e aceite do Demonstrativo de Execução do Serviço, entregue pelo SERPRO mensalmente.

O não cumprimento dos prazos especificados para serviço de segurança da informação, configura execução do serviço em desacordo com os termos contratados, passível de sanção nos termos da Cláusula Décima Terceira do Contrato.

5.5 Acordos de Nível de Serviço

ANS 1 – Indicador de Disponibilidade dos circuitos	
Item	**Descrição**
Finalidade	Garantir a disponibilidade dos circuitos que atendem às Unidades da RFB.
Meta a cumprir	• Pelo menos 100% dos circuitos – 97,00%

	• Pelo menos 80% dos circuitos – 97,20% • Pelo menos 60% dos circuitos – 97,40%
Instrumento de medição	Relatórios de ANS de Redes de Longa Distância (Prestação de Contas). O SERPRO deverá disponibilizar mensalmente à RFB, relatórios de ANS com os índices apurados diariamente, totalizados e apresentados mensalmente por circuito. Para todos os circuitos, inclusive para os que apresentarem operabilidade plena, deverão ser apresentados: o tempo de indisponibilidade (horas e minutos) e o tempo de interrupções programadas.
Forma de acompanhamento	Análise dos Relatórios de ANS, bem como ferramentas de monitoramento.
Periodicidade	Mensal
Mecanismo de cálculo	Disponibilidade efetiva do circuito (%)= (Quantidade de minutos disponíveis no mês / Quantidade de minutos no mês) x 100
Início de vigência	Início da prestação do serviço.
Descontos no pagamento	Desconto por indisponibilidade: A partir do primeiro dia do mês de apuração, as indisponibilidades deverão ser contabilizadas. a) Número de circuitos com disponibilidade menor que 97,4% / Número total de circuitos > 40% e Número de circuitos com disponibilidade menor que 97,2% / Número total de circuitos < 20% Então: Para cada circuito com (97,4% > disponibilidade efetiva >= 97,0%): Desconto = [2 x (0,974 – Disponibilidade efetiva do circuito) x (custo da interconexão do circuito)] b) Número de circuitos com disponibilidade menor que 97,4% / Número total de circuitos > 40% e Número de circuitos com disponibilidade menor que 97,2% / Número total de circuitos > 20% Então: Para cada circuito com (97,4% > disponibilidade efetiva >= 97,0%): Desconto = [3 x (0,974 – Disponibilidade efetiva do circuito) x (custo da interconexão do circuito)] c) Circuito com disponibilidade < 97,0% Então: Desconto por circuito cuja disponibilidade seja inferior a 97,0% = [5 x (0,97 – Disponibilidade efetiva do circuito) x (custo da interconexão do circuito)]
Sanções	Quando o total de circuitos com disponibilidade abaixo de 94,5% for superior a 5% da quantidade total dos circuitos contratados, configura-se execução do serviço em desacordo com os termos contratados, passível de sanção nos termos da Cláusula Décima Terceira do Contrato.

ANS 2 – Indicador de tempo de reparo ou restabelecimento	
Item	**Descrição**
Finalidade	Garantir o perfeito funcionamento dos circuitos de comunicação que

	atendem às Unidades da RFB.
Meta a cumprir	• Para as capitais dos Estados, exceto Região Norte – Prazo limite de 6 horas; • Para capitais dos Estados da Região Norte – Prazo limite de 8 horas; • Cidades do interior (todas, exceto as capitais dos Estados) – Prazo limite de 36 horas; • Cidades com dificuldades de acesso (RF-Óbidos, IRF-Balsa Candiru, IRF-Oiapoque, ARF-Laranjal do Jarí, ARF-Conceição do Araguaia, ARF-Itaituba, ARF-Oriximina, ARF-Monte Alegre, ARF-Altamira, ARF-Humaitá, ARF-Manes, IRF-Tabatinga e ARF-Tefé) – Prazo limite de 72 horas.
Instrumento de medição	Relatórios de ANS de Redes de Longa Distância (Prestação de Contas). A SERPRO deverá disponibilizar relatórios de ANS com os valores apurados por circuito. Os relatórios deverão fornecer, para cada unidade da RFB, os valores de tempo de atendimento gasto para reparo/restabelecimento do circuito com indicação das violações dos prazos e consolidação mensal por Região Fiscal.
Forma de acompanhamento	Análise dos relatórios de ANS, bem como análise dos registros da Central de Serviços.
Periodicidade	Mensal
Mecanismo de cálculo	É o tempo medido entre o início da indisponibilidade e o retorno ao estado pleno de funcionamento apurado para cada Circuito de comunicação. É dependente da distância da Unidade da RFB em relação à capital do Estado da Federação em que ocorreu a falha ou indisponibilidade. Se depois de fechada uma ocorrência, restabelecendo o estado operacional pleno do circuito de comunicação, ocorrer uma nova falha ou indisponibilidade, mesmo que de causa semelhante à anterior será considerada uma nova falha ou indisponibilidade e inicia-se uma nova contagem de tempo para reparo ou estabelecimento.
Início de vigência	Início da prestação do serviço.
Descontos no pagamento	Desconto por descumprimento = [(Soma do número de horas acima do limite definido na Métrica para cada ocorrência) dividido por 730 x (custo da interconexão do circuito)], sendo 730 horas a média mensal de horas considerando o ano com 365 dias, 24 horas no dia e 12 meses no ano, a ser calculado no momento do encerramento da demanda.
Sanções	Após 8 (oito) horas do prazo previsto no ANS, multa moratória nos termos da Cláusula Décima Terceira do Contrato.
Observações	Este ANS deverá ser analisado individualmente para cada circuito.

ANS 3 – Indicador de Prazo para instalação de circuito	
Item	**Descrição**
Finalidade	Garantir um atendimento célere às demandas para instalação de novos circuitos da RFB.
Meta a cumprir	• Região Norte urbano: prazo máximo de 60 dias; interurbano: prazo máximo de 75 dias. • Região Nordeste: urbano: prazo máximo de 55 dias;