0081687 08620.043831/2015-75

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA
FUNDAÇÃO NACIONAL DO ÍNDIO
SERVIÇO DE CONTRATOS

**ANEXO**

ANEXO II DO CONTRATO Nº. 009/2017

MODELO DE NEGÓCIO DOS SERVIÇOS DE SEGURANÇA

**CATEGORIA SEGURANÇA**

Os serviços dessa categoria são: Ponto de Proteção à Rede e/ou Aplicação – *Firewall*, Controle de Acesso a sítios Web – Filtro de Conteúdo,

O serviço de **Ponto de Proteção à Rede e/ou Aplicação – *Firewall*** tem como objetivo implantar numa rede de comunicação de dados determinada política de segurança.

O serviço de **Controle de Acesso a sítios Web – Filtro de Conteúdo** tem como objetivo o controle do acesso a sítios da Internet, por meio de políticas previamente definidas é possível permitir ou negar que uma rede tenha acesso a determinados grupos de sítios de acordo com tabela específica.

O serviço de **Prevenção à Intrusão - IPS** tem como finalidade promover a proteção aos serviços publicados em ZDM do SERPRO ou Clientes para acessos provenientes da Internet ou da rede local.

O serviço de **Proteção de Ataques de Negação de Serviço – DDOS,** consiste em atividades necessárias para monitorar, detectar e mitigar anomalias no acesso aos sítios monitorados, que podem ser alvos de ataques de negação de serviço.

**SEGURANÇA - SERVIÇO DE PONTO DE PROTEÇÃO À REDE E/OU APLICAÇÃO - FIREWALL Status: Disponível**

O serviço de Ponto de Proteção à Rede e/ou Aplicação – *Firewall* tem como finalidade configurar regras de tráfego de rede no ambiente de *firewall* virtual do SERPRO, ambientado em instâncias/contextos de *firewalls* instalados em *appliances* físicos com alta disponibilidade.

O serviço consiste em execução de atividades dispostas em 3 fases:

LEVANTAMENTO

- Coleta de informações sobre as características do ambiente;
- Levantamento da topologia do(s) serviço(s);
- Levantamento das regras existentes, contendo as portas, protocolos e endereços de origem e destino dos *hostnames*;
- Levantamento sobre procedimentos operacionais;
- Levantamento sobre documento de regras de acesso;
- Levantamento do Cronograma e Procedimentos para Implementação;

IMPLEMENTAÇÃO

- Migração de regras de *firewall*;
- Troca de endereçamento público;
- Reconfiguração de DNS;
- Configuração da Gerência do *firewall*;
- Criação de contas na solução de monitoramento;
- Desenho de topologia na solução de monitoramento; e

MONITORAÇÃO e MANUTENÇÃO

- Backup das regras;
- Atualizações de vulnerabilidades no ambiente de *firewall*;
- Monitoração 24 x7 do ambiente de *Firewall*;
- Criação ilimitada de regras, atendendo o prazo das requisições de serviço;

O Serviço de Ponto de Proteção à Rede e/ou Aplicação - *Firewall* é instalado e administrado no ambiente do SERPRO, sua administração será realizada somente por empregados do SERPRO. As informações monitoradas serão apresentadas, no modo 'somente leitura, ao cliente por meio de portal Web.

| 1 – COMPONENTES | |
|---|---|
| **Infraestrutura** | – *Firewall* virtual |
| | – Console de gerência para administração do *firewall* |
| | – *Cluster* de *switch* Internet |
| | - *Cluster* de *switch* Intranet |
| | - Solução de *backup* |
| | - Solução de monitoramento |
| | - Solução de publicação de informações aos clientes |
| **Suporte** | – Suporte técnico especializado na solução de *firewall* |

1.1 – Infraestrutura

***Firewall* Virtual**

O conjunto de especificações de hardware representa a solução física completa, sendo que cada *firewall* virtual compartilha os recursos físicos de forma virtualizada.

Consiste um cluster de *firewall* com as seguintes características:

- Composto de 2 (dois) *Gateway* em alta disponibilidade;
- Capacidade de ***Throughput*** de 110Gbs (cluster de *firewalls*);
- Interfaces redundantes de 1 ou 10GB (Fibra e Cobre).

**Console de gerência para administração do *Firewall***

Hardware de desenvolvimento próprio da empresa fornecedora, capaz de gerenciar todos os *firewalls* virtuais criados no cluster, destinado ao SERPRO e seus clientes.

***Cluster* de *switch* Internet**

O *cluster* de *firewall* Corporativo, destinado ao SERPRO e seus clientes, está interligado ao Site Tronco, através de uma redundância de *switch* de alta capacidade, com portas de 10Gb, para interligar as ZDMs aos *firewalls* e os *firewalls* a toda a infraestrutura de *Internet*.

***Cluster* de *switch* Intranet**

O *cluster* de *firewall* Corporativo destinado ao SERPRO e seus clientes está interligado ao Site Tronco, através de uma redundância de *switch* de alta capacidade, com portas de 10Gb, para interligar ao *Firewalls* toda a infraestrutura de Intranet.

**Solução de *backup***

Conjunto de ferramentas tecnológicas utilizadas para realizar *backup* e *restore* das regras de *firewall* e configurações do ambiente de *firewall*, em conformidade com a política de backup vigente.

**Solução de monitoramento do serviço**

Conjunto de ferramentas tecnológicas utilizadas para monitorar:

- Descarte de pacotes nas interfaces físicas;
- Erro nas interfaces;
- *Status* do Serviço:
  - Espaço em disco para a gerência do serviço;
  - Espaço em disco no cluster de *firewall.*
- Uso de CPU (processos de *log* e *firewall*);
- Número de conexões simultâneas:
  - Limite;
  - Atual;

- Pico.
- Memória livre.

**Solução de publicação de informações aos clientes**

Todas as informações de nível de serviço acordado serão publicadas no site do Portal GTIC, destinado aos clientes do SERPRO verificarem os níveis de serviços contratados.

1.2 – Suporte

As ocorrências devem ser encaminhadas aos grupos de suporte especializados na administração e manuseio da solução de *firewall*.

2 – INSUMOS

Unidade de *firewall* virtual

3 – NIVEIS DE SERVIÇO

No caso de solicitação de níveis de serviços diferenciados, ou seja, diferente dos disponibilizados no Acordo de Nível Operacional – ANO padrão, estes deverão ser previamente negociados juntamente à área de Gestão de Atendimento a Demandas da SUPGS e ao Gestor do Serviço desta SUPOP.

| **Indicadores de Serviço** | **Definição** | **Nível de Serviço** |
|---|---|---|
| Tempo de recuperação do Serviço em caso de falhas | Demonstra o tempo de atendimento das ocorrências tratadas pelo suporte técnico especializado | Até 2h |
| Disponibilidade | Demonstra a disponibilidade do serviço | 98% (24 x 7) |
| Tempo para criação/exclusão de regra de *firewall* (requisição de serviço) | Demonstra o tempo para atendimento de uma solicitação de criação/exclusão de regra de *firewall* | 5 (cinco) dias úteis após a abertura da requisição de serviço |

4 – PRAZOS DE ATENDIMENTO

O tempo para atendimento à implementação do serviço para um novo cliente dependerá da disponibilidade de recursos no momento da requisição: capacidade do ambiente de *firewall* para criação de instância/contexto de *firewall* virtual e ambiente do cliente estar acessível através da Rede SERPRO.

O prazo de atendimento para o levantamento e implantação do serviço será negociado entre as PARTES.

5 – FORMAS DE SOLICITAÇÃO DO SERVIÇO

5.1 – Processo para novas Demandas

Solicitação de implantação de novos serviços ou ampliação de serviços em produção deverão ser tratados junto ao Departamento de **Gestão de Demandas da SUPGS – GDNS.**

5.2 – Processo para atendimento/suporte

Solicitações para serviços já em produção poderão ser direcionados a **Central de Serviços – CSS** ou a **Gestão de Demandas da SUPGS – GDNS.**

A **Central de Serviços SERPRO** é o ponto único de contato dentro do ambiente de Tecnologia da Informação – TI disponibilizado para os clientes e usuários dos produtos e serviços SERPRO. É uma função estratégica pois agrega os componeentes necessários à percepção e satisfação dos clientes em relação aos serviços prestados pelo SERPRO. ***(A contratação deste serviço e maiores informações verificar no catálogo da SUPOP de Gerência de Serviço)***

*O acesso à Central pode ser realizado via telefone 0800, fax, e-mail css.serpro@serpro.gov.br ou acessando o sítio www.serpro.gov.br ."*

**SEGURANÇA - SERVIÇO DE CONTROLE DE ACESSO A SÍTIOS WEB - FILTRO DE CONTEÚDO** **Status: Disponível**

O serviço de Controle de Acesso a sítios Web – Filtro de Conteúdo é baseado em levantamento das políticas de acesso a sítios Internet, configuração dos parâmetros de utilização, monitoração do acesso e gerenciamento da solução de filtro de conteúdo.

O serviço consiste em execução de atividades dispostas em 3 fases:

LEVANTAMENTO

- Levantamento de política de acesso;
- Levantamento de requisitos técnicos do ambiente; e
- Levantamento de quantidade de usuário que acessam a Internet.

IMPLEMENTAÇÃO

- Elaboração da política de acesso;
- Configuração das categorias e política de acesso;
- Configuração da Gerência do filtro de conteúdo;
- Criação de contas na solução de monitoramento;
- Desenho de topologia na solução de monitoramento.

MONITORAÇÃO e MANUTENÇÃO

- Backup das configurações;
- Atualizações no ambiente de filtro de conteúdo;
- Monitoração 24 x7 de todo ambiente de filtro de conteúdo.

| Característica por modelo | Modelo Avançado |
|---|---|
| Bloqueio acesso HTTP/HTTPS aos sítios Internet conforme política estabelecida | HTTP e HTTPS |
| Uso de solução de antimalware* | Sim |
| Página de bloqueio customizada | Sim (mensagem e logomarca) |
| Políticas de acesso | Até 10 (dez) políticas com diferentes sítios/categorias |
| Reputação de Sítios | Sim |
| Controle de aplicações (Facebook, Youtube, Twitter) | Sim |
| Emissão de relatórios | Até 10 relatórios por mês ou customizados |
| Permissão de URLs (white list) | Até 100 URLs por ano |

*Analise de conteúdo suspeito e de tráfego malicioso com identificação das estações de trabalho que estão infectadas com aplicativos ilícitos (*malwares*, vírus, *trojans*).

O Serviço de Serviço de Controle de Acesso a sítios Web – Filtro de Conteúdo é instalado e administrado no ambiente SERPRO.

| 1 – COMPONENTES | |
|---|---|
| **Infraestrutura** | – Solução de Filtro de Conteúdo |
| | – Balanceador de carga |
| | - Solução de backup |
| | - Solução de monitoramento |
| **Suporte** | – Suporte técnico especializado na solução de filtro de conteúdo |

1.1 – Infraestrutura

**Solução de Filtro de Conteúdo**

Consiste de solução de filtro de conteúdo com a seguinte especificação de hardware:

- *Cluster* destinado à solução corporativa de Filtro de conteúdo *Web*.

**Balanceador de carga**

O conjunto de *appliances* responsável pela filtragem de conteúdo web estão interligados a um balanceador de carga que desvia todo o tráfego HTTP e HTTPS. O deslocamento destes protocolos permite que cada *appliance* receba de forma balanceada a quantidade de conexões estabelecidas. Assim, a qualidade e a disponibilidade da conexão do usuário é duplicada de forma transparente para o usuário.

**Solução de backup**

Conjunto de ferramentas tecnológicas utilizadas para realizar *backup* e *restore*, em conformidade com a política de *backup* vigente, das configurações do ambiente de filtro de conteúdo e das *logs* de acesso geradas.

**Solução de monitoramento**

Conjunto de ferramentas tecnológicas utilizadas para monitorar:

- Tempo de resposta
- Número de conexões simultâneas
- Uso de CPU
- Erro de *interface* no balanceador
- Balanceamento entre os equipamentos
- Categorização do sítio
- Identidade do usuário
- Política de acesso

1.2 – Suporte

As ocorrências devem ser encaminhadas aos grupos de suporte especializados na administração e manuseio da solução de filtro de conteúdo.

2 – INSUMOS

Quantidade de usuários/mês.

3 – NIVEIS DE SERVIÇO

No caso de solicitação de níveis de serviços diferenciados, ou seja, diferente dos disponibilizados no Acordo de Nível Operacional – ANO padrão, estes deverão ser previamente negociados juntamente à área de Gestão de Atendimento a Demandas e ao Gestor do Serviço desta SUPOP.

| **Indicadores de Serviço** | **Definição** | **Nível de Serviço** |
|---|---|---|
| Tempo de recuperação do Serviço em caso de falhas | Demonstra o tempo de recuperação do serviço | Até 2h |
| Disponibilidade | Demonstra a disponibilidade do serviço | 95% (24 x 7) |
| Tempo para análise de liberação/bloqueio de sítios (requisição de serviço) | Demonstra o tempo para atendimento de uma solicitação de liberação/bloqueio de acesso a um sítio. | 3 (três) dias úteis após a abertura da requisição de serviço |

4 – PRAZOS DE ATENDIMENTO

O tempo para atendimento à implementação do serviço para um novo cliente dependerá da disponibilidade de recursos no momento da requisição: capacidade de conexões simultâneas da solução de filtro de conteúdo, ambiente do cliente estar acessível por meio da Rede SERPRO.

O prazo de atendimento para o levantamento e implantação do serviço será negociado entre as **PARTES**.

5 – FORMAS DE SOLICITAÇÃO DO SERVIÇO

| 5.1 – Processo para novas Demandas |
|---|
| Solicitação de implantação de novos serviços ou ampliação de serviços em produção deverão ser tratados junto ao Departamento de **Gestão de Demandas da SUPGS – GDNS.** |

| 5.2 – Processo para atendimento/suporte |
|---|
| Solicitações para serviços já em produção poderão ser direcionados a **Central de Serviços – CSS** ou a **Gestão de Demandas da SUPGS – GDNS.**<br><br>A **Central de Serviços SERPRO** é o ponto único de contato dentro do ambiente de Tecnologia da Informação – TI disponibilizado para os clientes e usuários dos produtos e serviços SERPRO. É uma função estratégica pois agrega os componentes necessários à percepção e satisfação dos clientes em relação aos serviços prestados pelo SERPRO. ***(A contratação deste serviço e maiores informações verificar no catálogo da SUPOP de Gerência de Serviço)***<br><br>*O acesso à Central pode ser realizado via telefone 0800, fax, e-mail css.serpro@serpro.gov.br ou acessando o sítio www.serpro.gov.br ."* |

**SEGURANÇA - SERVIÇO DE PREVENÇÃO À INTRUSÃO - IPS** **Status: Disponível**

O serviço de Prevenção à Intrusão - IPS tem como finalidade promover a proteção aos serviços publicados em ZDM do SERPRO ou Clientes para acessos provenientes da Internet ou da rede local. A proteção tem como escopo: monitorar, detectar e bloquear ataques direcionados à ZDM do cliente, por meio de aplicação de assinaturas dedicadas.

| 1 – COMPONENTES | |
|---|---|
| **Infraestrutura** | – Intrusion Detection System (IPS) |
| | - Assinaturas Atualizadas |
| | - Sistema de ByPass Automático |
| | - Sistema com Politicas Abrangentes na Borda |
| | - Sistema de Proteção com Politicas Restritivas nas ZDMs. |
| | - Solução de publicação de informações aos clientes |
| | - Solução de Backup |
| | - Solução de Monitoramento |
| **Suporte** | – Suporte técnico especializado na solução de IPS |

| 1.1 – Infraestrutura |
|---|
| **Intrusion Detection System (IPS)**<br><br>Consiste de um ativo Intrusion Detection System (IPS) com a seguinte especificação de hardware:<br><br>• *Appliances* com capacidade de 7 e 10 Gbs de analise de tráfego;<br>• Solução de Gerenciamento, monitoração e aplicação de políticas. |
| **Assinaturas Atualizadas**<br><br>O arquivo de assinatura é um pacote de assinaturas de rede criado como uma atualização das assinaturas que já existem nos produtos da McAfee e SourceFire com funções de IPS ou IDS. Estas assinaturas são usadas pelas soluções IPS ou IDS para comparar o tráfego de rede com outros modelos dentro da biblioteca de arquivos de assinatura. O IPS/IDS utiliza esta comparação para detectar tráfego de rede não autorizado ou suspeito. Quando a solução IPS estiver instalada, o arquivo de assinatura servirá de base de dados, a qual serve para detectar qualquer movimento suspeito. |
| **Sistema com Políticas Abrangentes na Borda**<br><br>Todo o tráfego entrante com destino aos serviços de publicação dos clientes tem uma politica abrangente, conhecida como “Menos Restritiva”. Essa forma de ação permite que assinaturas abrangentes a todos os clientes, e que não contenham assinaturas personalizadas ou específicas, sejam filtradas diretamente na entrada da Rede SERPRO. |
| **Sistema de Proteção com Politicas Restritivas nas Zdms** |

Diferente da Politica Abrangente, os IPS localizados depois dos *firewalls* são os responsáveis por manter as Politicas Restritivas, que contemplam as assinaturas personalizadas para cada cliente, ou sistema de clientes. Nestes equipamentos, o cliente tem a oportunidade de, junto com a equipe de Segurança do SERPRO, alterar, configurar e bloquear assinaturas que não prejudicam outros sistemas compartilhados.

**Sistema de *ByPass* Automático**

O *Bypass* oferece proteção contra "caso de falha" para garantir a disponibilidade de uma rede protegida. Se a conformidade do IPS falha por qualquer razão, o *bypass* é designado para garantir que a rede permaneça funcional e que os usuários tenham acesso irrestrito a aplicativos importantes.

**Solução de backup**

Conjunto de ferramentas tecnológicas utilizadas para realizar *backup* e *restore*, em conformidade com a política de backup vigente, das regras e configurações do ambiente de IPS.

**Solução de monitoramento**

Conjunto de ferramentas tecnológicas utilizadas para monitorar:

- Utilização de memória
- Status do equipamento e comunicações
- Descarte de pacotes no equipamento
- Descarte de pacotes nas *interfaces*

**Solução de publicação de informações aos clientes**

Todas as informações de nível de serviço acordado serão publicadas no site do Portal GTIC, destinado aos clientes do SERPRO verificarem os níveis de serviços contratados.

1.2 – Suporte

As ocorrências de solicitação devem ser encaminhadas aos grupos de suporte especializados na administração e manuseio do ativo *Intrusion Detection System* (IPS).

## 2 – INSUMOS

Segmento de Portas de 100Mb (conjunto de portas de 100mbps)

## 3 – NIVEIS DE SERVIÇO

No caso de solicitação de níveis de serviços diferenciados, ou seja, diferente dos disponibilizados no Acordo de Nível Operacional – ANO padrão, estes deverão ser previamente negociados juntamente à área de Gestão de Atendimento a Demandas e ao Gestor do Serviço desta SUPOP.

| **Indicadores de Serviço** | **Definição** | **Nível de Serviço** |
|---|---|---|
| Tempo de recuperação do Serviço em caso de falhas | Demonstra o tempo de recuperação do serviço | Até 2h |
| Disponibilidade | Demonstra a disponibilidade do serviço | 98% (24 x 7) |

## 4 – PRAZOS DE ATENDIMENTO

O tempo para atendimento à implementação do serviço para um novo cliente dependerá da disponibilidade de recursos no momento da requisição: ambiente do cliente estar acessível através da Infovia ou Rede SERPRO.

## 5 – FORMAS DE SOLICITAÇÃO DO SERVIÇO

5.1 – Processo para novas Demandas

Solicitação de implantação de novos serviços ou ampliação de serviços em produção deverão ser tratados junto ao Departamento de **Gestão de Demandas da SUPGS – GDNS.**

| 5.2 – Processo para atendimento/suporte |
|---|
| Solicitações para serviços já em produção poderão ser direcionados a **Central de Serviços – CSS** ou a **Gestão de Demandas da SUPGS – GDNS.**<br><br>A **Central de Serviços SERPRO** é o ponto único de contato dentro do ambiente de Tecnologia da Informação – TI disponibilizado para os clientes e usuários dos produtos e serviços SERPRO. É uma função estratégica pois agrega os componentes necessários à percepção e satisfação dos clientes em relação aos serviços prestados pelo SERPRO. ***(A contratação deste serviço e maiores informações verificar no catálogo da SUPOP de Gerência de Serviço)***<br><br>*O acesso à Central pode ser realizado via telefone 0800, fax, e-mail css.serpro@serpro.gov.br ou acessando o sítio www.serpro.gov.br ."* |

**SEGURANÇA - SERVIÇO DE PROTEÇÃO DE ATAQUES DE NEGAÇÃO DE SERVIÇO - DDOS** **Status: Disponível**

O Serviço de Proteção de Ataques de Negação de Serviço - DDOS consiste em atividades necessárias para monitorar, detectar e mitigar anomalias no acesso aos sítios monitorados, que podem ser alvos de ataques de negação de serviço.

O monitoramento visa definir o comportamento padrão do acesso ao sítio e parametrizar os protocolos utilizados no acesso e os níveis de utilização de cada um deles. Também será definida uma linha de base de utilização de banda e de quantidade de pacotes por segundo esperado, utilizando o histórico de acesso para calcular os valores esperados.

Definidos os parâmetros de normalidade do acesso ao sítio, serão definidos níveis de tolerância máximos para utilização de cada protocolo envolvido e do tráfego de rede.

Quando ultrapassados, serão gerados alertas e notificações, que serão correlacionados e analisados para confirmação da situação de ataque de negação de serviço. Confirmado o ataque, serão ativados mecanismos para mitigá-lo e manter ou normalizar a disponibilidade do sítio monitorado. Serão utilizados múltiplos mecanismos de contra-medidas para bloquear os acessos inválidos e minimizar a interferência nos acessos dos clientes válidos.

É escopo do serviço:

- Possuirá configuração e monitoração por cada IP do sítio internet, solicitado pelo cliente;
- Protegerá todas as aplicações acessadas no IP monitorado, considerando o formato IP/Aplicação (ex: meu_site_IP/aplicacao01, meu_site_IP /aplicacao02, etc.);
- Contemplará a inspeção, monitoração e proteção do(s) IP a ser(em) informado(s) pelo cliente no momento da instalação do serviço

Está excluído do escopo:

- Proteção de sites ou aplicações por domínio (endereço nominal do sítio), não podendo ser aplicado para domínios disponíveis na Internet por meio de *clusters*. Neste caso, sua proteção deverá ser aplicada especificamente para cada nó (IP) do *cluster*.
- Proteção de sites ou aplicações disponibilizadas em IP diferente do IP definido para ser protegido, mas que em alguns casos são acessadas (via navegação web ou chamadas embutidas) pelo usuário a partir do sítio protegido.

O serviço consiste em execução de atividades dispostas em 3 fases:

LEVANTAMENTO

- Levantamento do sítio a ser monitorado;
- Descrição dos protocolos mais utilizados; e
- Descrição das características de acesso ao sítio a ser monitorado.

IMPLEMENTAÇÃO

- Configuração inicial dos parâmetros de detecção de anomalias (os níveis máximos de uso dos protocolos, tipos de pacotes, banda utilizada e a tolerância às anomalias detectadas no acesso ao objeto monitorado);
- Configuração dos parâmetros de mitigação padrão

MONITORAÇÃO e MANUTENÇÃO

- Backup das configurações;
- Atualizações no ambiente da solução de proteção de ataques de negação de serviço;
- Monitoração 24 x7 de todo ambiente da solução de proteção de ataques de negação de serviço.

O Serviço de proteção de ataques de negação de serviço - DDOS é instalado e administrado no ambiente do SERPRO. A administração da solução de proteção de ataques de negação de serviço serão realizadas somente por empregados do SERPRO.

| 1 – COMPONENTES | |
|---|---|
| **Infraestrutura** | – CP (Collector Platform) |
| | – TSM (Threat Management System) |
| | – Roteador de borda |
| | - Solução de monitoramento |
| **Suporte** | – Suporte técnico especializado na solução de proteção de ataques de negação de serviço |

1.1 – Infraestrutura

**CP (Collector Platform)**

*Appliance* adquirido pelo SERPRO, utilizado para coletar e analisar o fluxo de pacotes que trafegam pela rede.

**TSM (Threat Management System)**

*Appliance* adquirido pelo SERPRO, utilizado para mitigar anomalias identificadas no fluxo de pacotes que trafegam pela rede.

**Roteador de borda**

O SERPRO faz parte do conjunto de empresas que mantêm o funcionamento da *Internet* no Brasil e é considerada um AS, Sistema Autônomo. Assim, com esta responsabilidade técnica, é capaz de concentrar uma grande quantidade de dados de *Internet* em seus roteadores de borda, permitindo uma largura de banda entrante de até 10Gb, distribuídos em seus 3 prestadores de serviços. Assim, os roteadores de bordas do SERPRO, ligados a solução de proteção de ataques de negação de serviço, são capazes de mitigar os ataques deste tipo.

**Solução de monitoramento**

Conjunto de ferramentas tecnológicas utilizadas para monitorar:

- Tráfego Suspeito
- Tráfego com anomalias
- IPs de listas negras internacionais

1.2 – Suporte

As solicitações devem ser encaminhadas aos grupos de suporte especializados na administração e manuseio da solução de proteção de ataques de negação de serviço.

2 – INSUMOS

Por URL/mensal

3 – NIVEIS DE SERVIÇO

No caso de solicitação de níveis de serviços diferenciados, ou seja, diferente dos disponibilizados no Acordo de Nível Operacional – ANO padrão, estes deverão ser previamente negociados juntamente à área de Gestão de Atendimento a Demandas e ao Gestor do Serviço desta SUPOP.

| **Indicadores de Serviço** | **Definição** | **Nível de Serviço** |
|---|---|---|
| Tempo máximo de mitigação* | Demonstra o tempo para que a mitigação automática interprete um ataque e entre em funcionamento | Até 5 (cinco) minutos a partir da identificação do ataque |
| Disponibilidade | Demonstra a disponibilidade do serviço | 98% (24 x 7) |
| Relatório Mensal do Serviço | Demonstra o quantitativo de ataques realizados por mês | 1 (um) relatório por mês, entregue até o 12º dia do mês subsequente a prestação do serviço |

** Este tempo oscila conforme a existência ou inexistência de outros ativos de rede, como IPS, Firewall, etc. e conforme as configurações periódicas, sempre que necessárias, realizadas para monitoração e identificação de ataques.*

4 – PRAZOS DE ATENDIMENTO

O tempo para atendimento à implementação do serviço para um novo cliente dependerá da disponibilidade de recursos no momento da requisição: ambiente do cliente estar acessível através da Infovia ou Rede SERPRO.
O prazo de atendimento para o levantamento e implantação do serviço será negociado entre as **PARTES**.

5 – FORMAS DE SOLICITAÇÃO DO SERVIÇO

5.1 – Processo para novas Demandas

Solicitação de implantação de novos serviços ou ampliação de serviços em produção deverão ser tratados junto ao Departamento de **Gestão de Demandas da SUPGS – GDNS.**

5.2 – Processo para atendimento/suporte

Solicitações para serviços já em produção poderão ser direcionados a **Central de Serviços – CSS** ou a **Gestão de Demandas da SUPGS – GDNS.**
A **Central de Serviços SERPRO** é o ponto único de contato dentro do ambiente de Tecnologia da Informação – TI disponibilizado para os clientes e usuários dos produtos e serviços SERPRO. É uma função estratégica pois agrega os componentes necessários à percepção e satisfação dos clientes em relação aos serviços prestados pelo SERPRO. ***(A contratação deste serviço e maiores informações verificar no catálogo da SUPOP de Gerência de Serviço)***
*O acesso à Central pode ser realizado via telefone 0800, fax, e-mail css.serpro@serpro.gov.br ou acessando o sítio www.serpro.gov.br ."*

## DESCRIÇÃO DOS SERVIÇOS

| Descrição dos serviços | Preço | Unidade | Quantidade | Preço Total mensal |
|---|---|---|---|---|
| 1 - Firewall virtual - unidade de firewall virtual | 0,00 | Parcela mensal | 1 | 0,00 |
| 2 - DDOS - por URL mensal | 0,00 | Parcela mensal | 1 | 0,00 |
| 3 - IPS - Segmento de portas de 100Mb (conjunto de portas de 100mbps) | 0,00 | Parcela mensal | 100 | 0,00 |
| 4 - Filtro de conteúdo - Acessos à sítios WEB | 0,00 | Parcela mensal | 1000/uso. mês | 0,00 |
| Por cada estação de trabalho - Qtde de usuários/mês | Por usuário | | | |

Atualizado(a) em 03 de março de 2017.

Documento assinado eletronicamente por **Daniel Silva Antonelli**, **Usuário Externo**, em 25/05/2017, às 10:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **MAXIMO OLIVEIRA DE SOUZA**, **Diretor(a) Substituto**, em 26/05/2017, às 17:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site: http://sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0081687** e o código CRC **084330BD**.

**Referência:** Processo nº 08620.043831/2015-75 SEI nº 0081687