



www.serpro.gov.br

Consulta pública para o serviço Anti-DDoS em Nuvem

Sumário

| | |
|--|----|
| 1 – Do Objeto | 3 |
| 2 – Da Especificação do objeto e local da execução dos serviços | 3 |
| 3. Da fiscalização dos serviços pelo Serpro e dos níveis de serviço..... | 11 |

1 – Do Objeto

1.1. Avaliar via consulta pública o processo de serviço Anti-DDoS em Nuvem e proteção adicional Anti-DDoS em Nuvem sob demanda.

2 – Da Especificação do objeto e local da execução dos serviços

2.1. O serviço Anti-DDoS em Nuvem e proteção Adicional Anti-DDoS em Nuvem, fornecida através de proteção baseadas em throughput (volume de dados) de tráfego limpo, sob demanda.

2.2. Com o objetivo de maior clareza caracteriza-se “tráfego limpo” como o tráfego não originado a partir de ataques DoS ou DDoS. Os tráfegos identificados como ataques não podem ser caracterizados como tráfego limpo;

2.3. O serviço em nuvem é identificado como um centro de limpeza (Scrubbing Center) e será entregue por meio do uso de solução em nuvem para o encaminhamento de tráfego a ser tratado em situações que o SERPRO julgar necessário;

2.4. Para o serviço, a quantidade a ser adquirida é definida na tabela, abaixo:

| Grupo | Item | Descrição | Unidade | Quantidade | Localidade |
|-------|------|--|-------------|------------|------------|
| 1 | 1 | Serviço Anti-DDoS em Nuvem com 5120 Mbps de throughput de tráfego limpo. | Mensalidade | 36 | Brasília |
| | 2 | Proteção Adicional para serviço Anti-DDoS em Nuvem de 1024 Mbps de throughput de tráfego limpo por mês | Bloco | 120 | Brasília |

2.5. O serviço Anti-DDoS em Nuvem, item 1, refere-se ao serviço em nuvem para entrega de 5120 Mbps de throughput de tráfego limpo encaminhado para as redes do Serpro após análise e descarte de todo o tráfego considerado malicioso executado pelo serviço em nuvem;

2.6. O item 2, Proteção Adicional para serviço Anti-DDoS em Nuvem, pode ser contratado por meio de unidades definidas como um bloco de throughput de tráfego limpo de 1024 Mbps adicional ou em múltiplas unidades (múltiplos de 1024 Mbps) adicionais, onde a proteção adicional poderá ser provisionada por períodos mínimos de 1 (um) mês e poderão ser desprovisionadas a qualquer tempo;

2.7. A contratação do item 1 com throughput de tráfego limpo para 5120 Mbps será provisionada no início do contrato, a proteção adicional, item 2, serão contratados sob demanda durante a vigência do contrato, não havendo obrigatoriedade de provisionamento do volume total estimado;

2.7.1. A proteção adicional, item 2, será contratada sob demanda durante a vigência do contrato, não havendo obrigatoriedade de provisionamento do volume total estimado;

2.8. Não há obrigatoriedade de provisionamento mínimo de proteção adicional, item 2.

2.9. Não caberá qualquer ônus entre os intervalos de proteção adicional provisionada e desprovisionada, somente sendo pago o período de uso;

2.10. O objeto a ser contratado deve atender todos os itens deste documento e são obrigatórios;

2.11. Da operacionalização do serviço e proteção adicional

2.11.1. O serviço Anti-DDoS em Nuvem, item 1, será provisionado no início do contrato;

2.11.2. As proteções adicionais, item 2, serão fornecidas sob demanda, de acordo com solicitação de serviço (SS) a ser emitida pelo SERPRO, limitado ao total de 5 (cinco) unidades, onde poderão ser provisionadas por um período mínimo de 1 (um) mês e desprovisionadas a qualquer tempo;

2.11.3. O serviço e proteção adicional devem fornecer a inspeção do tráfego contratado, baseado no perfil médio de utilização, e não devem limitar a quantidade de recursos protegidos nem o throughput na ocorrência de picos (sobrecargas) de utilização;

2.11.4. A Solicitação de Serviço (SS), que deve ser elaborada pelo SERPRO, detalhará a demanda e as informações relacionadas a alteração do quantitativo;

2.11.5. A CONTRATADA terá o prazo de até 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinatura da solicitação de serviço (SS);

2.11.6. A CONTRATADA terá o prazo de 10 (dez) dias úteis após a emissão da Solicitação de Serviço (SS) para a entrega do Item 2

2.11.7. A proteção adicional, item 2, será solicitada sob demanda, não havendo obrigatoriedade de realização do total ou de parte estimada;

2.11.8. A CONTRATADA deve providenciar a alteração do quantitativo na data estipulada na solicitação de serviço (SS);

2.11.9. A entrega do serviço e provisionamento de proteção adicional devem constar como entregues na localidade do SERPRO, na Regional Brasília;

2.11.10. As versões de software do serviço devem ser as últimas disponíveis no mercado na data de entrega do produto;

2.11.11. O idioma da documentação técnica deve ser em português do Brasil ou em inglês;

2.11.12. A documentação técnica, composta por manuais de instalação, configuração e operação poderá ser em formato digital;

2.12. Características Gerais

2.12.1. O serviço tem como objetivo proteger os serviços e manter disponível os links internet, independentemente da operadora de telecomunicação e consequentemente proteger todo o tráfego do SERPRO direcionado a CONTRATADA;

2.12.2. O serviço irá garantir a entrega de tráfego limpo para as localidades definidas pelo SERPRO;

2.12.3. O serviço deve ser fornecido com todas as funcionalidades aqui especificadas, operando de forma funcional, em todos os componentes, sem custo adicional para o SERPRO;

2.12.4. A CONTRATADA deve possuir centros de limpeza (scrubbing centers) próprios e com uma capacidade total agregada de no mínimo 4 (quatro) Tbps;

2.12.5. A CONTRATADA deve possuir pelo menos um centro de limpeza (Scrubbing Center) no Brasil com capacidade de depuração adequada e possibilidade de entrega de 50 (cinquenta) Gbps de tráfego limpo para o SERPRO, de forma que o tráfego legítimo com origem no Brasil seja tratado no centro de limpeza no Brasil. Este centro deve estar ativo e funcional no momento da entrega do serviço;

2.12.6. A CONTRATADA deve garantir a capacidade de entrega de tráfego limpo em taxa mínima equivalente aos quantitativos provisionados;

2.12.7. A CONTRATADA deve possuir centros de limpeza na Ásia, Américas e Europa e devem tratar ataques originados fora do Brasil em centros de limpeza mais próximos à origem dos ataques;

2.12.8. O serviço deve permitir um número ilimitado de acionamentos para a depuração/limpeza do tráfego do SERPRO, sem custo adicional;

2.12.9. A CONTRATADA fica responsável por todos os ajustes de configuração e reconfiguração do ambiente sem custo adicional para o SERPRO.

2.12.10. O serviço fornecido pela CONTRATADA, uma vez configurado, deve ter a opção de ser desativado e ativado sem precisar fazer alterações em aplicações ou DNS (Domain Name System), não afetando o serviço oferecido aos usuários;

2.12.11. O serviço não pode de forma alguma armazenar dados do SERPRO, bem como de seus clientes, a análise e tratamento do tráfego será pura e exclusivamente para a detecção e mitigação de ataques;

2.12.12. A CONTRATADA deve fornecer um número para comunicação direta com o SOC e permitir a comunicação via chat seguro com os especialistas do SOC na medida do necessário;

2.13 Arquitetura e Implantação

2.13.1. O serviço fornecido pela CONTRATADA deve possuir suporte e capacidade de mitigação para redes IPv4 e Ipv6;

2.13.2. O acionamento do desvio de tráfego para os centros de limpeza deve ser disponibilizado via publicação de rotas via BGP e console de gerenciamento WEB publicada na Internet;

2.13.3. Serviço deve estar ativo e licenciado para operar com a proteção e divulgação de 30 redes máscara /24 bem como a sumarização em máscaras /23 e /22.

2.13.4. O serviço deve permitir a configuração de endereço IP e grupos de IPs para a mitigação do tráfego, possibilitando que apenas o tráfego de aplicações desejadas seja inspecionado no centro de limpeza, evitando assim que seja feita a mitigação do tráfego de aplicações que não devem ser inspecionados;

2.13.5 O serviço deve ser capaz de suportar os métodos de entrega do tráfego limpo de volta a rede do SERPRO, conforme características mínimas:

2.13.5.1. Suportar túnel GRE;

2.13.5.2. Suportar Conexão direta e dedicada;

2.13.6. O tráfego limpo de ser entregue em todos os Centro de Dados do Serpro, em São Paulo/SP e Brasília/DF;

2.13.7. O tráfego limpo deve ser entregue via conexão direta e dedicada em todos os Centro de Dados do Serpro sem comprometimento da latência do acesso e experiência do usuário;

2.13.7.1. Fica a critério do Serpro a utilização dos tuneis GRE para entrega do tráfego limpo;

2.13.8. O serviço deve suportar, no mínimo, os modos operacionais abaixo:

2.13.8.1. Passivo: Detecção completa de ataques, sem bloqueio;

2.13.8.2. Ativo: Detecção completa de ataques, interceptação e bloqueio;

2.13.9. O serviço deve permitir que o tráfego limpo seja entregue ao SERPRO em equipamentos diferentes para balanceamento de carga, sem custo adicional;

2.13.10. A CONTRATADA deve ser capaz de disponibilizar o serviço de adaptação e implementação na fase de configuração inicial para garantir a configuração adequada do serviço em um ambiente de produção, sem causar nenhum tipo de impacto a outros serviços;

2.13.11. Permitir a comunicação em português via chat seguro por meio de recursos que garantam a segurança na comunicação com os especialistas do SOC durante as interações necessárias entre as equipes da CONTRATADA e do SERPRO;

2.13.12. O serviço deve possibilitar o armazenamento de logs de auditoria e alertas;

2.13.13. O serviço deve possibilitar a exportação de logs para fontes externas;

2.13.14. O serviço deve detectar, identificar e mitigar ameaças em tempo real e entregar o tráfego legítimo ao SERPRO;

2.14. Funcionalidades de Proteção e Mitigação

2.14.1. O serviço deve fornecer recursos de detecção e mitigação de ataques DDoS;

2.14.2. O serviço deve fornecer proteção de DDoS para as camadas 3 (três), 4 (quatro) e 7 (sete);

2.14.3. O serviço deve fornecer proteção DDoS da camada 7 (sete) para tráfego criptografado e não criptografado, sem custo adicional;

2.14.4. O serviço deve ter capacidade de aprender automaticamente os perfis de acesso e o comportamento esperado de uma rede protegida, sem intervenção manual;

2.14.5. O serviço deve por meio dos serviços gerenciados ser capaz de realizar a detecção, mitigação e gerenciamento centralizado do tráfego destinado aos centros de limpeza;

2.14.6. O serviço deve prover funções administrativas de atualização das políticas, políticas personalizadas e de relaxamento para reduzir falsos positivos;

2.14.7. O serviço deve implementar listas de acesso (accesslist) e listas de bloqueio (blocklist) via interface de gerência WEB

2.14.8. O serviço deve ser capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas por bots e ataques automatizados;

2.14.9. O serviço deve realizar a mitigação dos ataques de forma transparente para os usuários e os acessos legítimos, garantindo que sua experiência não seja prejudicada durante os ataques e eliminando alertas de falso positivo, mesmo quando a origem do um ataque for de uma estação com acessos válidos;

2.14.10. O serviço deve proteger contra-ataques de volumetria, complexos e com múltiplos vetores distintos;

2.14.11. Os parâmetros de proteção do serviço em nuvem listados devem ser editáveis sem restrições via interface de gerência WEB:

2.14.11.1 Endereço IP/máscara submetido às proteções do serviço;

2.14.11.2 Listas de bloqueio de:

2.14.11.2.1. IPs;

2.14.11.2.2. Portas de serviço TCP e UDP;

2.14.11.2.3. Protocolos TCP, UDP e ICMP;

2.14.11.3. Lista de acesso de:

2.14.11.3.1. IPs;

2.14.11.3.2. Portas de serviço TCP e UDP;

2.14.11.3.3. Protocolos TCP, UDP e ICMP;

2.14.12. O serviço deve suportar mecanismos de detecção baseados em:

2.14.12.1. Assinaturas de ataques;

2.14.12.2. Padrões de acesso histórico;

2.14.12.3. Comportamento em não conformidade com as RFCs;

2.14.12.4. Volumétrico em pacote e bytes por segundo;

2.14.12.5. Limites predefinidos de tráfego por protocolos TCP, UDP e ICMP;

2.14.13. O serviço deve suportar mecanismos de mitigação baseados em:

2.14.13.1. Bloqueio por IP, protocolo, socket TCP e localização geográfica do ponto de acesso e operação à rede do serviço;

2.14.13.2. Liberação por IP, protocolo, socket TCP e localização geográfica do ponto de acesso e operação à rede do serviço;

2.14.13.3. Lista de reputação de IPs maliciosos detectados, atualizados e fornecidos pela fabricante do serviço;

2.14.13.4. Limite da quantidade de tráfego em pacotes e bytes por segundo de uma determinada origem IP;

Limite da quantidade de tráfego em pacotes e bytes por segundo de uma determinada região do globo terrestre;

2.14.13.6. No estabelecimento das conexões criptografadas em HTTPS;

2.14.13.7. Ataques de baixa velocidade;

2.14.13.8. Pacotes mal-formados;

2.14.13.9. Identificação e validação de acessos com origens forjadas;

2.14.13.10. Bloqueio de pacotes por conexão TCP;

- 2.14.13.11. Bloqueio de datagramas por fluxo UDP;
- 2.14.13.12. Bloqueio e mitigação de ataques nos roteadores mais próximos da origem do ataque;
- 2.14.14. O serviço deve detectar o invasor e registrar sua identificação de forma individual;
- 2.14.15. O serviço não deve impedir o tráfego em conformidade com as RFCs associadas;
- 2.14.16. O serviço deve possuir mecanismos necessários para a mitigação de ataques DDoS, sejam eles baseados em volume, em protocolos de rede (camadas 3 e 4) e em nível básico de aplicação (camada 7), considerando no mínimo a seguinte lista (não exaustiva):
 - 2.14.16.1. SYN Flood;
 - 2.14.16.2. ACK Flood;
 - 2.14.16.3. UDP Flood;
 - 2.14.16.4. ICMP Flood;
 - 2.14.16.5. TCP Flag Null Flood;
 - 2.14.16.6. HTTP Flood;
 - 2.14.16.7. HTTPS Flood;
 - 2.14.16.8. DNS Query Flood;
 - 2.14.16.9. FIN/RST Flood;
 - 2.14.16.10. Connection Flood;
 - 2.14.16.11. TCP Misuse;
 - 2.14.16.12. TCP Fragment;
 - 2.14.16.13. UDP Fragment;
 - 2.14.16.14. Amplificação:
 - 2.14.16.14.1. DNS;
 - 2.14.16.14.2. NTP;
 - 2.14.16.14.3. SSDP;
 - 2.14.16.14.4. SNMP;
 - 2.14.16.15. Low-Slow, como Slowloris e Slow Read;
 - 2.14.16.16. SYN+UDP ou ICMP+UDP (Mixed);
 - 2.14.16.17. DNS malformed;
 - 2.14.16.18. Bad ICMP Frame;
 - 2.14.16.19. Bad ICMP Checksum;
 - 2.14.16.20. ICMP Frame too Large;
 - 2.14.16.21. Header Length Too Short;

- 2.14.16.22. Bad TCP Checksum;
- 2.14.16.23. Bad TCP Flags;
- 2.14.16.24. Ataques de reflexão;
- 2.14.17. Ataques DDoS que utilizem novas técnicas que venham a ser desenvolvidas durante a vigência do contrato;
- 2.14.18. O serviço deve detectar e bloquear ataques baseado em análise comportamental;
- 2.14.19. O serviço deve ser capaz de identificar origens IP forjadas;
- 2.14.20. O serviço deve possuir mecanismos para diferenciar entre usuários humanos e botnets;
- 2.14.21. O serviço deve ser ajustado sempre que novas formas de ataque se tornarem públicas;

2.15. Interface de Gerência Web, Monitoração e Logs

- 2.15.1. O serviço deve prover interface de gerência Web que forneça acesso a todos os serviços disponíveis, como a detecção de DdoS, visualização de tráfego, política e mitigação;
- 2.15.2. O serviço deve possuir um Dashboard que faça sumarização dos ataques em tempo real;
- 2.15.3 O serviço deve permitir a utilização de usuários com perfis de acesso de somente leitura e administrativo;
- 2.15.4. O serviço deve mostrar o número de ataques e os endereços IPs que participam do ataque;
- 2.15.5. O serviço deve disponibilizar via interface de gerência WEB informações pós-incidente com o mínimo de 30 dias consecutivos contendo as informações:
 - 2.15.6.1. Eventos registrados;
 - 2.15.6.2. Vetores de ataque;
 - 2.15.6.3. Origens do ataque identificados;
 - 2.15.6.4. Destino do ataque identificados;
 - 2.15.6.5. Tráfego bloqueado e liberado;
 - 2.15.6.6. Regras de acesso e bloqueio acionadas;
 - 2.15.6.7. Bloqueios por pontos de operação do serviço;
 - 2.15.6.8. Critério de identificação do fluxo malicioso;
 - 2.15.6.9. Estatísticas do fluxo malicioso;
 - 2.15.6.10 Monitoração do fluxo nas listas de acesso;

- 2.15.7. Integração com Grafana hospedado na rede Serpro sem necessidade de scripts e rotinas paralelas;
- 2.15.8. Capacidade de realizar a captura de tráfego em tempo real nos pontos de operação e acesso do serviço nos padrões do Wire Shark (PCAP);
- 2.15.9. O serviço deve possuir interface intuitiva, com a capacidade de trabalhar com políticas distintas para diferentes redes protegidas;
- 2.15.10. O serviço deve prover interface de gerência Web que suporte no mínimo os navegadores os Mozilla Firefox ESR 45 e Google Chrome versão 72, Microsoft Edge, Safari e superiores;
- 2.15.11. O serviço deve ter capacidade de analisar eventos com atraso máximo de 1 (um) minuto e opção de geração de relatórios durante a avaliação do tráfego;
- 2.15.12. O serviço deve possuir dashboard com gráficos estatísticos da disponibilidade do serviço;
- 2.15.13. O serviço deve suportar os registros das operações do sistema e das ações de início e término de sessão (login);
- 2.15.14. O serviço deve possuir uma trilha de auditoria para que as alterações de configurações sejam mostradas quando necessário, informando quando foram executadas e por qual usuário;

3. Da fiscalização dos serviços pelo Serpro e dos níveis de serviço

3.1. Suporte Técnico e Atualização

- 3.1.1. O suporte técnico e atualização contemplarão atendimento técnico quanto à configuração e solução de problemas envolvendo o produto fornecido, bem como a atualização de novos recursos no serviço contratado;
- 3.1.2. O serviço de atualização deve incluir correções ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades do serviço contratado;
- 3.1.3. A cada nova versão ou atualizações do serviço, a CONTRATADA deve apresentar as novas funcionalidades para o SERPRO que analisará a adesão de novas funcionalidades, não haverá nenhum ônus adicional pela adesão das novas funcionalidades;
- 3.1.4. Nas intervenções corretivas, em que haja risco de indisponibilidade total ou parcial, o SERPRO deve ser previamente notificado;

3.2. Do Nível de Disponibilidade e Sancionamentos

- 3.2.1. A garantia de disponibilidade operacional do serviço deve ser realizado conforme critérios abaixo:

3.2.1.1. A Disponibilidade Mensal do Serviço (DMS), para o serviço e seus componentes, conforme especificações contidas neste documento deve ser de 99,99% (noventa e nove vírgula noventa e nove por cento);

3.2.1.2. A Disponibilidade Mensal do Serviço apurada será calculada pela seguinte fórmula:

3.2.1.2.1. $DMS (\%) = (1 - (\text{Tempo Total de Interrupção Mensal} / \text{Tempo Total Mensal})) \times 100$;

3.2.1.3. Dever ser entendida como “Tempo Total de Interrupção Mensal” a soma de todos os tempos (em minutos) entre a(s) formalização(ões) do(s) registro(s) o(s) chamado(s) e a completa solução do(s) problema(s) com o respectivo fechamento entre o SERPRO e a CONTRATADA, desde que não seja constatada responsabilidade do SERPRO.

3.2.1.3.1. O SERPRO fará a formalização do registro de chamado nas seguintes situações:

3.2.1.3.1.1 A impossibilidade de direcionamento de tráfego para o centro de limpeza da CONTRATADA, causados por problemas da CONTRATADA; 3.2.1.3.1.2. A impossibilidade de entrega do “tráfego limpo” (tráfego mitigado) para o SERPRO, causados por problemas da CONTRATADA;

3.2.1.3.1.3. A indisponibilidade das ferramentas de visibilidade e administração do serviço;

3.2.1.3.1.4. O não atendimento a qualquer um dos indicadores técnicos descritos neste documento;

3.2.1.4. Ocorrências que se repitam em um período de menos de 03 (três) horas serão consideradas problemas intermitentes, sendo considerado o tempo decorrido entre a primeira e a última ocorrência para efeito de cálculo do tempo de interrupção; 3.2.1.5. Não serão computadas no cálculo do DMS, 2 (duas) interrupções anuais do serviço, agendadas, em comum acordo, com antecedência mínima de 15 (quinze) dias corridos, ou outro período concedido pelo SERPRO, sendo de no máximo 4 (quatro) horas de duração;

3.2.1.6. Falhas na infraestrutura sob responsabilidade do SERPRO, que comprometam a disponibilidade do Serviço contratado, não acarretarão ônus à CONTRATADA; 3.2.1.7. A CONTRATADA deve garantir a mitigação de uma vazão de no mínimo 95% (noventa e cinco por cento) do throughput contratado, considerando para este cálculo a carga de todos os protocolos utilizados pelo SERPRO, independente de falhas em rotas alternativas. O não atendimento a este item será entendido como indisponibilidade do serviço;

3.3. Penalidades

3.3.1. As sanções serão aplicadas pelas indisponibilidades acumuladas no mês, conforme tabela abaixo:

| Indicador | Disponibilidade | Penalidade |
|---|------------------------------|--|
| Disponibilidade Mensal do Serviço (DMS) | $\geq 99,90\%$ | ISENTO |
| | $< 99,90\%$ e $\geq 99,80\%$ | Multa de 1% (um por cento) do valor total dos serviços prestados do mês de ocorrência. |
| | $< 99,80\%$ e $\geq 99,70\%$ | Multa de 2% (dois por cento) do valor total dos serviços prestados do mês de ocorrência. |
| | $< 99,70\%$ e $\geq 99,60\%$ | Multa de 3% (três por cento) do valor total dos serviços prestados do mês de ocorrência. |
| | $< 99,60\%$ e $\geq 99,50\%$ | Multa de 4% (quatro por cento) do valor total dos serviços prestados do mês de ocorrência. |
| | $< 99,50\%$ | Multa de 5% (cinco por cento) do valor total dos serviços prestados do mês de ocorrência. |

3.3.2. Nos casos em que a disponibilidade for menor que 99,5%, será aplicada penalidade cumulativa de 2% (dois por cento) para cada 1% a menos de disponibilidade.

3.4. Modalidade de Atendimento e Prazos

3.4.1. Quando houver redirecionamento de tráfego do SERPRO para o centro de limpeza da CONTRATADA, a CONTRATADA deve realizar a mitigação de ataques de forma automática e proativa para, no mínimo, os ataques listados neste instrumento, e deve notificar o SERPRO por telefone e correio eletrônico em até 10 minutos a partir do início do ataque, por telefone e correio eletrônico, informando o tipo e o(s) alvo(s) do ataque;

3.4.2. Para os casos em que não for possível a mitigação automática e for acionada manualmente, através de redirecionamento do tráfego via BGP, após a efetivação da nova rota para a CONTRATADA, a CONTRATADA terá até 5 (cinco) minutos para iniciar a mitigação;

3.4.3. O SERPRO poderá solicitar a mitigação do tráfego destinado a CONTRATADA para um único IP específico, conjunto de IP ou range de IP; 3.4.4. O SERPRO poderá solicitar regras de mitigações específicas de acordo com sua necessidade;

3.4.5. Não haverá limitação na quantidade de mitigações de ataques e do volume de tráfego a ser tratado durante o período de vigência contratual;

3.4.6. A CONTRATADA terá o prazo de até 15 (quinze) minutos para realizar as alterações a partir da solicitação formal do SERPRO, bem como a resolução do problema relatado através dos canais de atendimento;

3.4.7. A CONTRATADA deverá disponibilizar um Centro Operacional de Segurança (SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento,

detecção e mitigação de ataques no regime de 24x7 (vinte quatro por sete) durante 365 (trezentos e sessenta e cinco) dias do ano, visando o atendimento ao ambiente em operação do SERPRO e suas equipes durante todo o período do contrato; 3.4.8. A funcionalidade de mitigação de ataques deve ser mantidas em operação ininterrupta durante 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual;

3.4.9. Caso seja constatado que o tráfego de DDoS que deve ser bloqueado não tenha sido bloqueado na rede da CONTRATADA após o tempo definido nas subcláusulas 3.4.1 e 3.4.2, o tempo de duração do ataque não bloqueado será contabilizado como indisponibilidade do serviço;

3.4.10. Caso seja constatado que o tráfego legítimo tenha sido bloqueado indevidamente por mau funcionamento do serviço da CONTRATADA, o tempo de duração do bloqueio indevido será contabilizado como indisponibilidade do serviço;

3.5. Chamados, Registro e Início de Prazos

3.5.1. O atendimento aos chamados deve conter no mínimo as seguintes informações:

3.5.1.1. Número de acionamento;

3.5.1.2. Descrição da ocorrência;

3.5.1.3. Localidade;

3.5.1.4. Severidade;

3.5.1.5. Nome do responsável do SERPRO pela abertura do chamado;

3.5.1.6. Data e hora de abertura do chamado;

3.5.1.7. Data e hora do início do atendimento;

3.5.1.8. Tipo do atendimento;

3.5.1.9. Data e hora de encerramento;

3.5.1.10. Descrição da resolução adotada;

3.5.2. O chamado será registrado na CONTRATADA, recebendo uma identificação para acompanhamento, controle e histórico;

3.5.4. Atendimento a chamados

3.5.4.1. A CONTRATADA deve prover acesso para suporte técnico do serviço, sem ônus adicional para o SERPRO;

3.5.4.2. Os chamados devem ser atendidos em conformidade com os requisitos definidos neste documento;

3.5.4.3. O tempo definido na subcláusula 3.4.6 abrange o tempo decorrido desde a abertura do chamado até seu fechamento;

3.5.5. Canais de Atendimento

3.5.5.1. Atendimento por meio site da Internet, através de portal para abertura de chamados, e de canal telefônico gratuito 0800 ou tarifação reversa, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana;

3.5.6. Entrega Mensal de Relatórios

3.5.6.1. Mensalmente deve ser entregue relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período;

3.5.6.2. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, localidade, severidade, nome do responsável do SERPRO pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, tipo do atendimento, data e hora de encerramento, descrição da resolução adotada, Tempo Total de Interrupção Mensal, Tempo Total Mensal, Disponibilidade Mensal do Serviço e tempo de redirecionamento de tráfego;

3.5.6.3. O relatório deve ser entregue mesmo quando não houver chamados no período;

3.5.6.4. A entrega do relatório deve ser realizada até o quinto dia útil do mês subsequente;

3.5.6.5. A entrega dos relatórios mensais será condição necessária para o SERPRO realizar o recebimento definitivo dos serviços e o respectivo pagamento.