ANTIDDOS-CUSTOM

DESCRIÇÃO DO PRODUTO

1. SERVIÇO ANTIDDOS-CUSTOM

O objetivo do serviço é atuar de forma inteligente criando uma camada de proteção no link de internet capaz de identificar, analisar e mitigar os ataques específicos de negação de serviço.

O AntiDDoS-Custom atua exclusivamente em links IP Internet fornecidos pela Telefonica. Não faz parte do escopo a atuação sobre links e soluções de outros fornecedores.

O serviço é composto por 4 processos:

Monitoramento

A primeira característica do serviço é o monitoramento de tráfego dos Clientes. Utilizando equipamentos que analisam o tráfego do Backbone IP da Vivo Empresas através da coleta de estatísticas por Netflow/cflowd dos seus roteadores (Vivo Empresas), o serviço caracteriza-se pela não necessidade da instalação de equipamentos na rede CLIENTE ou de desvio de todo o tráfego para um centro de análise quando não existe ataque em andamento. Além disso, visando proteger a confidencialidade das comunicações dos Clientes, esta monitoração é passiva e não intrusiva, pois analisa unicamente informações estatísticas do tráfego e não seu conteúdo.

Esta funcionalidade do serviço não introduz nenhum ponto de falha adicional na infraestrutura do CLIENTE, assim como não afeta a disponibilidade de seus serviços de conectividade. Em caso de falhas na infraestrutura de monitoração, o único ponto afetado será a capacidade de detectar ataques DDoS.

Os ataques DDoS distribuídos são gerados a partir de vários pontos geográficos da Internet, podendo ser de vários países diferentes ou de dentro do mesmo país, apesar do primeiro cenário ser o mais frequente. Considerando isto, a monitoração é realizada utilizando as seguintes estratégias:

- Nacionalmente, nos pontos de acesso da rede em que o tráfego é entregue ao CLIENTE;
- Nacionalmente, nos pontos de interconexão da rede IP de trânsito nacional, possibilitando a detecção de ataques nacionais e internacionais provenientes de outras operadoras que estejam direcionados para rede da Vivo Empresas;
- Nas conexões com backbone internacional, visando a detecção dos ataques iniciados em vários países de forma coordenada;
- Esta estratégia e modelo de monitoração somente permite que o serviço seja ofertado para Clientes que possuam conectividade internet através do serviço IP Internet da Vivo Empresas, e não de outros provedores. Consequentemente, para Clientes multi-homed, isto é, conectados a dois ou mais provedores, o serviço somente poderá ser oferecido para as conexões IP Internet da Vivo Empresas.

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

Detecção

A mitigação de ataques pode ocorrer após o processo de detecção proativa realizado automaticamente pela plataforma do serviço ou após notificação pelo CLIENTE:

- Detecção proativa:

No caso em que o SOC da Telefónica Tech detecte um possível ataque com destino aos blocos de rede do CLIENTE, ela contatará aos responsáveis designados pelo CLIENTE, para verificar a condição de ataque, avaliar conjuntamente a informação disponível e solicitar autorização parar iniciar o processo de mitigação.

Esta detecção é realizada automaticamente pela plataforma quando há a identificação de anomalia de tráfego com base em dois processos de detecção do perfil do tráfego dos serviços monitorados:

Baseline: nos primeiros 15 dias de monitoramento do serviço a plataforma identificará o perfil habitual de tráfego do CLIENTE que avalia, entre outros indicadores, a quantidade de pacotes por segundo e/ou em bits por segundo;

Template de monitoração: são os indicadores máximos (thresholds) para geração de alertas definidos pelo CLIENTE e configurados na plataforma pelo SOC Telefónica Tech.

Para otimizar o processo de detecção proativa de ataques, o CLIENTE deve manter o SOC da Telefónica Tech atualizado sobre quaisquer alterações em sua rede, seja na lista de blocos IP monitorados, serviços anunciados ou no perfil de uso da banda do link monitorado. Em caso de alterações no monitoramento do serviço, é necessário um prazo mínimo de 15 dias para que a plataforma possa atualizar o perfil habitual de tráfego do CLIENTE (baseline) e garantir a precisão nos processos de detecção e de mitigação de ataques. Em caso de alteração do perfil do tráfego do cliente sem aviso prévio pelo Cliente ao SOC Telefónica Tech, seja por conta de uma campanha, alteração de blocos de redes ou serviços monitorados, não será possível garantir a eficiência nos processos de detecção e de mitigação.

O serviço é capaz de detectar e mitigar ataques com tráfego criptografado cujos pacotes não estão em conformidade com a RFC dos protocolos (abuso de protocolo).

- Detecção reativa:

No caso que o CLIENTE detecte uma anormalidade no comportamento dos seus blocos IP monitorados, utilizando-se de seus próprios sistemas, deverá contatar o SOC da Telefónica Tech para solicitar a análise e, se necessário, iniciar um processo de mitigação. Somente os contatos autorizados pelo CLIENTE poderão informar ao SOC da Telefónica Tech a suspeita de um ataque e ativar a mitigação.

Uma vez estabelecido o contato, o SOC da Telefónica Tech e o CLIENTE avaliarão conjuntamente a informação disponível e, em caso de confirmar o ataque, o SOC da Telefónica Tech solicitará autorização para iniciar a mitigação.

O serviço Proteção DDoS, através da coleta de dados estatísticos dos roteadores do Backone IP da Vivo Empresas, oferece unicamente a detecção Proativa de ataques volumétricos, sejam eles massivos ou de exaustação de recursos. Não poderão ser detectados aqueles ataques que não provoquem variações significativas no seu perfil habitual de tráfego (baseline) em quantidade de bits ou pacotes por segundo,

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

e/ou que não atinjam os thresholds definidos pelo CLIENTE com o apoio do SOC da Telefónica Tech para geração de alertas e/ou aqueles no qual o componente malicioso esteja incluso no payload dos pacotes. Nestes casos, é requerida a colaboração do CLIENTE para detectar os possíveis ataques e contatar o SOC da Telefónica Tech para coordenar as ações necessárias para a mitigação (Detecção Reativa).

A detecção automática dos ataques de nível de aplicação ou com baixo volume de bits ou pacotes por segundo, assim como para a análise e mitigação de ataques com tráfego criptografado cujo conteúdo malicioso esteja contido no payload dos pacotes, requerem soluções específicas para este fim pois geralmente exigem o monitoramento e análise de todo o tráfego e não apenas estatístico. Esse tipo de escopo é atendido por meio da instalação de softwares e/ou equipamentos adicionais na infraestrutura do CLIENTE, o que não será parte da oferta padrão deste serviço.

Os alarmes são registrados no sistema de trouble ticketing para sua consequente avaliação por parte do SOC Telefónica Tech. O serviço tem a capacidade de oferecer a mitigação efetiva de ataques DDoS que se utilizam de tráfego não criptografado. Levando em consideração aqueles que são qualificados com severidade Alta e Média, os analistas do SOC verificam se realmente existe um ataque em curso. Quando a avaliação é positiva, o SOC entra em contato o CLIENTE.

Antes dos períodos indicados acima como necessários para criação ou alteração do perfil habitual de tráfego não é garantida a eficiência dos processos de detecção e de mitigação.

Mitigação

O processo de mitigação inicia-se somente após a autorização explícita do CLIENTE. Além de reduzir os efeitos negativos do ataque (indisponibilidade da conectividade ou de algum serviço), a tecnologia utilizada e o modelo de operação do serviço dispõem de capacidade para garantir um tempo de reação máximo. Este tempo se divide da seguinte maneira:

- T detecção:

o Detecção proativa: o tempo que transcorre desde que se gera o primeiro alerta do nível medium associado a um ataque até que o SOC avalie a incidência como possível ataque e tente comunicar com o CLIENTE;

o Detecção Reativa: o tempo que transcorre desde que o CLIENTE comunica ao Service Desk do serviço que está vivendo uma anomalia que considera como ataque DDoS até que a equipe do SOC analise a situação, verifique que se trata de um ataque e o entre em contato com o CLIENTE;

- T autorização: tempo necessário para o CLIENTE autorizar a mitigação do ataque, desde solicitação até sua autorização;

O SOC se encarrega de realizar uma análise detalhada do alarme identificando as características do ataque e quais as contramedidas que deverão ser utilizadas. Após o início da mitigação for iniciada, é realizada uma nova análise do efeito da mesma. Nesse momento, ajustes mais finos podem ser feitos ou novas contramedidas podem ser ativadas caso seja necessário.

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

É importante destacar que o atacante, quando detectar que o Serviço Web do CLIENTE foi recuperado, tentará alterar a técnica de ataque, portanto o SOC e o CLIENTE deverão seguir em contato para verificar se a mitigação continua sendo efetiva até o final do ataque.

Ainda dentro do contexto da mitigação, estão contemplados os seguintes conceitos:

o Janela de mitigação: duração máxima de mitigação antes de ser contabilizada uma nova mitigação.

o Desativação da mitigação: tempo máximo para que o SOC da Telefónica tech desative o desvio de tráfego para as plataformas de mitigação por um período de até 2 (duas) horas após o término de um ataque.

o Intervalo entre mitigações: tempo máximo entre uma mitigação e outra antes de ser contabilizada uma nova mitigação.

- Mitigação inteligente

Uma vez que se confirme o ataque e que o CLIENTE autorize, será ativado o processo de mitigação. O processo consiste em:

o Desviar os fluxos de tráfego direcionado para os blocos de rede alvos do ataque para as plataformas de mitigação;

o Identificar o tráfego de ataque e descartá-lo, permitindo que o tráfego legítimo flua normalmente para a rede do cliente;

o Entregar o tráfego legítimo ao seu destino final.

- Comunicação durante o processo de mitigação

o O SOC manterá o contato com o CLIENTE para informar sobre o ataque e o estado da mitigação.

o Caso seja necessário se poderá estabelecer uma comunicação de áudio direta junto ao CLIENTE para melhor resolução do problema.

o O SOC da Telefónica Tech notificará ao CLIENTE cada vez que se detectem mudanças significativas no perfil do ataque e/ou nas contramedidas de mitigação adotadas.

o O ataque é considerado encerrado quando não houver mais identificação de tráfego ilícito pelas plataformas de mitigação. Após o encerramento do ataque a Vivo Empresas poderá manter o tráfego desviado para as plataformas de mitigação por um período máximo de até 2 horas. O SOC da Telefónica Tech informará previamente ao CLIENTE sobre desativação da mitigação.

Em caso de comprometimento da infraestrutura da Vivo Empresas devido a ataques simultâneos aos Clientes do serviço Proteção DDoS, a prioridade de mitigação será a Vivo Empresas, visando sempre manter a infraestrutura de serviços disponível, proporcionando qualidade aos serviços prestados aos Clientes.

- Reinserção do tráfego

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

Para que o serviço seja completamente transparente para os Clientes, o desvio e a reinserção do tráfego são realizados por meio de anúncio BGP/32 que se propaga dentro do backbone IP da Vivo Empresas. Essa técnica permite o encaminhamento do tráfego dos blocos de rede atacados para as plataformas de mitigação e a devolução do tráfego limpo para a rede do CLIENTE.

- Finalização da mitigação

A mitigação será interrompida a qualquer momento, mediante solicitação do CLIENTE ou após decorridas 2 horas do encerramento do ataque.

Relatórios

- Relatório de ataque mitigado

Uma vez finalizada a mitigação, o SOC da Telefónica Tech iniciará o preparo de um relatório sobre o volume e as características do ataque, sua evolução e as medidas tomadas para mitigá-lo, contemplando as seguintes informações:

o Tempo de início e fim do ataque, conforme registrado na ferramenta (mitigação proativa) ou notificado pelo CLIENTE (mitigação reativa);

o Tempo de início e fim da mitigação;

o Tipo do ataque e sua evolução (considerando que os atacantes tenham utilizado várias técnicas durante o ataque);

o Gráfico com a evolução temporal do tráfego dos ataques desde seu início até seu fim;

o Tempo de ativação de cada contramedida e respectiva avaliação de sua efetividade até a resolução definitiva do incidente;

o Tipo de detecção: proativa (SOC Telefónica Tech) ou reativa (CLIENTE).

Os relatórios de ataque mitigado serão disponibilizados manualmente ao CLIENTE pelo SOC de Clientes (através de e-mail).

- Relatório de tráfego

A monitoração do tráfego do CLIENTE também pode oferecer informações de valor ao CLIENTE, independentemente se houve ou não ataques no período em questão. As seguintes informações são disponibilizadas:

o Estatísticas sobre o volume de tráfego dividido por aplicação (especificada através de protocolo e porta);

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

o Distribuição dos países que geram maior volume médio e máximo (pico) de tráfego para CLIENTE;

o Resumo de mitigações ocorridas desde o inicio do contrato do CLIENTE, caso tenham ocorrido.

Estes relatórios agregam um valor adicional ao serviço, principalmente aos Clientes que não são alvos frequentes de ataques, pois confirmaria como o serviço está sempre em execução e protegendo suas redes. Os relatórios de tráfego serão disponibilizados ao CLIENTE pelo SOC da Telefónica Tech (através de e-mail) mensalmente.

A Vivo Empresas possui responsabilidade de mitigar o volume de tráfego contratado, em consonância com o plano de serviços adquirido pelo Cliente. Entretanto, importante enfatizar que, em havendo um ataque cibernético que ultrapasse o volume de tráfego contratado, a Vivo Empresas não terá responsabilidade direta ou indireta por eventuais danos sofridos pelo Cliente.".

1.1 VANTAGENS DA SOLUÇÃO

A solução AntiDDoS-Custom da Vivo Empresas apresenta as seguintes vantagens:

- Solução não intrusiva: como a instalação acontece na própria rede da Vivo Empresas, a mesma não necessita de alterações na rede do CLIENTE;
- Diferencia o tráfego malicioso do legítimo: se comparada a outras soluções do mercado que descartam todo o tráfego (legítimo e malicioso) em caso de ataque, o serviço Proteção DDoS da Vivo Empresas é capaz de limpar o tráfego permitindo a passagem daquele legítimo;
- Preserva a conectividade: preserva a conexão de Internet e impede que tráfego malicioso interrompa ativos críticos para os negócios do CLIENTE;
- Mínima latência: O desvio de tráfego para sua mitigação é realizado dentro da rede local da Vivo Empresas, minimizando a latência introduzida pela solução;
- Disponibilidade: a solução da Vivo Empresas é redundante, sem custos adicionais para o CLIENTE;.

1.2 FACILIDADES

O serviço é baseado em 2 (dois) centros de mitigação localizados no Brasil, com capacidade agregada para mitigar até 120 Gbps de tráfego, é possível garantir ao cliente as melhores práticas de mercado, combinando a flexibilidade de um parceiro local com a robustez de uma operadora global.

1.3 SERVIÇOS ADICIONAIS

N/A

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

2. SLA DE DISPONIBILIDADE

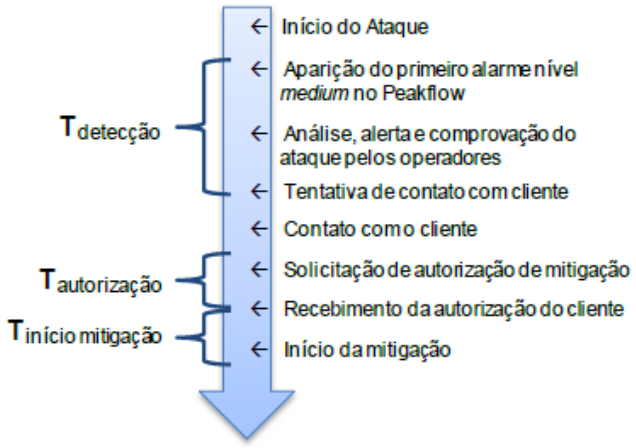
O prazo máximo para disponibilização do serviço de AntiDDoS-Custom será de até 60 dias (sessenta dias), após instalação do acesso, salvo negociação específica com as áreas operacionais a ser realizada durante a fase de elaboração da proposta. Este prazo não contempla a disponibilização de equipamentos, no caso de vendas ou locação, assim como os prazos de instalação de links de dados, quando inclusos nos projetos. Limitações ou situações específicas de cada CLIENTE e projeto podem causar variação nos prazos estabelecidos.

Ao finalizar o período de provisão do serviço, o CLIENTE e Vivo Empresas acordarão testes de configuração para verificar o funcionamento correto de funcionalidade de desvio de tráfego e reinserção de tráfego e garantir que o serviço funcione corretamente. Com o objetivo de customizar os limiares de detecção para aperfeiçoar o serviço ao CLIENTE, a Vivo Empresas solicitará ao CLIENTE, informações específicas de sua infraestrutura de rede interna e equipamento de segurança existente. Tais informações serão confidenciais e não poderão ser divulgadas pela Vivo Empresas.

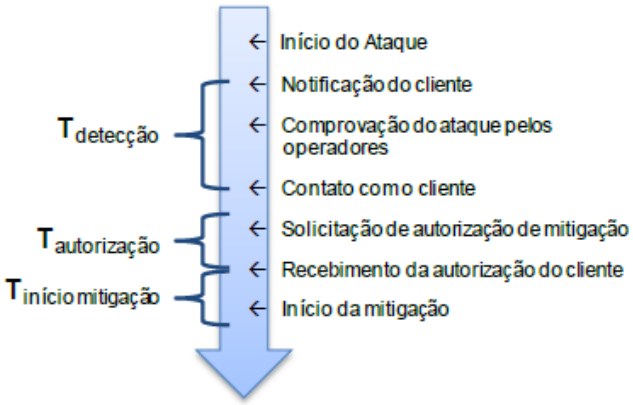
SLO de Incidentes

Para definir estes indicadores, utilizaremos os seguintes fluxos de atendimento, dependendo do tipo de detecção:

Sequência Temporal – Mitigação Proativa



Sequência Temporal – Mitigação Reativa



Mitigação - Sequência Temporal

O tempo T autorização depende exclusivamente do CLIENTE, por consequência não é considerado como medida de qualidade do serviço. Serão, portanto, sujeitos a acordos de nível de serviços os seguintes tempos:

- T detecção
- T início da mitigação

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

3. SLA DE REPARO

A Central de atendimento para abertura de chamados para reparo, funciona 24 horas, 7 dias por semana, durante todo o ano. Os contatos telefônicos são registrados em nosso sistema para acompanharmos a resolução do problema até sua finalização, mantendo atualizados o histórico e informações de contato. O contato deve ser feito no número descrito na tabela a seguir:

Central de Atendimento Corporativo Vivo	Categorização
103 15	PME, VIVO ONE E TOP
0800 0151 551	CORPORATE, ASSOCIAÇÕES, GOVERNO E TOP +

Indicador	Crítico
TEMPO DE ATENDIMENTO a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	15 min
TEMPO DE RESPOSTA a partir da aparição do primeiro alerta médium até tentativa de contato com o cliente	20 min
TEMPO DE INÍCIO DA MITIGAÇÃO a partir da autorização do cliente até a mitigação ser iniciada	15 min
TEMPO MÁXIMO DE RESPOSTA para dúvidas relacionadas a um incidente aberto, alteração de parâmetros de mitigação em andamento etc.	15 min

Indicadores de Consultas

Serão sujeitos a acordos de serviço os seguintes tempos:

- Tempo de atendimento a consultas: a partir da comunicação do CLIENTE até a atribuição do ticket a um analista do SOC
- Tempo de resolução de consultas: a partir da comunicação do CLIENTE até que o SOC comunique a resolução do mesmo

São previstas as seguintes consultas para este serviço:

- Lista de redes monitoradas;
- Alertas e mitigações;
- Informações sobre ataques recebidos;
- Lista de contatos autorizados pelo CLIENTE.

Indicadores de Solicitações

Serão sujeitos a acordos de serviço os seguintes tempos:

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

- Tempo de atendimento a solicitações: a partir da comunicação do CLIENTE até a atribuição do ticket a um analista do SOC
- Tempo de resolução de solicitações: a partir da comunicação do CLIENTE até que o SOC comunique a resolução do mesmo

São previstas as seguintes solicitações para este serviço:

- Adicionar/retirar rede do monitoramento;
- Modificação na lista de contatos autorizados do CLIENTE;
- Modificação no mapa de serviços do CLIENTE;
- Solicitação de relatório de dados do tráfego do CLIENTE monitorado em um período específico.

Indicador	Prazo
Tempo de atendimento a partir da comunicação do CLIENTE até a atribuição do ticket a um analista do SOC	1 h
Tempo de resolução a partir da comunicação do CLIENTE até que o SOC comunique a resolução do mesmo	10 h
Tempo de atendimento de solicitações a partir da comunicação do CLIENTE até a atribuição do ticket a um analista do SOC	1 h

SLO de Apresentação de Relatórios

Serão medidos os seguintes prazos:

- Prazo de entrega do relatório mensal: a partir do quinto dia do mês até o décimo.
- Prazo de entrega de relatórios de ataques: a partir da finalização do ataque até a entrega do relatório do ataque.

Indicador	Prazo
Tempo de entrega de relatórios de tráfego periódicos (mensal), conforme a modalidade.	Até 10º dia útil do mês subsequente ao período acordado
Tempo de entrega de relatório de incidente após a finalização de uma mitigação	5 dias úteis

SLO de Prestações de Serviço

Métrica	SLA	Aplica-se a
Tempo de Atendimento	95%	Consultas, requisições e incidentes
Tempo de Resposta	95%	Consultas, requisições e incidentes

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

Tempo de Notificação	95%	Consultas, requisições e incidentes
Tempo de Resolução	95%	Consultas, requisições e incidentes

Objetivo: garantir o atendimento de 95% dos SLOs por mês.

Somente se considera para efeitos de penalização:

- Incidentes Críticos e Altos;
- As requisições categorizadas como Altas pelo CLIENTE na abertura do chamado.

Assim, os itens que excedam não cumpram o SLA definido estarão sujeitos a um desconto, que serão liquidadas mensalmente pela fórmula:

$$Vpd = \frac{(Te \times 100)}{(1.440 \times Nd)}$$

Na qual:

- Vpd = percentual de minutos excedidos no respectivo mês;
- Te = tempo excedido em minutos além do determinado na tabela de SLO para o serviço em questão;
- Nd = Número de dias no mês.

Sendo constatado o não cumprimento do SLA, os índices de descontos, da tabela, abaixo, serão aplicados sobre o valor mensal a ser pago pelo cliente. Os descontos serão aplicados no mês subsequente ao mês da confirmação da ocorrência.

Percentual	Descontos %
0 < Vpd £ 2	0,5
2 < Vpd £ 4	1,0
4 < Vpd £ 6	2,5
6 < Vpd £ 10	5,0
10 < Vpd £ 20	7,5
Vpd > 20	10,0
0 < Vpd £ 2	0,5

Interrupções

A disponibilidade que garante o serviço obedece às seguintes condições:

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

- Não se contabilizarão dentro do tempo da não disponibilidade as interrupções do serviço que foram provocadas por causas imputáveis ao CLIENTE;
- CLIENTE está obrigado a facilitar o acesso a suas dependências, das pessoas designadas pela Vivo Empresas, para a resolução dos problemas, ou a operação do serviço que seja necessária. O tempo necessário para obter esta permissão está fora do cálculo da disponibilidade;
- A Vivo Empresas se reserva no direito de efetuar, mediante aviso prévio ao CLIENTE, paradas técnicas que não se contabilizam no cômputo da disponibilidade;
- São excluídas interrupções do serviço devidas a causas de força maior (por exemplo, desastres naturais).

Interrupções Programadas

As interrupções programadas de disponibilidade do serviço sejam elas pelas causas motivadas pelo item anterior, de períodos de manutenção, ou motivadas por alguma solicitação do CLIENTE, não serão contabilizadas para o cálculo da disponibilidade do serviço.

Períodos de Manutenção

Por necessidade de manutenção, pode ser necessário interromper o serviço prestado ao CLIENTE, com o objetivo de executar reconfigurações, atividades de manutenção, etc., na plataforma de prestação de serviços. Tais atividades serão executadas, necessariamente, durante um período pré-programado de manutenção.

As severidades são definidas de acordo com impacto do evento, conforme tabelas abaixo:

Incidentes de Serviço	Definição
Crítico	Incidentes que têm um impacto significativo na segurança do sistema ou dos dados. Interrupção completa do serviço ou comprometimento grave da integridade, confidencialidade ou disponibilidade. Ameaças imediatas à conformidade regulatória ou legal.
Alto	Incidentes que causam interrupções substanciais, mas não são catastróficas. Comprometimento moderado da integridade, confidencialidade ou disponibilidade. Potencial impacto financeiro significativo.
Médio	Problemas que afetam a operação, mas não causam uma interrupção significativa. Comprometimento limitado da integridade, confidencialidade ou disponibilidade. Impacto financeiro moderado.
Baixo	Questões que têm um impacto mínimo na operação e na segurança.

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.

	Comprometimento mínimo da integridade, confidencialidade ou disponibilidade. Impacto financeiro baixo ou insignificante

Telefônica Brasil - Av. Engenheiro Luís Carlos Berrini, 1376. Cidade Monções, São Paulo - SP, 04571-936.

Propriedade da telefônica. Toda e qualquer reprodução, distribuição, comunicação pública é expressamente proibida sem a sua prévia autorização. *** Clasificado PÚBLICO por TELEFÓNICA. *** Classified PUBLIC by TELEFÓNICA. *** Classificado como PÚBLICO pela TELEFÓNICA. *** Von TELEFÓNICA als ÖFFENTLICH eingestuft.