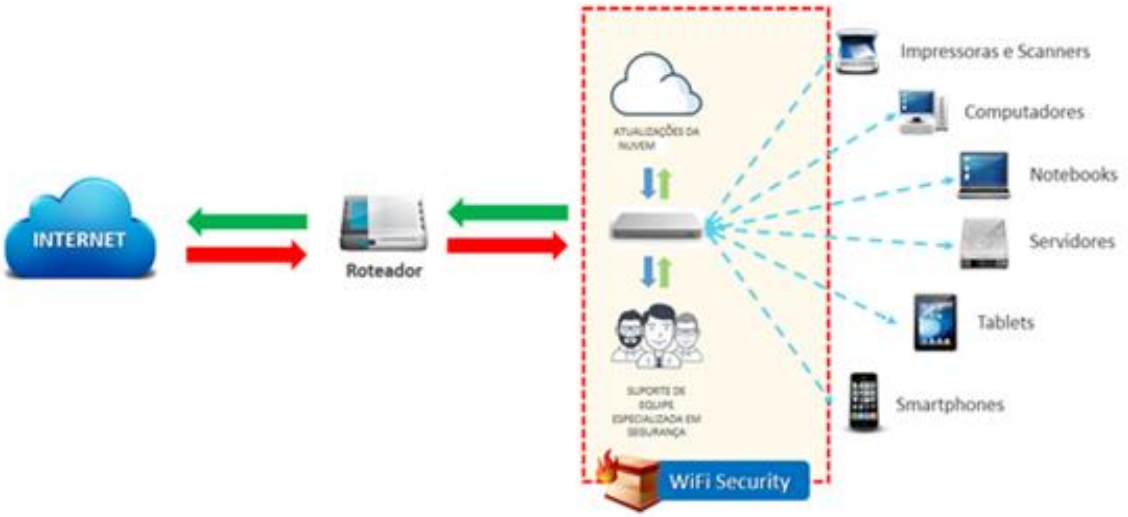
# Termo Específico do Produto

# WI-FI SEGURO

# 1 WI-FI SEGURO

Elevar a proteção de redes WiFi privadas ou públicas através de uma solução como serviço que agrega ao WiFi tradicional camadas de segurança, capazes de controlar e identificar as ameaças cibernéticas conhecidas de baixa complexidade.

Ambientes de negócio trafegam dados sensíveis para o negócio em redes WiFi, por isso, proteger essas redes é fundamental para garantir o negócio.




**IMPORTANTE >>** Conforme topologia acima, o equipamento (access point) é posicionado *"atrás do roteador"*, para filtrar o tráfego e aplicar as funcionalidades de segurança. Não é possível conectar à rede cabeada.

## 1.1 CARACTERÍSTICAS DO WIFI SEGURO

- Gestão de redes e usuários na rede WiFi;
- Visão em tempo real de todo tráfego na rede WiFi;
  - Controle de banda utilizada por cada rede WiFi;
- Criação de "Splash Page" para a autenticação de usuários em redes guest;
- Controle de portas, IPs e protocolos de interação com a Internet;
  - Regras customizadas de firewall para permitir apenas a entrada e saída de tráfego autorizado;
- Bloqueio do acesso a "Conteúdo Adulto" na Internet;
- Equipe de especialistas em segurança da informação provendo suporte ao equipamento incluindo a Manutenção do mesmo em caso de avarias que necessite a troca.

# 2 ÁREA DE COBERTURA DO SINAL WIFI

Avaliar a área de cobertura do equipamento e as características da planta onde será instalada a solução é fundamental para assegurar a qualidade, distribuição e alcance do sinal WiFi. Por isso, criamos limites claros específicos de um modelo de ambiente para *"orientar"* a definição de quantidade de equipamentos.

## 2.1 CARACTERÍSTICA DO AMBIENTE PADRÃO

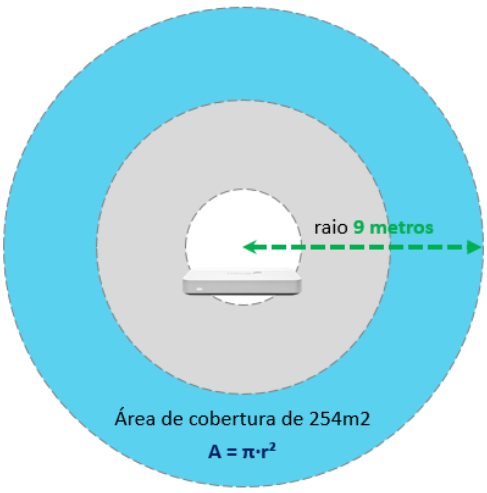
Para orientar a definição do alcance do sinal WiFi do equipamento para produto o WiFi Seguro, levamos em consideração algumas características que são fundamentais para que a solução atinja a área de cobertura necessária. Para isso, é essencial que o ambiente seja compatível ao cenário apresentado abaixo:

- ✓ A superfície do ambiente deve ser plana e sem elevações;
- ✓ Não conter obstruções como: paredes, divisórios, vidros, equipamentos ou alta concentração de pessoas;
- ✓ O pé direito do ambiente deve ser de no máximo 3 (três) metros;
- ✓ Circulação de pessoas deve corresponder aos limites estabelecidos nos planos;
- ✓ Não conter outros sinais magnéticos;
- ✓ O equipamento (access point) não deve ser posicionado em ambientes fechados, com baixa propagação de sinal.

Definir a quantidade e o posicionamento de equipamentos para garantir a cobertura de sinal WiFi na área física é de responsabilidade da contratante. A VIVO EMPRESAS não disponibiliza serviço de site survey para implantação dessa solução.

## 2.2 ALCANCE DO SINAL WIFI

Para cada equipamento é necessário considerar um alcance máximo de 9 (nove) metros de raio, com a capacidade de distribuir o sinal para uma área de até 254m2, para um ambiente conforme descrito no item 2.1. Vale ressaltar que são valores de referência e podem variar conforme ambiente da contratante. Veja exemplo na imagem abaixo:



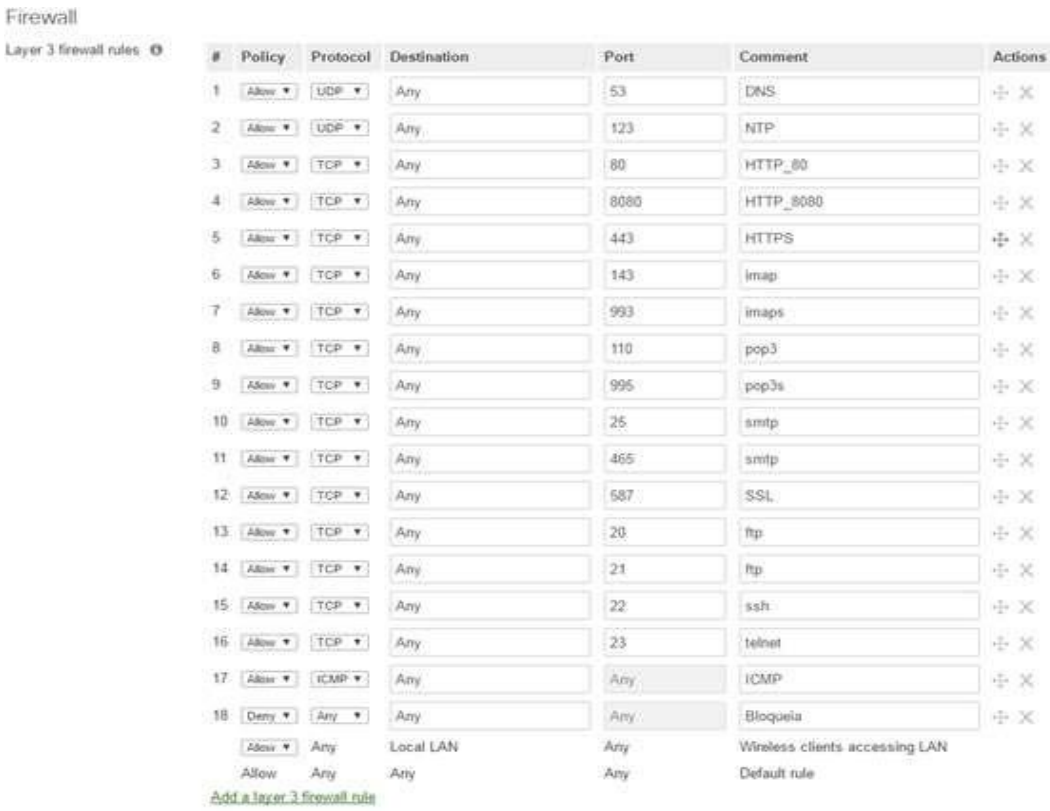
# 3 FUNCIONALIDADES DE SEGURANÇA

Dentre todas as funcionalidades de segurança disponíveis, habilitaremos as funcionalidades específicas descritas abaixo para formar diferentes camadas de proteção, cada uma com um objetivo diferente. Veja a descrição de cada funcionalidade de segurança e como será a configuração inicial.

## 3.1 CAMADA DE FIREWALL

Essa camada é responsável por determinar quais operações de transmissão e recepção de dados podem ser realizadas. Isso acontece através de regras que permitem liberar ou bloquear tráfego entre IP, porta e protocolo.

Abaixo, uma imagem ilustrativa do template de configuração inicial que será habilitado no momento da instalação para a camada de Firewall.

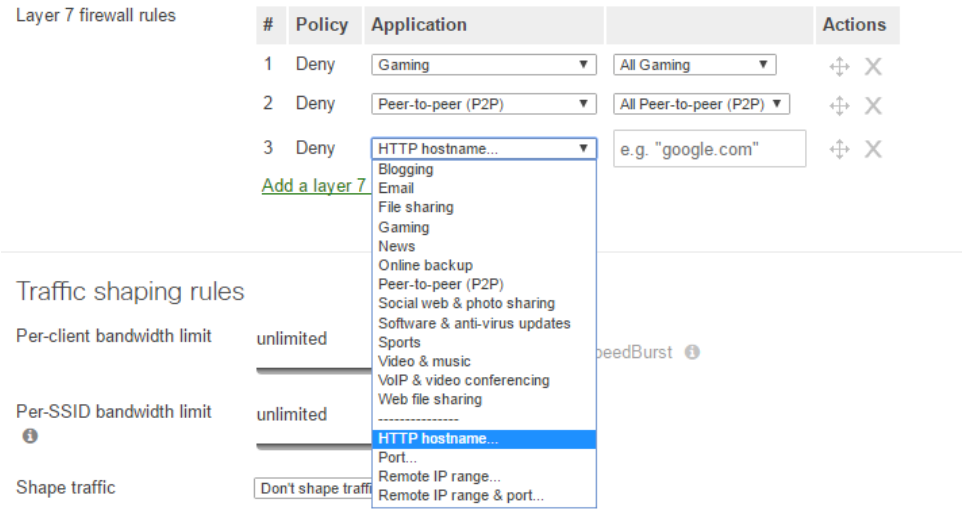



**IMPORTANTE >>** Todos as alterações e melhorias na configuração acima poderão ser realizadas através de abertura de chamados no SOC, após a instalação, na etapa de administração conforme o limite de chamados do plano escolhido pela contratante.

## 3.2 CONTROLE DE APLICAÇÃO

Essa camada é responsável por entender os recursos disponíveis em sites e aplicações, possibilitando o controle de acesso a elas.

Abaixo, uma imagem ilustrativa de como será realizada a configuração inicial:




A configuração inicial já prevê o bloqueio das categorias de “jogos” e Peer-to-peer”.

**IMPORTANTE >>** É possível realizar apenas filtro e bloqueio “blacklist”, **não** sendo possível realizar filtro de “Whitelist” com liberação de determinados sites. Todos as alterações e melhorias na configuração acima poderão ser realizados através de chamados para o SOC após a instalação, na etapa de administração conforme o limite do plano escolhido pela contratante.

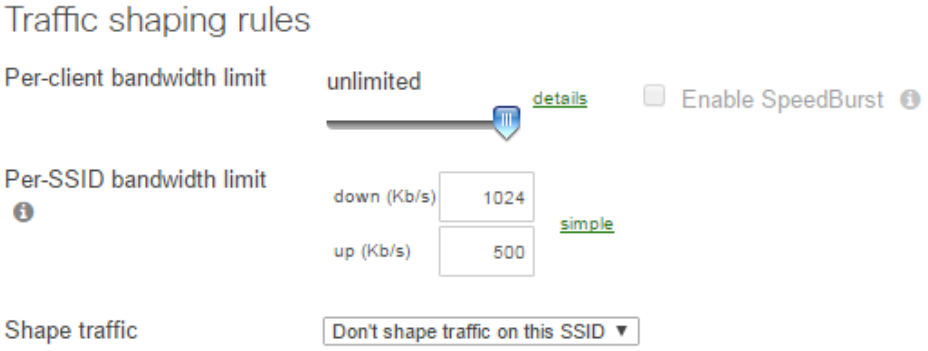
## 3.3 BLOQUEIO DE CONTEÚDO ADULTO

Essa camada é responsável por bloquear sites e aplicações que exibam conteúdo categorizado pelo fabricante como “adulto”, sendo que, é possível apenas habilitar e desabilitar esse bloqueio, conforme imagem ilustrativa abaixo.


## 3.4 TRAFFIC SHAPING

Essa camada é responsável por distribuir o tráfego dos links de internet conforme necessidade do negócios e sites e aplicações prioritárias.

A configuração inicial contempla o acesso ilimitado para os usuários do SSID da rede corporativa, e acesso restrito para usuários do SSID “Guest”, conforme imagem ilustrativa abaixo:



**IMPORTANTE >>** Aplicável apenas para os planos M ou G.

## 3.5 VPN

VPN é um termo em inglês para "V*irtual* P*rivate* N*etwork"*, e esta camada é responsável por estabelecer canais de comunicação entre dois pontos de forma privada e segura, com por exemplo, filiais se conectando a matriz, equipe em campo se conectando as filiais entre outras aplicações.

O uso de VPN IPSec possibilita o acesso à infraestrutura de forma remota através de qualquer local com acesso à Internet, permitindo customizar as políticas de acesso. Para o Wi-Fi Seguro, é possível criar novas VPNs apenas utilizando outros equipamentos concentradores de VPNs do mesmo fabricante que não estão contemplados nessa proposta, e não permitem a utilização de IP dinâmico na solução. Caso seja necessário a implementação dessa solução, necessário seguir com fluxo de projeto especial acionando seu Gerente de Negócios.

## 3.6 ARMAZENAMENTO DE LOGS

Logs são todos os eventos realizados pelos usuários através da rede WiFi e permitem obter informações históricas desse comportamento. Para isso, é necessário destinar um servidor de log ou espaço.

### 3.6.1 Visualização dos logs

O armazenamento de logs na nuvem por padrão prevê espaço limitado definido pelo fabricante da solução. Dependendo do volume de eventos gerados pela contratante, o período de armazenamento pode variar de no mínimo de 7 (sete) a no máximo 30 (trinta) dias. Caso a contratante necessite armazenar por um período maior, é a responsabilidade da contratante disponibilizar, configurar e gerenciar esses logs.

## 3.7 CONFIGURAÇÕES GERAIS

### 3.7.1 Plano P

#### 3.7.1.1 Configuração 1

**SSID 1**

- ✓ Acesso corporativo;
- ✓ Autenticação preshared (SSID e Preshared deverão ter 16 caracteres no mínimo contendo letras maiúsculas, minúsculas números e caractere especial).

#### 3.7.1.2 Configuração 2

**SSID 2**

- ✓ Acesso corporativo;
- ✓ Autenticação de preshared + usuários locais.

### 3.7.2 Plano M e Plano G

#### 3.7.2.1 SSID1

- ✓ Acesso Corporativo;
- ✓ Autenticação Preshared (SSID e PreShared deverão ter no mínimo 16 caracteres contendo letras maiúsculas, minúsculas, números e caracteres especiais);
- ✓ Prioridade de banda.

#### 3.7.2.2 SSID2

É habilitado quando necessário disponibilizar acesso de **"Guest Ambassador"** para o cliente criar usuários corporativos.

- ✓ Acesso Corporativo;
- ✓ Autenticação usuários locais;
- ✓ Prioridade de banda.

#### 3.7.2.3 SSID3

É habilitado quando é necessário disponibilizar acesso **"Guest Ambassador"** para o cliente realizar a criação e gestão de usuários na rede "Guest".

- ✓ Acesso Guest com Splash page;
- ✓ Autenticação local.

#### 3.7.2.4 SSID4

É habilitado quando o cliente tiver uma página de negócio no Facebook.

- ✓ Acesso Guest;
- ✓ Autenticação Facebook ou Google.

## 3.8 PREMISSAS E PRÉ-REQUISITOS

É imprescindível para o avanço das atividades de instalação do equipamento o comprometimento da contratante em disponibilizar os recursos listados abaixo:

- ✓ A contratante deverá informar previamente a topologia física e lógica do ambiente;
- ✓ A instalação deve ser executada em apenas uma visita, sem interrupções. Caso isso não seja possível, será cobrado da contratante um custo adicional para a finalização da instalação;
- ✓ O trabalho deve ser acompanhado por um responsável da contratante em tempo integral;
- ✓ A contratante deverá informar o nome, telefone e e-mail de um profissional habilitado a fornecer detalhes técnicos do ambiente, e que o mesmo esteja disponível para tal;
- ✓ A contratante deve prover:
    - Energia elétrica;
    - Suportes, parafusos e demais itens para a fixação caso necessário;
    - Estrutura de cabeamento para realizar as conexões;

- Sistema de refrigeração caso necessário;
- Local livre de humidade, boa ventilação e protegido contra iluminação direta do sol ou intempéries climáticas.

✓ A contratante deverá providenciar, se necessário, o acesso remoto de profissionais da VIVO EMPRESAS ao ambiente. Esse acesso remoto deverá ser realizado através de username / password únicos de forma que possam ser rastreados;

✓ Não está contemplado a instalação, configuração, atualização de nenhum outro equipamento de T.I. que não seja o equipamento contratado nessa proposta comercial;

- Não está contemplado troubleshooting para resolução de problemas ocorridos em outros equipamentos que não descritos nessa proposta técnica e comercial.

✓ O equipamento será enviado e instalado no endereço de instalação da contratante que consta na proposta comercial;

✓ Os agendamentos deverão ser feitos com no mínimo 48 (quarenta e oito) horas de antecedência ao início da atividade;

✓ Para as localidades remotas, ou seja, que dependem de transporte aéreo ou barco para acessar a localidade, os agendamentos deverão ser feitos com no mínimo 72 (setenta e duas) horas de antecedência ao início da atividade;

✓ O cliente deverá fornecer todas as informações solicitadas pertinentes e necessárias para execução do serviço.

✓ Instalação da solução está sujeito a viabilidade técnica.

## 3.9 ITENS FORA DO ESCOPO DA INSTALAÇÃO

As atividades não especificadas nesse documento serão automaticamente consideradas como “Fora de Escopo”. Além disso, ressaltamos os seguintes pontos:

✓ Fornecimento de qualquer tipo de hardware e software;

✓ Alteração ou configuração de equipamentos já instalados na rede da contratante;

✓ Migração de configurações e regras de outros equipamentos para o contratado nessa proposta;

✓ Serviços de obra civil e elétricos para viabilizar a instalação do equipamento contratado nessa proposta;

✓ Não está previsto a segunda visita ou novas instalações devidas:

- Em caso da primeira visita improdutiva, será cobrado uma taxa adicional do retorno para nova tentativa da instalação do equipamento;
- Novas instalações ou instalações adicionais por conta da aquisição de novos equipamentos que não o descrito nessa proposta;
- Mudança do endereço descrito nessa proposta ou deslocamento do equipamento para uma outra localidade física.

✓ O SOC não atua na etapa de instalação. Essa etapa é 100% conduzida pelo integrador indicado pela VIVO EMPRESAS.

## 3.10 JANELA DE INSTALAÇÃO

O serviço de instalação será executado de segunda a sexta-feira das 8h às 18h.

## 3.11 ITENS FORA DO ESCOPO

- ✓ Treinamento de usuários, administradores ou gestores;
- ✓ Suporte técnico à usuários, administradores e gestores;
- ✓ Apoio consultivo para a definição de políticas de segurança;
- ✓ Confecção de manual de uso para usuários, administradores e gestores;
- ✓ Desenvolvimento do plano de endereçamento IP, VLANs, roteamento, NAT, PAT, etc;
- ✓ Integração com Active Directory (AD) da contratante;
- ✓ Definição, customização ou implementação de plataformas de gerenciamento e monitoramento de rede e segurança;
- ✓ Definição, customização ou implementação de serviços de:
  - DNS;
  - RADIUS;
  - TACACS;
  - NTP;
  - AAA;
  - VLANs.
- ✓ Roteamento estático ou dinâmico;
- ✓ Mecanismos de qualidade de serviço (QoS).

# 4 SUPORTE E ADMINISTRAÇÃO REMOTA DO EQUIPAMENTO

Após o processo de instalação do equipamento com as configurações iniciais na infraestrutura da contratante, dá início ao processo de administração remota do equipamento, que é realizado pelo SOC, Centro de Operação de Segurança da VIVO EMPRESAS.

## 4.1 OBJETIVO DA ADMINISTRAÇÃO REMOTA

Prover expertise e equipe especializada para manter a proteção de equipamento ativa, atualizada e de acordo com a necessidade da empresa.

O serviço de administração do equipamento é prestado de forma remota através da estrutura do SOC VIVO EMPRESAS que se conecta no equipamento instalado na Infraestrutura da contratante, para realizar a administração das funcionalidades de segurança e manutenção do equipamento em casos de avarias que ocasionem indisponibilidade.

Caso a contratante suspeite do mau funcionamento do equipamento, deve-se abrir um chamado para o SOC realizar o diagnóstico do problema apresentado.

## 4.2 MÓDULO DE MANUTENÇÃO

Esta camada é responsável viabilizar um novo equipamento e uma nova instalação em caso de avarias que causem indisponibilidade no equipamento.

O SOC fará a interface entre o fabricante e a contratante para a abertura, evolução e encerramento do processo de substituição do equipamento danificado.

Este serviço também contempla a gestão dos contratos de manutenção da contratante, auxiliando-o na renovação do contrato de manutenção com o fabricante. O custo dessas renovações não está incluído na prestação do serviço e deverá ser faturado independentemente.

### 4.2.1 Atendimento e Níveis de Serviço

Abaixo, os níveis de serviço (SLA) para essa atividade:

<table>
<tr><th rowspan="2">WiFi Seguro</th><th rowspan="2">Itens</th><th rowspan="2">Abertura de um novo chamado</th><th colspan="3">Atendimento a</th></tr>
<tr><th>Incidentes</th><th>Solicitações</th><th>Consultas</th></tr>
<tr><td rowspan="2">Módulo de Manutenção</td><td>Novas solicitações de serviço</td><td rowspan="2">24x7</td><td>12x5</td><td colspan="2">8x5</td></tr>
<tr><td>RMA – Substituição do Equipamento</td><td colspan="3">8x5</td></tr>
</table>

### 4.2.2 Incidentes e Solicitações

São previstas as seguintes solicitações para este serviço:

- ✓ Manutenção do equipamento com avaria;
- ✓ Modificação na lista de contatos autorizados da contratante;
- ✓ Consulta de status do RMA (Return Merchandise Authorization) / troca de dispositivo com defeito.

### 4.2.3 Premissas & Prazos

- ✓ É necessário que o equipamento da contratante possua um contrato de manutenção ativo com a VIVO EMPRESAS ou que ainda esteja em garantia;
- ✓ O módulo de manutenção e RMA é válido apenas para os contratos que estão dentro do prazo de vigência;
- ✓ Os contratos que já excederam o prazo e estão com a vigência vencida não são elegíveis ao serviço de Manutenção (RMA);
- ✓ É importante salientar que não existe nível de serviço acordado (SLA) para o fabricante;
- ✓ O prazo máximo para a ativação de um novo equipamento é de no máximo 5 (cinco) dias úteis a partir do diagnóstico da avaria.

## 4.3 MÓDULO DE SUPERVISÃO

Serão considerados como itens indispensáveis para o módulo de supervisão:

- ✓ Supervisão da disponibilidade do equipamento;
- ✓ Canal de comunicação ao cliente via e-mail apenas quando um componente monitorado estiver indisponível.

### 4.3.1 Requisitos de Conectividade

Este serviço necessita conectividade 24x7 entre o SOC da VIVO EMPRESAS e o equipamento objeto desse documento instalado na infraestrutura da contratante.

### 4.3.2 Atendimento

Abaixo, as janelas de atendimentos para cada modalidade:

| WiFi Seguro | Abertura de um novo chamado | Atendimento a | | |
|---|---|---|---|---|
| | | Incidentes | Solicitações | Consultas |
| **Módulo de Supervisão** | 24x7 | 12x5 | 8x5 | |

#### 4.3.2.1 Solicitações e Consultas

São previstas as seguintes consultas para este serviço:

- ✓ Incidente no equipamento: indisponibilidade do equipamento administrado;
- ✓ Mapa de serviços;
- ✓ Notificação de alertas a contratante que foram gerados pela ferramenta de monitoração;
- ✓ Lista de contatos autorizados pela contratante.

### 4.3.3 Itens FORA do escopo

Não estão contemplados no escopo desse serviço os itens:

- ✓ O serviço não inclui o desenvolvimento ou a implantação de agentes personalizados de monitoração;
- ✓ O monitoramento da saúde e capacidade do equipamento, ou de outros dispositivos e componentes de rede;
- ✓ O armazenamento dos logs por prazos maiores dos informados no item 3.6 desse documento;
- ✓ Esse módulo não disponibiliza relatórios periódicos.

## 4.4 MÓDULO DE SUPORTE ESPECIALIZADO DO EQUIPAMENTO

Esta camada é responsável por realizar a administração remota do equipamento de segurança alocado na infraestrutura do ciente, buscando disponibilizar equipe especializada do SOC - Centro de operação com certificação na norma ISO 27001, que rege os processos de segurança, além da experiência e conhecimento da VIVO EMPRESAS para manter as configurações do equipamento ativas e atualizadas.

### 4.4.1 Características da Administração do equipamento

O SOC irá disponibilizar recursos especializados para realizar as seguintes atividades:

- ✓ **Participação na resolução de incidentes de segurança:** os operadores de segurança passam responder problemas relacionados as funcionalidades de descritas no item 3 desse documento;
- ✓ **Planejamento e implementação de mudanças:** contempla a avaliação e implementação de mudanças nos dispositivos por meio de solicitações da contratante, baseados nas melhores práticas de gestão. Esta atividade não contempla mudanças na arquitetura do equipamento administrado, atividades que podem ser cobertas através de um projeto especial ou consultoria de segurança adicional;
- ✓ **Resolução de solicitações feitas pelos clientes:** contempla a realização das tarefas operacionais solicitadas pelo cliente, tais como executar o backup das configurações armazenadas na nuvem, entre outros;
- ✓ **Gestão de suporte do fabricante:** o SOC será responsável por acionar o suporte do fabricante em casos em que tal apoio seja necessário;
- ✓ **Garantir o correto funcionamento do equipamento administrado:** o SOC irá monitorar funcionamento dos dispositivos, visando garantir o bom funcionamento e a disponibilidade das funcionalidades de segurança.
- ✓ **Manter e atualizar o software do equipamento:** o SOC irá atualizar o software e assinaturas de defesa sempre que recomendado pelo fabricante ou quando solicitado pelo cliente. Toda atualização será feita somente se autorizada pelo cliente, através do processo de gestão da mudança do SOC. Esta atividade inclui aplicação de patches para a correção de vulnerabilidades e prevenção de incidentes de segurança.

### 4.4.2 Atendimento

| WiFi Seguro | Abertura de um novo chamado | Atendimento a | | |
|---|---|---|---|---|
| | | Incidentes | Solicitações | Consultas |
| **Módulo de Administração** | 24x7 | 12x5 | 8x5 | |

#### 4.4.2.1 Incidentes

Os seguintes alguns tipos de incidentes podem ocorrer para este serviço:

- ✓ Incidente no equipamento: indisponibilidade ou degradação do serviço do equipamento administrado.

Caso a contratante suspeite do mau funcionamento do equipamento, deve-se abrir um chamado para o SOC realizar o diagnóstico do problema apresentado.

#### 4.4.2.2 Solicitações e Consultas

Os seguintes alguns tipos de solicitações e consultas podem ocorrer para este serviço:

- ✓ Alteração na política (regras de segurança) do equipamento;
- ✓ Modificação na lista de alterações pré-autorizadas pela contratante;
- ✓ Modificação na lista de contatos autorizados da contratante.

### 4.4.3 Requisitos Gerais

Os seguintes itens devem ser observados para a prestação de serviço:

- ✓ A gestão de todos os usuários das ferramentas que compõem a solução de gestão será para uso exclusivo da VIVO EMPRESAS;
- ✓ A autenticação para acesso administrativo aos dispositivos se dará através do serviço de autenticação da VIVO EMPRESAS.

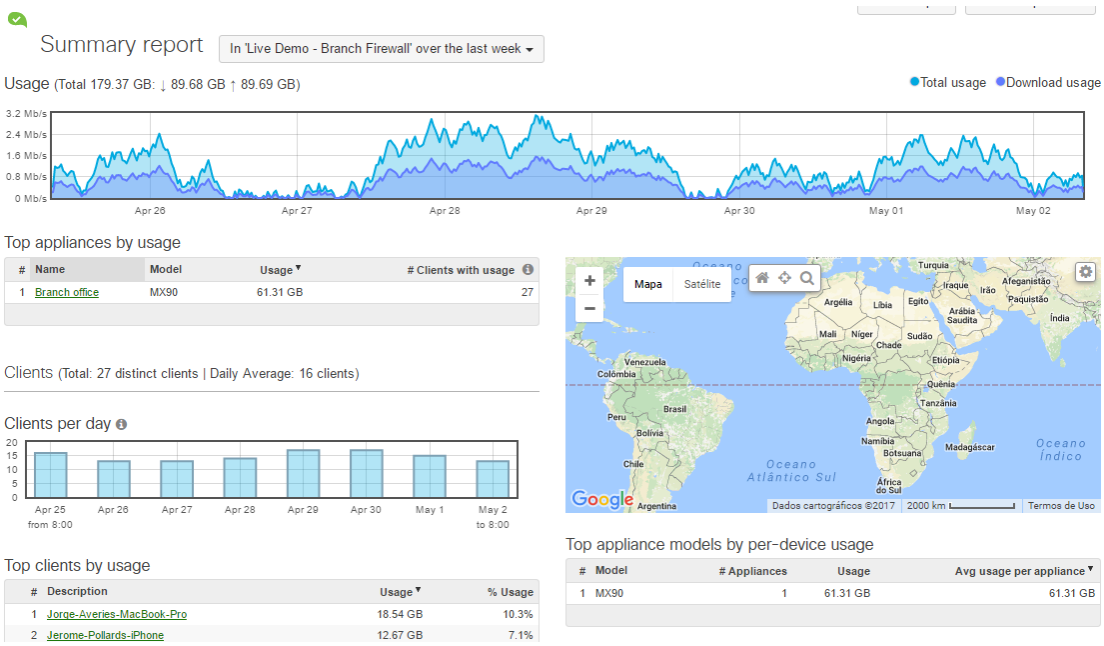
### 4.4.4 Requisitos de Conectividade

É necessária conectividade 24x7 do equipamento administrado com o SOC VIVO EMPRESAS.

## 4.5 PORTAL DO CLIENTE

O Portal do Cliente é baseado na web e irá fornecer todas as informações referentes ao equipamento, tráfego e funcionalidades de segurança ativas, através de acesso restrito, sendo necessário “login e senha” para apenas colaboradores autorizados pela empresa.

Veja uma imagem do portal meramente ilustrativa abaixo:




### 4.5.1 Gestão de Usuários

A contratante irá receber o acesso ao portal de clientes, com privilégios para gerenciar os seguintes itens:

- ✓ Incluir, excluir e alterar usuários na rede WiFi Guest;

### 4.5.2 Definições de Acesso | SOC VIVO EMPRESAS

Para alterações nas funcionalidades de segurança, a contratante deve abrir uma solicitação no SOC com detalhes da modificação, para que, nos SLA previstos nessa proposta, o chamado seja atendido pelo nosso Centro de Operação de segurança para garantir que as melhores práticas de segurança estão sendo aplicadas.

- ✓ Ajustes e configurações no console/painel do equipamento;
- ✓ Configurações relacionadas as funcionalidades de segurança;
- ✓ Criação e alteração de regras de firewall;
- ✓ Criação e alteração das configurações de “Traffic Shaping”;
- ✓ Novas configurações e regras de controle de aplicação.

#### 4.5.2.1 Itens fora do Escopo

Qualquer outra necessidade não descrita nesse termo específico deverá ser tratada como um projeto especial adicional. Veja abaixo alguns itens não contemplados.

- ✓ Controle de acesso por “mac address”;
- ✓ Configuração SSID oculto.

### 4.5.3 Característica do Portal do Cliente

#### 4.5.3.1 Tipo e Formato

Os dados estão disponibilizados em uma portal web com acesso restrito apenas aos usuários da empresa.

#### 4.5.3.2 Insumo de Dados

Os dados serão apresentados em inglês em tempo real sem intervenções humanas.

Cabe lembrar que devido este relatório ser extraído do próprio equipamento, este poderá ocasionar eventuais oscilações no tráfego devido ao incremento do processamento gerado.

#### 4.5.3.3 Idioma

Todas as informações no portal são por padrão em inglês.

## 5 PLANOS DISPONÍVEIS

A proposta comercial apresentada para a contratante pela VIVO EMPRESAS é composta pelos 3 (três) planos que consistem em configurações diferentes:

| vivo EMPRESAS | | | |
|---|---|---|---|
| **Planos Wi-Fi Seguro** | **Plano P** | **Plano M** | **Plano G** |
| Usuários Simultâneos (Recomendado / Máximo) | De 10 a 20 usuários | De 20 a 30 usuários | De 30 a 50 usuários |
| Recomendação de Banda de Link Internet | Até 100 Mbps | Até 200 Mbps | Até 300 Mbps |
| Interface para Link por Equipamento | 1 | | |
| Quantidade de SSIDs | 1 SSID | Até 4 SSIDs | Até 4 SSIDs |
| Portal de Cliente na Nuvem | Sim | | |
| Servidor de Log Adicional | Não | | |
| **2. Instalação do Equipamento** | | | |
| Instalação Básica | Instalação de um equipamento novo, considerando a configuração padrão | | |
| Política de Segurança e Configuração inicial | Sim | | |
| Integração com Lista de Usuários (AD) | Não | | |
| **3. Suporte e Administração do Equipamento** | | | |
| Número de Atendimentos (chamados) | Até 3/mês | Até 5/mês | |
| Novas regras de Firewall | Até 6/ano | Até 12/ano | |
| Novas Configurações de Traffic Shaping | N/A | Até 6/ano | |
| RMA - Manutenção do equipamento | Sim | | |

**IMPORTANTE >>** Para garantir a performance de hardware do equipamento até o final da vigência do contrato, deve ser previsto pelo gerente de vendas e a contratante a taxa de crescimento do negócio antes de escolher um dos planos acima. O indicador é deixar até 40% de hardware livre no momento da venda para prever o crescimento do negócio.

## 5.1 IMPOSTOS

Os valores com impostos contemplam, conforme legislações aplicáveis: ISS, PIS e COFINS.

## 5.2 VALIDADE DA PROPOSTA

O prazo de validade desta proposta é de 30 (trinta) dias, contados a partir da data indicada neste documento.

## 5.3 FATURAMENTO

Os serviços serão faturados mensalmente, a partir da data de aceite do serviço.

## 5.4 PRAZO DE INSTALAÇÃO

O prazo previsto para instalação do serviço é de até 90 (noventa) dias, contados após a assinatura do contrato e disponibilização dos dados necessários para a configuração dos serviços, através de cronograma a ser estabelecido de comum acordo entre as partes.

## 5.5 ÍNDICE DE REAJUSTE

Os valores descritos na proposta comercial e/ou termo de aceite serão corrigidos anualmente de acordo com a variação do Índice Geral de Preços – Disponibilidade Interna, IGP-DI, divulgado pela Fundação Getúlio Vargas.

# 6 RESPONSABILIDADES POR ATIVIDADES

As atividades listadas abaixo representam o compartilhamento de responsabilidades entre o a contratante e a VIVO EMPRESAS, considerando as etapas para a ativação do produto e a natureza de cada atividade.

O atendimento dessa matriz por ambos os lados é fundamental para garantir o cumprimento de prazos estabelecidos.

## 6.1 MATRIZ DE RESPONSABILIDADES

Legenda:

**A** APOIO **R** RESPONSABILIDADE

| ATIVIDADE | RESPONSABILIDADES | |
|---|---|---|
| | VIVO EMPRESAS | CONTRATANTE |
| **SEGURANÇA E GOVERNANÇA** | | |
| Definição das políticas e diretrizes de segurança da informação voltadas aos negócios da contratante | - | R |
| Confecção e manutenção do “mapa de rede e serviços” com a descrição da arquitetura e dos principais serviços no ambiente da contratante | - | R |
| Análise e avaliação de riscos imediatos ao ambiente gerenciado pelo SOC frente as solicitações da contratante | R | A |
| O armazenamento dos logs gerados pelo equipamento | A | R |
| **GESTÃO DE PROBLEMAS** | | |
| Centralizar problemas de usuários com estrutura de Service Desk | - | R |

| | | |
|---|---|---|
| Garantir a disponibilidade, ativação do equipamento e das funcionalidades de Segurança | **R** | **-** |
| Informar e atualizar lista de contatos da contratante para o processo de escalonamento | **-** | **R** |
| Encaminhar problemas aos grupos solucionadores da contratada | **-** | **R** |
| **GESTÃO DE MUDANÇAS** | | |
| Planejamento técnico de mudanças nos ativos gerenciados (limitado às alterações no próprio ativo) | **-** | **R** |
| Planejamento técnico de mudanças na arquitetura do ambiente da contratante | **-** | **R** |
| Validação e aprovação de todas as mudanças que provoquem impactos nos serviços e negócios em produção | **A** | **R** |
| Avaliação técnica de solicitações e demandas da contratante pertinentes ao ativo gerenciado (solicitações de regras nos firewalls, alterações Filtro de conteúdo, etc) | **R** | **A** |
| Implementação das mudanças aprovadas no escopo do serviço | **R** | - |
| Execução de testes após nova configuração / alteração | **-** | **R** |
| **MONITORAÇÃO** | | |
| Acionamento a contratada em caso de problema no equipamento | **A** | **R** |
| Configurar e suportar as ferramentas de monitoração do SOC | **R** | **-** |
| **GESTÃO DO NÍVEL DE SERVIÇO** | | |
| Definição do processo de comunicação entre a contratada**,** o fornecedor e terceiros envolvidos | **R** | **R** |
| **GESTÃO DE ACESSO** | | |
| Reset de senha de usuário no portal | **R** | **-** |
| Criação de novos usuários no portal | **R** | **-** |
| Gerencia de acesso dos usuários internos da contratante | **-** | **R** |
| Criação / remoção / alteração de perfis para acesso a console administrativa mediante a solicitação da contratante | **R** | **A** |
| **CENTRAL DE ATENDIMENTO E OPERAÇÃO** | | |
| Abertura das solicitações e chamados | **-** | **R** |
| Informação de status das solicitações e chamados | **R** | **-** |
| Indicação dos níveis de prioridades de atendimento para as solicitações e chamados | **R** | **R** |
| **GESTÃO DE LICENÇAS E SUPORTE DO FABRICANTE** | | |
| Comunicação sobre a necessidade de renovação de licenças e suporte do fabricante desde que informações do ativo sejam fornecidas pela contratante | **R** | **-** |
| Aquisição e renovação de licenças e suporte do fabricante | **-** | **R** |

## 6.2 RESPONSABILIDADES POR TIPO DE ATIVO GERENCIADO

| | | |
|---|---|---|
| **ATIVIDADE COMUNS AOS ATIVOS GERENCIADOS** | | |
| Alteração de configurações (regras, políticas, componentes, etc) mediante solicitação da contratante | **R** | **-** |
| Backup e “restore” da configuração dos ativos | **R** | **-** |
| **ATIVIDADES DE FIREWALL** | | |
| Criação / Remoção / Alteração de regras de segurança solicitadas pela contratante | **R** | - |

| | | |
|---|---|---|
| Identificação de aderência de regras com política de segurança da contratante | - | R |
| **ATIVIDADES DE FILTRO DE CONTEÚDO/PROXY** | | |
| Bloqueio de URLs mediante solicitação da contratante | R | - |
| Criação / alteração / remoção de política de acesso mediante solicitação da contratante. | R | - |
| Criação / alteração / remoção de política de controle de aplicativos mediante solicitação da contratante. | R | - |
| Instalação / Reinstalação do "agente" em máquinas de usuários | - | R |
| Criação/alteração de arquivo PAC (proxy auto configuration). | - | R |

# 7 ATENDIMENTO AO CLIENTE

## 7.1 ABERTURA DE CHAMADOS

As solicitações sobre o serviço deverão ser efetuadas a Central de Relacionamento da VIVO EMPRESAS pelo telefone **0800 151551** códigos **1620**. O atendimento é realizado 24 horas por dia, 7 (sete) dias por semana, 365 dias por ano.

A contratante poderá designar até 03 (três) administradores de sua empresa, unidade de negócio ou filial para contato com a Central de Relacionamento, os nomes deverão ser informados durante o processo de implantação do serviço. A Central de Relacionamento da VIVO EMPRESAS não efetua atendimento ao usuário final.

O SOC efetuará o acompanhamento das solicitações e das soluções dadas a contratante. A cada solicitação será associado um número de registro da chamada e quando for o caso, um nível de severidade, conforme o grau crítico do problema avaliado.

## 7.2 FECHAMENTO DO CHAMADO

O chamado somente será concluído com o aceite dado por um dos 3 (três) administradores designados pela contratante, sendo o contato efetuado por telefone ou e-mail.

## 7.3 HORÁRIO DE ATENDIMENTO

Para os serviços que possuem atendimento na modalidade 8x5, o horário de atendimento é das 08:00 às 17:00 horas de Brasília, de segunda a sexta-feira.

## 7.4 FLUXO DE ATENDIMENTO

Para controle das solicitações e da resolução das mesmas, bem como para o adequado acompanhamento do desempenho do serviço, a contratante deve instruir e garantir que não haverá interação direta de seus usuários finais com a Central de Relacionamento da VIVO EMPRESAS, sendo tal atividade atribuída apenas à equipe de suporte do cliente.

No caso de necessidade de interação com o cliente para a resolução de algum problema no equipamento, a equipe técnica do SOC, através do Centro Técnico, entrará em contato com um dos três administradores designados pelo cliente, que serão os pontos focais.

O ponto de contato do cliente sempre será a Central de Relacionamento (nível 0), seja para abrir novas solicitações, reportar problemas ou consultar o status de chamados abertos. A

Central de Relacionamento é responsável por registrar todos os chamados dos clientes. Uma vez que registrado, o chamado é direcionado para a Equipe de Supervisão do SOC (nível 1) que realiza a triagem e o primeiro atendimento, visando a resolução do chamado. Se necessário este chamado é direcionado a Equipe de Operação do SOC (nível 2) que é responsável por solucionar o chamado e, quando necessário, envolver parceiros tecnológicos (nível 3) para atender ao chamado do cliente.

# 8 SUPORTE AO CLIENTE

O SOC disponibiliza três níveis de suporte para atendimento aos serviços contratados pela contratante:

- ✓ **Suporte 1º Nível:** é o primeiro nível de atendimento do SOC para tratar solicitações de qualquer grau de severidade de chamados.
- ✓ **Suporte 2º Nível:** é um perfil profissional que é acionado pelo 1º Nível para tratar solicitações mais complexas dentro do SLA/SLO.
- ✓ **Suporte 3º Nível:** realizado pela equipe de especialistas do SOC que trabalha 8x5 (oito horas por dia, 5 dias por semana), podendo ser acionada fora deste horário pelo 2º Nível para cumprimento de SLO/SLA dos serviços.

O relacionamento com os fornecedores ou parceiros envolvidos na solução dos problemas é de responsabilidade da equipe técnica do SOC VIVO EMPRESAS.

Este item define as métricas para avaliação dos recursos e serviços disponibilizados, viabilizando a comparação dos resultados obtidos com as métricas estabelecidas, tanto em qualidade como quantidade e tempos de resposta do serviço.

## 8.1 DESCRIÇÃO DE SEVERIDADES

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

| Incidentes de Serviço | Definição |
|---|---|
| **Crítico** | Evento que indisponibiliza os serviços de um ativo classificado como crítico. |
| **Alto** | Evento que degrada os serviços de um ativo classificado como crítico ou que indisponibilidade dos serviços de um ativo não crítico. |
| **Médio** | Evento que degrada os serviços de um ativo classificado como não crítico |
| **Baixo** | Evento que não afeta os serviços. |

Critérios de Severidade – Incidentes

## 8.2 SLO DE SOLICITAÇÕES E CONSULTAS

| Serviço | Definição | Prazo |
|---|---|---|
| **Todos** | **Tempo de atendimento** a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC | 5h. |
| **Todos** | **Tempo de resposta** a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo | 30h. |

## 8.3 SLO DE RESPOSTAS

| Serviço | Definição | Prazo |
|---|---|---|
| **Todos** | **Tempo de atendimento** a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC. | 4h. |
| **Todos** | **Tempo de resposta** a partir da comunicação do cliente até que SOC faça o primeiro diagnóstico. | 8h. |

## 8.4 SLA DE PRESTAÇÃO DOS SERVIÇOS

O SLA para a família de serviços SOC segue as definições das tabelas abaixo.

| Métrica | SLA | Aplica-se a |
|---|---|---|
| **Tempo de Atendimento** | 95% | Consultas, requisições e incidentes. |
| **Tempo de Resposta** | 95% | Consultas, requisições e incidentes. |
| **Tempo de Notificação** | 95% | Consultas, requisições e incidentes. |
| **Tempo de Resolução** | 95% | Consultas e requisições. |

Tabela 1 - SLA

Somente se considera para efeitos de penalização 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:

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

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 |

Índices de descontos

## 8.5 INTERRUPÇÕES

A disponibilidade que garante o serviço obedece às seguintes condições:

- ✓ Não se contabilizarão dentro do tempo da não disponibilidade as interrupções do serviço que foram provocadas por causas imputáveis ao Cliente;
- ✓ O Cliente está obrigado a facilitar o acesso a suas dependências, das pessoas designadas pela VIVO EMPRESAS, para a resolução dos problemas no ativo de segurança descrito nessa proposta. 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).

## 8.6 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.

## 8.7 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 da contratada, não serão contabilizadas para o cálculo da disponibilidade do serviço.

# 9 GESTÃO OPERACIONAL DO CONTRATO

A prestação dos serviços pela VIVO EMPRESAS e o cumprimento do contrato a ser firmado deverão ser fiscalizados, monitorados e geridos pelas partes para fins de contínua avaliação e melhoria dos serviços prestados.

A gestão operacional do futuro contrato será feita através da gerência técnico-operacional da VIVO EMPRESAS, que deverá zelar pelo bom desenvolvimento de todos os projetos e processos ligados aos serviços prestados ao Cliente, mantendo um canal de alto nível para comunicação entre as empresas.

## 9.1 PRESTADORAS DE SERVIÇO CONTRATADAS PELA VIVO EMPRESAS

A VIVO EMPRESAS poderá contratar terceiros para a prestação dos serviços, sendo que, neste caso, ela será a única e diretamente responsável perante a contratada por todos os serviços prestados por terceiros.

## 9.2 RESPONSABILIDADES DO CLIENTE

Clientes que venham a contratar serviços da VIVO EMPRESAS irão assumir as seguintes responsabilidades:

- ✓ A contratante deverá fornecer informações suficientes com relação às suas necessidades;
- ✓ Informar a VIVO EMPRESAS com antecedência mínima de 30 (trinta) dias sobre qualquer mudança que possa afetar a prestação de Serviços
- ✓ Informar a VIVO EMPRESAS sobre qualquer mudança com relação à prestação dos serviços, com a devida antecedência, permitindo que a mesma tenha tempo suficiente para preparar e implementar as alterações necessárias, conforme tais alterações ou mudanças afetem a prestação dos serviços.
- ✓ Zelar pela conservação e correto manuseio da infraestrutura disponibilizada pela VIVO EMPRESAS, responsabilizando-se pelos eventuais danos, pessoais e materiais, decorrentes de ações e utilizações indevidas por parte de seu pessoal ou de seus equipamentos;
- ✓ Informar internamente e aos seus outros prestadores de serviços, o escopo de contrato com a VIVO EMPRESAS, quando relacionado a suas atividades.

## 9.3 RESPONSABILIDADES DA VIVO EMPRESAS

A VIVO EMPRESAS assume as seguintes responsabilidades perante os Clientes que venham a contratar seus serviços.

- ✓ Tornar disponíveis recursos VIVO EMPRESAS necessários para execução dos serviços;
- ✓ Executar os serviços de acordo com os objetivos de níveis de serviço;
- ✓ Executar todas as atividades dentro dos padrões de qualidade VIVO EMPRESAS e conforme estabelecido no contrato com o cliente;
- ✓ Cumprir os prazos estabelecidos nas atividades do projeto, desde que as responsabilidades da contratante sejam cumpridas.

# 10 PREMISSAS GERAIS

As seguintes premissas foram utilizadas para o desenho tecnológico e prestação de serviços baseada na solução para atendimento dos requisitos da contratante:

1) Para a contratação, é OBRIGATÓRIO que o cliente atenda aos limites de capacidade e serviços descritos em cada plano, considerando sua necessidade de crescimento com base no período do contrato;
2) Todos os planos disponíveis não contemplam um equipamento adicional para prover alta disponibilidade (H.A);
3) Administração das funcionalidades de segurança será realizada somente através do SOC;

a) As alterações poderão ser solicitadas via chamado para o SOC após a instalação e de acordo com o limite do plano contrato.

4) A configuração inicial de cada funcionalidade de segurança é padrão e está detalhada no item 3 desse documento. Caso na estrutura da contratante, onde os equipamentos (access points) serão instalados, existam equipamentos de segurança tal como Firewall, as configurações expostas no item 3 desse documento podem sofrer alterações.

5) Todos os SLAs de atendimento estão firmados em proposta e não podem ser alterados;

6) Para essa solução não será permitida a customização de prazos, SLA ou características dos planos diferentes descritas nesse documento;

7) O escopo da proposta não prevê consultoria especializada para investigações de incidentes que incluam outros dispositivos de TI;

8) Essa proposta não prevê passagem de conhecimento do equipamento, portal da solução e treinamento para equipe interna do cliente.