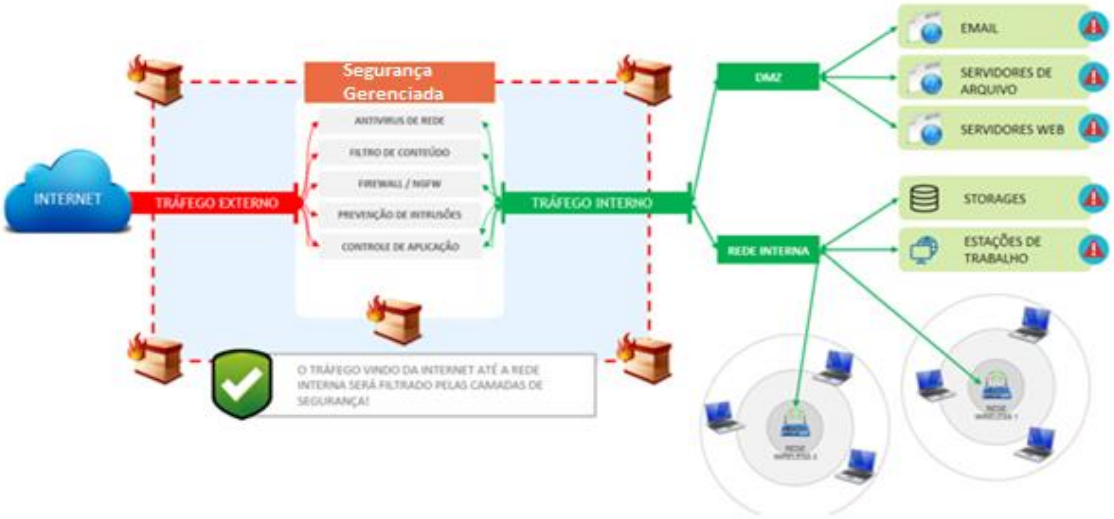
Termo Específico do Produto

Vivo Segurança Gerenciada

1 VIVO SEGURANÇA GERENCIADA | MSS – PLANOS P, M, G

1.1 PROPOSTA DE VALOR

Utilizando as principais funcionalidades de segurança, vamos instalar, configurar e administrar o equipamento na infraestrutura da contratante, para construir uma camada de proteção posicionada entre a rede interna e a internet, e através do SOC, realizar a administração remota do equipamento implementando as políticas de segurança do cliente bem como as melhores práticas de segurança para manter o perímetro seguro contra ameaças conhecidas.



IMPORTANTE >>. Conforme topologia acima, o equipamento é posicionado na *"borda"*, entre a rede interna e a internet e contempla apenas (1) uma rede LAN e uma (1) uma DMZ. Caso a estrutura da empresa tenha mais segmentações, é necessário seguir com projeto especial.

1.2 VANTAGENS DA SOLUÇÃO

- Visão completa de todo tráfego da rede entre a empresa e internet;
- Bloqueia o download de vírus no tráfego da internet;
- Permite o acesso apenas para conteúdo autorizado na Internet;
- Controla o acesso às aplicações incluindo Facebook e outras redes sociais, de forma uniforme para todos os usuários(1);
- Detecta intrusos conhecidos vindos da internet através da base de conhecimento do fabricante;
- Especialistas de segurança atuando na configuração e na supervisão da saúde do equipamento.

(1) Para aplicar este tipo de controle é necessário que os usuários que serão controlados tenha o certificado digital do firewall instalado em suas respectivas máquinas.

1.3 BENEFÍCIOS PARA O NEGÓCIO

A empresa fica mais protegida contra as ameaças cibernéticas! O ambiente de T.I passa a identificar e bloquear ameaças cibernéticas conhecidas.	**Visibilidade total do ambiente de TI e ameaças bloqueadas!** Relatórios sob demanda mostrando ameaças bloqueadas e muito mais.
Conexões seguras com terceiros, filiais e equipe em campo! Crie conexões seguras através de canais criptografados para evitar acessos indevidos as informações.	**Acessos seguro e autorizados para sites e aplicações!** Mapeia as portas para a internet e garante que apenas os usuários autorizados entrem por elas.
Mantem o rendimento através do bloqueio de vírus! Analisa os servidores para identificar e bloquear vírus trafegando pela rede.	**Aumenta a qualidade da internet através do controle de banda!** Disponibiliza mais banda para sites e aplicações importantes para aumentar o desempenho.

2 FUNCIONALIDADES DE SEGURANÇA

2.1 ANTIVÍRUS DE REDE (GATEWAY)

Vírus é um software malicioso que é desenvolvido por hackers que, tal como um vírus biológico, tenta infectar um computador, faz cópias de si mesmo e tenta se espalhar para outros computadores.

O antivírus de rede será responsável por bloquear os vírus no momento em que trafegam entre a internet e a rede interna, evitando que esses arquivos maliciosos cheguem até a estação do usuário. Importante ressaltar que não é se trata de um antivírus de “EndPoint”, não atua na remoção dos vírus do computador, apenas na identificação e bloqueio de vírus tentando acessar os servidores.

O Antivírus é destinado ao bloqueio de vírus maliciosos vindos de fora da empresa, através da internet, com o objetivo de infectar os servidores. Essa camada será habilitada pela VIVO EMPRESAS com a ação Block Detect Viruses em todas as políticas com tráfego de Internet e Para bloqueio de virus em tráfego criptografado (ex: https, ssh e etc) se faz necessário que o certificado digital do firewall seja instalado nos dispositivos que acessarão à internet.

2.2 FIREWALL

Essa camada é responsável por analisar o tráfego de rede, a partir de um conjunto de regras, para determinar quais operações de transmissão e recepção de dados podem ser realizadas. Isso acontece através de recursos avançados que permitem criar regras customizadas por IP, porta, protocolo, dispositivos de rede e aplicação.

Abaixo a configuração padrão do Firewall (Next Generation Firewall) que será aplicada no momento da instalação do equipamento.

DESCRIÇÃO	FLUXO DE TRÁFEGO ORIGEM	PORTA ORIGEM	FLUXO DE TRÁFEGO DESTINO	PORTA DESTINO / SERVIÇO	AÇÃO
BLOQUEIO_TOR	REDE LAN	ANY	Tor-Relay.Node (atualizada pelo fabricante)	Internet Service	DENY
BLOQUEIO_PORTAS	REDE LAN	ANY	ANY	SAMBA SMB SNMP ONC-RPC DCE-RPC TCP_UDP_1 TCP_UDP_108 TCP_UDP_128 TCP_UDP_137 TCP_UDP_138 TCP_UDP_7743 TCP_UDP_6881 TCP_UDP_9000-9001 TCP_UDP_9003 TCP_UDP_9030 TCP_UDP_9050-9051 TCP_UDP_9101	DENY
BLOQUEIO_GEOIP	REDE LAN	ANY	GEOIP_Afghanistan GEOIP_Aland_Islands GEOIP_Albania GEOIP_Algeria GEOIP_American_Samoa GEOIP_Andorra GEOIP_Angola GEOIP_Anguilla GEOIP_Bahrain GEOIP_Bangladesh GEOIP_Bolivia GEOIP_Bulgaria GEOIP_China GEOIP_Czech GEOIP_Egypt GEOIP_Estonia GEOIP_Hong_Kong GEOIP_India GEOIP_Indonesia GEOIP_Iran GEOIP_Latvia GEOIP_Morocco GEOIP_Namibia GEOIP_Nauru GEOIP_Netherlands_Antilles GEOIP_Nigeria GEOIP_North_Korea GEOIP_Norway GEOIP_Outlying_Islands GEOIP_Reunion GEOIP_Russian GEOIP_Saint_Martin GEOIP_Sao_Tome_Principe GEOIP_Saudi_Arabia GEOIP_Singapore GEOIP_South_Africa GEOIP_Sri_Lanka GEOIP_Syrian GEOIP_Taiwan GEOIP_Thailand GEOIP_Timor_Leste GEOIP_Trinidad_Tobago GEOIP_Turkmenistan GEOIP_Turks GEOIP_Uganda GEOIP_Ukraine	ANY	DENY

			GEOIP_Uzbekistan GEOIP_Venezuela		
NAVEGACAO WEB	REDE LAN	High ports	ANY (INTERNET) (External interface)	ALL_ICMP ALL_ICMP6 DNS (TCP/UDP 53) FTP (TCP 20,21,PASV Port) HTTP (TCP 80) HTTP (TCP 8080) SSL (TCP 443) IMAP (TCP/UDP 143) IMAPS (TCP 993) POP3 (TCP 110) POP3S (TCP 995) SMTP (TCP/UDP 25) SMTP SSL (TCP 465,587) SSH (TCP 22) TELNET (TCP 23) NTP (UDP 123)	Permit
REGRAS IMPLANTACAO	**REDE LAN**	**DE ACORDO COM FORMULARIO**	**DE ACORDO COM FORMULARIO**	**DE ACORDO COM FORMULARIO**	**Permit**
O que não se permite explicitamente se proíbe	**ANY**	**ANY**	**ANY**	**ANY**	**DENY**

IMPORTANTE: em infraestruturas que seja necessário a implementação de regras diferentes da padrão, é obrigatório que a contratante informe as necessidades antes a instalação do firewall, para que as configurações estejam aderentes à política de segurança da empresa e suas necessidades.

Na configuração padrão, não está contemplado a transcrição de um dispositivo de segurança para o que a VIVO EMPRESAS está implementando.

Após a instalação, todos os ajustes e melhorias na configuração que não foram informados antes da implantação através do formulário / check-list de implantação, só poderão ser realizadas através de chamados para o SOC.

2.3 FILTRO DE CONTEÚDO DE NAVEGAÇÃO

Está camada é responsável pelo controle da navegação dos usuários pela Internet, através da categorização dos websites que permite liberar o acesso apenas para os sites/aplicações autorizadas, com base na necessidade de produtividade e segurança da empresa.

- ✓ Criação de perfil de navegação único para toda rede;
- ✓ Bloqueios e liberação de sites através categorias específicas (ex: Youtube, Netflix, Facebook, Torrent e entre outros);
- ✓ Liberação por tempo determinado (ex: Liberar até 60 minutos de navegação para os usuários por dia);
- ✓ Liberação em períodos pré-definidos do dia (ex: Liberar redes sociais na hora do almoço).

O webfilter deverá ser habilitado para todos os acessos a Internet efetuado pelos usuários, as categorias abaixo são as que devem ser bloqueadas como recomendação mínima.

- ✓ Hacking

- ✓ Proxy Avoidance
- ✓ Pornography
- ✓ Malicious Websites
- ✓ Phishing
- ✓ SpamURLs

IMPORTANTE >>. Ajustes e melhorias na configuração poderão ser realizados através de chamados para o SOC apenas após a instalação.

2.4 PREVENÇÃO DE INTRUSÃO (IPS - INTRUSION PREVENTION SYSTEM)

Esta camada é responsável por monitorar o tráfego e/ou atividades dos sistemas em busca de comportamentos maliciosos ou não desejáveis com base em assinaturas, para bloquear e prevenir essas atividades.

Essa camada ainda conta com uma base assinaturas globais, alimentada 24x7 com novas ameaças detectadas pelo fabricante do equipamento em todo mundo, permitindo ampliar a capacidade de bloqueio através de uma ampla base de conhecimento de intrusões.

Na configuração inicial, esta feature será habilitada com todas as assinaturas ativas e em todas as políticas com tráfego de internet.

IMPORTANTE >> Todos os ajustes e melhorias na configuração acima poderão ser realizadas através de chamados para o SOC apenas após a instalação.

2.5 BALANCEAMENTO DE LINKS DE INTERNET

Esta camada é responsável pela priorização da banda de internet, viabilizando a seleção dinâmica de caminhos para o fluxo de tráfego sendo capaz de identificar aplicativos de forma inteligente e determinar o melhor caminho a ser seguido para maximizar a funcionalidade. Além disso, o recurso de auto recuperação direciona o tráfego automaticamente para o próximo melhor link disponível, caso ocorra alguma falha no link principal. Além de reduzir a complexidade da rede, esse recurso automatizado proporciona também uma melhor experiência do usuário e aumenta o desempenho das aplicações

Exemplo.: Pode determinar que um link de 10Mbps tenha 1Mbps garantido para e-mails, 5Mbps para navegação e o restante do acesso ao ERP.

IMPORTANTE >> Os links de internet do cliente deverão estar instalados e operacionais (sem bloqueios) no momento da instalação do produto Vivo Segurança Gerenciada.

2.6 VPNS

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 VPNs IPSec, possibilita o acesso à infraestrutura de forma remota através de qualquer local com acesso à Internet, permitindo customizar as políticas de acesso, definir os dados que podem ser acessados através de cada perfil de VPN configurado.

Será criada a VPN IPSec entre o equipamento na infraestrutura do cliente e o SOC, para permitir acesso do SOC e viabilizar a administração do equipamento.

A VIVO EMPRESAS se responsabiliza apenas no estabelecimento de VPNs entre dispositivos pertencentes ao mesmo projeto e sob responsabilidade da VIVO EMPRESAS.

IMPORTANTE >>. Para as outras VPNs inclusas no plano de serviço contratado, o cliente deve abrir um chamado com o SOC para que sejam realizadas criação das mesmas.

3 INSTALAÇÃO E CONFIGURAÇÃO DO EQUIPAMENTO

3.1 ENVIO DO EQUIPAMENTO PARA O ENDEREÇO CADASTRADO

O equipamento será enviado através de um distribuidor autorizado VIVO EMPRESAS para o endereço cadastrado nessa proposta, e após o recebimento, será agendado a instalação pelo Gerente de Projetos VIVO EMPRESAS.

3.2 INSTALAÇÃO FÍSICA DO EQUIPAMENTO

Ao chegar ao local de endereço de instalação, o profissional irá posicionar o equipamento no local definido pelo cliente. Nessa etapa, é indispensável providenciar os pré-requisitos descritos nessa proposta.

3.3 ATIVAÇÃO DA CONFIGURAÇÃO PADRÃO DAS FUNCIONALIDADES DE SEGURANÇA

Após acomodado, o equipamento será energizado e conectado na rede do cliente considerando os detalhes da topologia descritos nessa proposta.

3.4 VALIDAÇÃO DA INSTALAÇÃO E CONEXÃO DO EQUIPAMENTO COM O SOC

A partir disso, o SOC (Centro de operação de segurança) assume a administração do equipamento para realizar a supervisão da saúde do equipamento e customizações nas funcionalidades de segurança.

3.4.1 Itens FORA do escopo

- ✓ Definição das políticas de Segurança;
- ✓ Integração com plataformas de diretório (AD - Active Directory, Radius ou outro Sistema de autenticação de usuários);
- ✓ Treinamento de usuários, administradores ou gestores;
- ✓ Suporte técnico à usuários, administradores e gestores;
- ✓ Disponibilização de acesso administrativo a contratante mesmo que em modo compartilhado com o SOC da VIVO EMPRESAS;
- ✓ Confecção de manual de uso para usuários, administradores e gestores;
- ✓ Desenvolvimento do plano de endereçamento IP, VLANs, Roteamento, NAT, PAT, etc;
- ✓ Definição, customização ou Implementação de plataformas de gerenciamento e monitoramento de rede e segurança;

- ✓ Definição, implantação e customização do Projeto de Gerência de Redes;
- ✓ Análise de regras de firewalls e ou políticas de IDS e/ou IPS;
- ✓ Transcrição de políticas de segurança de outros dispositivos para o dispositivo objeto desta proposta;
- ✓ Análise do ambiente de rádio frequência de rede sem fio de qualquer espécie;
- ✓ Análise e/ou revisão das configurações e funcionalidades do sistema de telefonia IP e/ou VoIP;
- ✓ Definição, customização ou Implementação de serviços de:
  - DNS;
  - RADIUS, TACACS;
  - NTP;
  - AAA;
  - VLANs;
- ✓ Roteamento estático ou dinâmico;
- ✓ Mecanismos de Qualidade de serviço (QoS).

3.5 MODELO DE INSTALAÇÃO

A VIVO EMPRESAS prevê apenas a ativação de um novo equipamento na rede, com as configurações padrões instaladas e habilitadas sem a necessidade de substituir um equipamento já existente. Essa instalação é indicada para empresas que estão comprando um novo equipamento de segurança.

3.5.1.1 Características da Instalação

Atividades	Detalhamento
Validação dos Pré-requisitos	Validação por parte da VIVO EMPRESAS dos pré-requisitos disponibilizado pelo cliente
Conferência / verificação da integridade física	Avaliação e testes físicos do equipamento
Instalação Física	Fixação do equipamento em rack ou armário de telecomunicações (racking)
	Energização do equipamento
	Testes de funcionamento / Conectividade
Sistema Operacional	Atualização de Sistema Operacional
	Ativação de licenças
	Configuração básica (IP/user/password/System)
	Caso necessário, realizar a atualização do último firmware estável disponível do fabricante, bem como sua consequente ativação e inicialização. Esta atividade inclui também a atualização de possíveis assinaturas (como Antivírus, IPS, URL e Categories e entre outros).
Aplicação dos scripts e templates padronizados	Aplicação de scripts e templates de configuração, incluindo também a de uma VPN IpSec com o SOC VIVO EMPRESAS, para

	viabilizar o processo de suporte e administração remoto do equipamento
Antivírus de rede	Ativação do Antivírus de rede com políticas padrão apenas para os servidores
Filtro de Conteúdo	Habilitação de filtro web (URL) com categorias de site padrão (bloqueio de pornografia, sites suspeitos, etc.) em modos de permissões e bloqueios
Firewall (Next Generation Firewall)	Ativação das políticas e regras de Firewall para a rede interna
IPS – Prevenção de Intrusão	Ativação das regras e configurações padrões de IPS para os servidores em modo bloqueio.
Testes de Homologação e Aceite	Antes do término das configurações básicas, o técnico in-loco entraremos em contato com a área de implantação para testar o acesso remoto ao equipamento e realizar possível troubleshooting, caso necessário, incluindo: ✓ Testes de funcionalidades do Firewall; ✓ Testes de integração VPN com o SOC; ✓ Testes de bloqueio de páginas; ✓ Testes de bloqueio de aplicações; ✓ Validação dos testes.

3.6 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 do cliente;
- ✓ Serviços de obra civil e elétricos para viabilizar a instalação do equipamento contratado nessa proposta;
- ✓ Instalações adicionais ou novas instalações devido a mudança de endereço descrito nessa proposta;
- ✓ Novas instalações ou instalações adicionais por conta da aquisição de novos equipamentos que não o descrito nessa proposta;
- ✓ O SOC não atua na etapa de instalação. Essa etapa é 100% conduzida pelo integrador indicado pela VIVO EMPRESAS.

3.7 JANELA DE INSTALAÇÃO

Instalação está disponível aos dias úteis, das 08:00 às 18:00 horas.

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 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;
- ✓ 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;
- ✓ Todos os componentes de T.I. são de responsabilidades da contratante veja lista abaixo:
  - Energia elétrica;
  - Espaço para o equipamento no rack;
  - Suportes, parafusos e demais itens para a fixação necessário;
  - Estrutura de cabeamento para conexão;
  - Sistema de refrigeração caso necessário;
  - Local livre de humidade e com boa ventilação;
  - Protegido contra iluminação direta do sol ou intempéries.
- ✓ O Cliente deverá informar previamente a topologia física e lógica do ambiente;
- ✓ O Cliente 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;
- ✓ Os serviços serão executados somente em horário comercial em dias úteis;
- ✓ O equipamento será enviado e instalado no endereço da contratante que consta na proposta comercial e/ou termo de adesão.

4 SERVIÇO GERENCIADO DE SEGURANÇA (MSS)

Após o processo de instalação do equipamento com as configurações padrões 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. Esse serviço é composto por 3 (três) etapas: Manutenção, Supervisão e Administração Remota do equipamento.

4.1 MÓDULO DE MANUTENÇÃO

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

Esse serviço é também conhecido pela sigla RMA (que em inglês significa Return Merchandise Authorization) e é composto pelas etapas de:

- ✓ A contratante aciona o SOC da VIVO EMPRESAS relatando problema no equipamento;
- ✓ SOC realiza um troubleshooting e se necessário, aciona o suporte do fabricante;
- ✓ O fabricante realiza o diagnóstico do problema apresentado no equipamento;

- ✓ O SOC faz a abertura de uma solicitação ao fabricante para envio de um novo equipamento;
- ✓ O fabricante realiza o envio de um novo equipamento a contratante;
- ✓ A VIVO EMPRESAS agenda a configuração/instalação do novo equipamento por um profissional.
- ✓ O profissional realiza os testes de conectividade e segurança do equipamento;
- ✓ Ativação de um novo equipamento realizada no máximo 5 (cinco) dias úteis a partir do diagnóstico da avaria.

O SOC Centro de Operação de Segurança será responsável por toda a interface entre o fabricante e o cliente, para a abertura e finalização do processo de RMA para substituição do equipamento danificado.

4.1.1 Atendimento e Níveis de Serviço

Uma vez que a contratante suspeite do mau funcionamento de um equipamento, abre-se um chamado para o SOC da VIVO EMPRESAS realizar o diagnóstico do problema apresentado.

Veja abaixo os níveis de serviço (SLA) para essa atividade:

Módulo SOC	Serviço	Atendimento a		
		Incidentes	Solicitações	Consultas
Manutenção (RMA)	Abertura de um novo chamado	12x5	8x5	8x5
	Substituição do equipamento	N/A		

4.1.2 Consultas e Solicitações

São previstas as seguintes solicitações e consultas para este serviço:

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

4.1.3 Premissas & Prazos

- ✓ É necessário que o equipamento do cliente possua um contrato de manutenção ativo com a VIVO EMPRESAS ou que ainda esteja em garantia;
  - o O módulo de manutenção e RMA é válido apenas para os contratos que estão dentro do prazo de vigência;
  - o 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;
- ✓ Não faz parte do escopo realizar manutenção no cabeamento de dados da rede da localidade;
- ✓ Durante os atendimentos a contratante deverá disponibilizar equipe técnica de apoio para eventuais procedimentos de testes e troubleshooting na localidade;
- ✓ Não faz parte do escopo dessa atividade fornecer orientação ou treinamento das pessoas da localidade para obter acesso à rede.

4.2 MÓDULO DE SUPERVISÃO

Esta camada é responsável por monitorar a capacidade e disponibilidade de hardware do equipamento segurança objeto dessa proposta, buscando garantir recursos físicos suficientes para sustentação da tecnologia, permanência das funcionalidades de segurança ativas afim de evitar indisponibilidade do serviço por falta de recursos de hardware.

Se for identificado que o equipamento atingiu um alto nível de utilização (threshold), um alerta será gerado via e-mail e encaminhado para os responsáveis por parte do contratante.

4.2.1 Itens DENTRO do escopo

Serão considerados como itens indispensáveis para o módulo de supervisão:

- ✓ Acompanhamento da saúde dos dispositivos supervisionados 24x7;
- ✓ Canal de comunicação ao cliente via e-mail apenas quando um componente monitorado apresentar exceder os limites de utilização.
- ✓ Monitorização da saúde dos ativos de segurança seguindo os itens predefinidos, conforme lista abaixo.
    - Utilização da CPU;
    - Utilização de memória;
    - Estado das interfaces de rede;
    - Estado das interfaces WAN e LAN;
    - Estado de serviços.

Estas verificações são ativadas no momento de implantação do serviço, utilizando definições padrão de “thresholds”.

4.2.2 Requisitos de Conectividade

Este serviço necessita conectividade 24x7x365 entre o SOC e o equipamento do cliente, logo, cliente deve manter equipamento ligado durante toda operação do serviço.

4.2.3 Atendimento

Veja abaixo as janelas de atendimentos para cada modalidade:

VIVO SEGURANÇA GERENCIADA	ATENDIMENTO A		
	Incidentes	Solicitações	Consultas
Supervisão	12x5	8x5	8x5

4.2.3.1 Incidentes

Os seguintes tipos de incidentes podem ocorrer para este serviço:

- ✓ Incidente em um equipamento: indisponibilidade ou degradação da sonda de monitoração utilizada para o serviço;
- ✓ Notificação de alertas ao cliente que foram gerados pela ferramenta de monitoração.

4.2.3.2 Consultas

São previstas as seguintes consultas para este serviço:

- ✓ Mapa de serviços;
- ✓ Variáveis e limites de supervisão aplicados;
- ✓ Lista de contatos autorizados pelo cliente.

4.2.3.3 Solicitações

São previstas as seguintes solicitações para este serviço:

- ✓ Modificação nos parâmetros de supervisão de um equipamento;
- ✓ Modificação na lista de contatos autorizados do cliente;
- ✓ Modificação no mapa de serviços do cliente.

4.3 MÓDULO DE ADMINISTRAÇÃO 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 VIVO EMPRESAS em segurança para manter as configurações do equipamento ativas e atualizadas.

4.3.1 Características da Administração do equipamento

O SOC irá disponibilizar recursos especializados para, pois, esta responsabilidade passa a ser do SOC, que realizará as seguintes atividades:

- **Participação na resolução de incidentes de segurança:** os operadores de segurança passam responder problemas relacionados as funcionalidades de UTM.
- **Planejamento e implementação de mudanças:** contempla a avaliação e implementação de mudanças nos dispositivos por meio de solicitações do cliente, baseados nas melhores práticas de gestão. Esta atividade não contempla mudanças

na arquitetura ou funcionalidade do equipamento administrado, atividades cobertas através de um projeto especial ou de consultoria.

- **Resolução de solicitações feitas pelos clientes:** contempla a realização das tarefas operacionais solicitadas pelo cliente, tais como executar backup de configurações, gerenciamento de usuários, 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 de forma proativa, visando garantir o bom funcionamento e a disponibilidade dos serviços.
- **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.

4.3.2 Atendimento

VIVO SEGURANÇA GERENCIADA	ATENDIMENTO A		
	Incidentes	Solicitações	Consultas
Administração Remota	12x5	8x5	8x5

Administração - Atendimento

4.3.2.1 Incidentes

Os seguintes tipos de incidentes podem ocorrer para este serviço:

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

4.3.2.2 Consultas

São previstas as seguintes consultas para este serviço:

- ✓ Mapa de serviços;
- ✓ Lista de alterações pré-autorizadas pelo cliente;
- ✓ Lista de contatos autorizados pelo cliente.

4.3.2.3 Solicitações

São previstas as seguintes solicitações para este serviço:

- ✓ Alteração na política (regras de UTM) do equipamento;
- ✓ Modificação na lista de alterações pré-autorizadas pelo cliente;
- ✓ Modificação na lista de contatos autorizados do cliente.

4.3.3 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;
- ✓ O contratante não poderá gerenciar os dispositivos em que este serviço é prestado;
- ✓ A autenticação para acesso administrativo aos dispositivos ser dará através do serviço de autenticação da VIVO EMPRESAS;
- ✓ Os dispositivos gerenciados devem ser sincronizados com servidor de tempo (NTP) da VIVO EMPRESAS.

4.4 RELATÓRIO SOB DEMANDA

Esta camada visa prover as informações referentes as funcionalidades de segurança ativas no equipamento através de relatórios padronizados do tráfego. Para o plano padrão, já está incluso sem necessidade da contratação do módulo adicional de “Relatório Mensal”, um relatório sob demanda.

Os relatórios devem ser solicitados pelo contratante através de chamado com antecedência de 15 (quinze) dias, onde o SOC irá ativar a captação das informações que irá compor o relatório.

IMPORTANTE >>. A informação do tráfego do ambiente não é capturada automaticamente pelo equipamento, é necessário solicitar a ativação desse recurso no SOC para gerar os insumos de dados para o mesmo.

4.4.1 Característica do Relatório sob demanda

4.4.1.1 Tipo

Relatório padrão utilizando as informações capturadas de tráfego do ambiente do cliente.

4.4.1.2 Formato

Formato do relatório é apenas em “.pdf”.

4.4.1.3 Insumo de Dados

Este relatório será gerado pela própria ferramenta em inglês com informações consolidadas mais comumente utilizadas, para o período de tempo de 7 (sete) dias, no formato PDF, 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.

4.4.1.4 Apresentação do Relatório

O relatório será enviado por e-mail e não está inclusa a apresentação presencial ou online do relatório.

4.4.1.5 Periodicidade

Sob demanda. O cliente deve solicitar através de chamado aberto junto ao SOC.

4.4.1.6 Limitação de quantidade por contrato

São limitados em 4 (quatro) unidades de relatório padrão no período de 12 (doze) meses.

4.4.1.7 Idioma padrão Relatório

Por padrão o relatório será entregue apenas em Inglês.

5 MÓDULOS ADICIONAIS

Para complementar os serviços ofertados através dos planos, temos a disposição um módulo adicional que pode ser contratado para complementar qualquer plano.

5.1 RELATÓRIO MENSAL *OPCIONAL

Esta camada tem um custo adicional sendo necessário consulta prévia junto ao time comercial da VIVO EMPRESAS e é responsável por disponibilizar todos os meses um relatório padrão com os vírus, trojans, adware, spyware e outras ameaças bloqueadas pelas funcionalidades de segurança ativa no equipamento. Além disso, é possível visualizar essas informações por usuários, aplicação, IPs e entre outros dispositivos. Veja mais detalhes do módulo abaixo.

5.1.1 Características do Módulo Relatório Adicional

5.1.1.1 Tipo

Relatório padrão utilizando as informações capturadas de tráfego do ambiente do cliente.

5.1.1.2 Formato

Formato do relatório é apenas em “.pdf”.

5.1.1.3 Insumo de Dados

Este relatório será gerado pela própria ferramenta em inglês com informações consolidadas mais comumente utilizadas, para o período de tempo de 7 (sete) dias, no formato PDF, 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.

5.1.1.4 Apresentação do Relatório

O relatório será enviado por e-mail e não está inclusa a apresentação presencial ou online do relatório.

5.1.1.5 Periodicidade

Mensal.

5.1.1.6 Limitação de quantidade por contrato

São limitados em 12 (doze) unidades de relatório padrão no período de 12 (doze) meses.

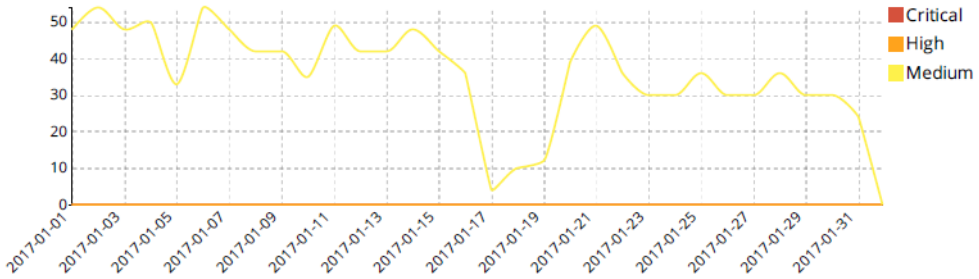
5.1.1.7 Idioma padrão do Relatório

Por padrão o relatório será entregue apenas em Inglês.

5.2 CONTEÚDO DO RELATÓRIO

5.2.1 Cronograma de Intrusões

Abaixo, uma imagem ilustrativa das tentativas de intrusões separadas pelo nível de criticidade.



5.2.2 Categorias mais acessadas

Abaixo, uma imagem ilustrativa com as categorias mais utilizadas parametrizadas pelos números de usuários que utilizaram e o volume de dados trafegados por categoria.

#	URL Category	User	Count	Bandwidth
1	File Sharing and Storage	111	1,039,537	1.34 GB
2	Meaningless Content	72	95,663	302.60 MB
3	Content Servers	155	34,125	116.40 MB
4	Internet Telephony	105	28,112	97.54 MB
5	Social Networking	219	24,313	74.99 MB
6	Instant Messaging	57	23,795	136.85 MB
7	Streaming Media and Download	105	14,845	47.75 MB
8	Malicious Websites	21	13,538	47.90 MB
9	Advertising	133	13,039	47.28 MB
10	Games	51	7,039	23.37 MB
11	News and Media	101	5,764	22.27 MB
12	Freeware and Software Downloads	166	5,226	20.22 MB
13	Web Chat	27	4,561	17.15 MB
14	Shopping and Auction	136	4,322	12.84 MB
15	Society and Lifestyles	32	4,306	10.26 MB
16	Unrated	60	3,631	19.74 MB
17	Reference	147	2,524	8.93 MB
18	Travel	40	1,967	5.01 MB
19	Personal Websites and Blogs	83	1,343	4.15 MB
20	Dating	5	1,122	2.99 MB
21	Sports	45	868	3.63 MB
22	Peer-to-peer File Sharing	14	729	2.72 MB
23	Internet Radio and TV	21	494	1.82 MB
24	Web-based Email	41	292	828.50 KB
25	Health and Wellness	15	261	860.38 KB

5.2.3 Principais sites de streaming vídeo por banda utilizada

#	Website	Bandwidth	Sent	Received
1	nflxvideo.net			12.32 MB
2	googlevideo.com			8.79 MB
3	uplynk.com			6.37 MB
4	netflix.com			4.96 MB
5	youtube.com			4.45 MB
6	apple.com			2.95 MB
7	dingit.tv			2.83 MB
8	globo.com			1.28 MB
9	xboxlive.com			927.10 KB
10	msn.com			478.89 KB

Um dos maiores ofensores do tráfego é o carregamento de streaming. O relatório fornece uma visão detalhada de quais são os maiores ofensores e o volume do tráfego gerado por cada um deles, vide imagem ilustrativa acima.

6 PLANOS E CARACTERISTICAS

A proposta comercial apresentada para o contratante pela VIVO EMPRESAS é composta pelos 3 (três) planos que consistem em configurações diferentes equipamento e planos de serviço, onde o cliente deve escolher apenas 1 (um) compatíveis com as características do seu ambiente de T.I.

vivo EMPRESAS	Plano P	Plano M	Plano G
1. Equipamento / Licença / Suporte			
Usuários Simultâneos	Até 40 usuários	Até 70 usuários	Até 100 usuários
Link de Internet (Capacidade do equipamento)	Até 30 Mbps	Até 50 Mbps	Até 80 Mbps
INSTALAÇÃO EQUIPAMENTO			
Instalação Padrão	Instalação de um equipamento novo, considerando a configuração padrão		
Administração do Equipamento			
N° Chamados / Mês	3	5	
Configuraçã de novas VPNs (client to site) / ano	2 VPNs / ano	3 VPNs / ano	
Criação de novas VPNs (Site to Site) / ano			
Gestão de regras de antívirus / mês	Total de 2 regras de UTM / mês	Total de 5 regras de UTM / mês	
Criação de regras - Filtro Web / mês			
Gestão das regras e políticas de firewall / mês			
Gestão de regras de IPS / mês			
Relatórios sob Demanda	Sim	Sim	Sim

(1) IMPORTANTE >>. Para garantir a performance de hardware do equipamento até o final da vigência do contrato, deve ser previsto pelo gerente de vendas e o 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. Veja o exemplo abaixo:

Se a empresa atualmente conta com 30 funcionários, mas prevê que em até 3 (três) anos estará com 60 funcionários, é recomendado nesse caso a aquisição do Plano M, mesmo que na data da contratação o Plano P atenda aos requisitos do cliente. Caso isso não aconteça, ao ultrapassar o número de 40 funcionários, o equipamento pode apresentar degradação no desempenho por falta de recursos de hardware, e seja necessário realizar uma substituição precoce do equipamento.

6.1 IMPOSTOS

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

6.2 VALIDADE DA PROPOSTA

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

6.3 FATURAMENTO

Os serviços serão faturados mensalmente com a nomenclatura na fatura de **Vivo MSS – Avançado**, a partir da data de aceite do serviço.

6.4 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.

6.5 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.

7 MATRIZ DE RESPONSABILIDADES

Veja abaixo a matriz de responsabilidades detalhada com as tarefas de responsabilidade da VIVO EMPRESAS e contratante.

A APOIO **| R** RESPONSABILIDADE

ATIVIDADE	RESPONSABILIDADES	
	SOC VIVO EMPRESAS	CLIENTE
SEGURANÇA E GOVERNANÇA		
Definição das políticas e diretrizes de segurança da informação voltadas aos negócios do contratante	-	R
Confecção e manutenção do “mapa de rede e serviços” com a descrição da arquitetura e dos principais serviços no ambiente do contratante	-	R
Análise e avaliação de riscos imediatos ao ambiente gerenciado pelo SOC frente as solicitações do contratante	R	A
Solicitar a coleta de insumos para a geração de relatórios futuros.	-	R
Geração de relatórios sob demanda com dados coletados no prazo máximo de 7 (sete) dias sempre que solicitado pelo contratante	R	-
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 e ativação do equipamento e das funcionalidades de UTM.	R	-
Informar e atualizar lista de contatos do contratante para o processo de escalonamento.	-	R
Encaminhar problemas aos grupos solucionadores do contratante.	-	R
GESTÃO DE MUDANÇAS		
Planejamento técnico de mudanças nos ativos gerenciados (limitado às alterações no próprio ativo)	-	A
Planejamento técnico de mudanças na arquitetura do ambiente do contratante	-	R
Encaminhamento de solicitações de mudanças ao comitê aprovador de mudanças (CAB) do contratante.	A	R
Defesa da mudança pertinente ao ativo gerenciado dentro do comitê aprovador de mudanças (CAB) do 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 do contratante pertinentes aos ativos gerenciados (solicitações de regras nos firewalls, alterações de configurações nos IPS, etc.)	R	A

Avaliação técnica de demandas sugeridas pelo SOC pertinentes ao ativo gerenciado (solicitações de regras nos firewalls, alterações de configurações nos IPS, etc.)	**A**	**R**
Implementação das mudanças aprovadas no escopo do serviço	**R**	
Execução de testes após nova configuração/ alteração	**-**	**R**
MONITORAÇÃO		
Monitoração de disponibilidade dos equipamentos gerenciados	**R**	**-**
Monitoração de performance dos equipamentos gerenciados	**R**	**-**
Definição das interfaces críticas a serem monitoradas nos ativos	**-**	**R**
Acionamento do contratante em caso de problema em ativo monitorado.	**R**	**-**
Configurar e suportar as ferramentas de monitoração do SOC.	**R**	**-**
GESTÃO DO NÍVEL DE SERVIÇO		
Definição do processo de comunicação entre o contratante**,** o fornecedor e terceiros envolvidos.	**R**	**R**
GESTÃO DA CAPACIDADE		
Monitorar a capacidade do equipamento através do serviço de Supervisão.	**R**	**-**
Aprovação das mudanças e melhorias identificadas.	**A**	**R**
GESTÃO DE ACESSO		
Criação/remoção de usuários para acesso a console.	**R**	**-**
Gerencia de acesso dos usuários internos do contratante.	**-**	**R**
Criação/remoção/alteração de perfis para acesso a console.	**R**	
Reset de senha de usuário.	**R**	
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 pelo cliente	**R**	**-**
Aquisição e renovação de licenças e suporte do fabricante	**-**	**R**

7.1 RESPONSABILIDADES POR TIPO DE ATIVO GERENCIADO

ATIVIDADE COMUNS AOS ATIVOS GERENCIADOS		
Alteração de configurações (regras, políticas, componentes, etc.) mediante solicitação do contratante.	**R**	**-**
Correção de vulnerabilidades e riscos no equipamento gerenciado.	**R**	**A**
Monitoramento de disponibilidade e performance dos equipamentos gerenciados	**R**	**-**
Backup e “restore” da configuração dos ativos	**R**	**-**
ATIVIDADES DE FIREWALL		
Criação / Remoção / Alteração de regras (ACLs, NAT, PAT, Anti-spoofing, Rotas, VPNs) solicitadas pelo contratante.	**R**	-

Interface e acionamento de parceiro peer VPN para criação/remoção/alteração de túnel VPN site-to-site.	-	R
Identificação de aderência de regras com política de segurança da contratante.	-	R
ATIVIDADES DE IPS		
Atualização das assinaturas do IPS	R	
Execução de liberação/bloqueio de endereços IP mediante solicitação/ aprovação da contratante	R	
Identificação e notificação de máquinas comprometidas com Malware ou fontes de ataques		R
Identificação de ataques direcionados		R
Remoção de Malware em máquinas afetadas		R
Remoção de hosts/IPs/Usuários bloqueados e/ou quarentenados registrados no IPS mediante solicitação/ aprovação da contratante	R	A
Alteração de configurações mediante solicitação do contratante.	R	
Criação/alteração/remoção de política de IPS, controle de aplicativos, políticas de limites de conexão, regras de ACL, regras de assinaturas, políticas de alertas	R	
Manutenção da base de ativos da ferramenta	R	A
ATIVIDADES DE FILTRO DE CONTEÚDO/PROXY		
Atualização das assinaturas de Anti Malware.	R	
Identificação e reporte do equipamento e URLs acessadas dentro de categorias de Riscos (malware, phishing, botnet, etc)	R	
Liberação ou bloqueio de URLs mediante solicitação do contratante.	R	
Criação/alteração/remoção de política de acesso mediante solicitação do contratante.	R	
Criação/alteração/remoção de política de Controle de aplicativos mediante solicitação do contratante.	R	
Instalação/ Reinstalação do "agente" em máquinas de usuários.		R
Criação/alteração de arquivo PAC (proxy auto configuration).	R	
Instalação/ remoção de arquivo PAC (proxy auto configuration).		R

8 ATENDIMENTO AO CLIENTE

8.1 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.

O cliente 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 ao cliente. 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.

8.2 FECHAMENTO DO CHAMADO

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

8.3 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.

8.4 FLUXO DE ATENDIMENTO

Para controle das solicitações e da resolução das mesmas, bem como para o adequado acompanhamento do desempenho do serviço, o cliente 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.

9 SUPORTE AO CLIENTE

O SOC disponibiliza três níveis de suporte para atendimento aos serviços contratados pelo cliente:

- ✓ **Suporte 1º Nível:** realizado pela equipe do SOC que trabalham 8x5 (vinte e quatro horas por dia, sete dias por semana) para atendimento a qualquer grau de severidade de chamados.
- ✓ **Suporte 2º Nível:** realizado pela equipe do SOC que trabalha 8x5 (oito horas por dia, 5 dias por semana), podendo ser acionado fora deste horário pelo 1º Nível para cumprimento de SLO/SLA dos serviços;
- ✓ **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.

9.1 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

9.2 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.

9.3 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.

9.4 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:

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

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

Índices de descontos

9.5 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).

9.6 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.

9.7 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 do contratante, não serão contabilizadas para o cálculo da disponibilidade do serviço.

10 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.

10.1 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 o contratante por todos os serviços prestados por terceiros.

10.2 RESPONSABILIDADES DO CLIENTE

Clientes que venham a contratar serviços da VIVO EMPRESAS estarão assumindo as seguintes responsabilidades:

- ✓ O cliente deverá fornecer informações suficientes com relação às suas necessidades e informações técnicas para configuração inicial do serviço até a data de implantação;
- ✓ 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.

10.3 RESPONSABILIDADES DA TELEFONICA | 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.

11 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) A infraestrutura física (energia elétrica, racks, cabeamento estruturado, sistema de refrigeração entre outros) para a instalação dos equipamentos ofertados é de responsabilidade da contratante;
3) Em caso de necessidade de RMA do equipamento, a política de troca seguirá a política do fabricante e ocorrerá em até 5 (cinco) dias úteis após o diagnóstico;
4) A administração do ambiente contratado é realizada somente através do SOC da VIVO EMPRESAS;
5) A contratante receberá da VIVO EMPRESAS um formulário e/ou “check-list” para que sejam coletadas regras a serem implementadas. Caso esse documento não seja enviado para VIVO EMPRESAS devidamente preenchido até o momento da instalação, a configuração inicial do serviço será padronizada, seguindo boas práticas de segurança e, alterações poderão ser solicitadas apenas via chamado para o SOC após a instalação e de acordo com o limite do plano contratado;
6) A solução prevê a inspeção somente de tráfego “https”. Outros formatos de tráfego criptografado não serão inspecionados;
7) Todos os planos disponíveis não contemplam um equipamento adicional para prover alta disponibilidade (H.A);
8) Todos os SLAs de atendimento firmados não podem ser alterados;
9) Não é possível ativar VPNs através do integrador no momento da instalação, apenas via SOC na etapa de administração do equipamento;
10) Não estão previstos equipamentos adicionais como access point (AP) para distribuição de sinal de internet sem fio (Wi-fi);

11) Prazo de instalação do equipamento no endereço indicado pela contratante é de até 90 (noventa) dias após a assinatura do contrato;

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

13) Não é possível contratar os itens que compõe o produto Vivo Segurança Gerenciada (MSS | Plano P, M, G) separadamente. A única opção de comercialização são os planos fechados;

14) O escopo da proposta contempla a atuação do SOC apenas para solução de problemas no equipamento objeto dessa proposta. Consultoria especializada para investigações que incluam outros dispositivos e infraestrutura de TI do cliente não estão incluídos;

15) Não inclui passagem de conhecimento do equipamento ou treinamento para equipe interna do cliente.