Termo Específico do Produto

Vivo Clean Email

1 VIVO CLEAN EMAIL

1.1 PROPOSTA DE VALOR

O serviço Vivo Clean Email é fornecido através de em um modelo global de SOCs, interagindo de forma coordenada e cooperativa, a fim de alcançar a maior eficiência nos serviços prestados. Este modelo possibilita maior disponibilidade dos serviços e de conhecimento aos clientes.

Neste sentido, os serviços de segurança gerenciada fornecem:

- Solução completa e abrangente;
- Continuidade;
- Operação e gestão coordenada sob os seguintes pressupostos:
    - Plataformas, processos e ferramentas comuns na rede global;
    - Escalabilidade.
- Eficiência na prestação de serviços:
    - Cobertura 24x7x365;
    - Conhecimento distribuído entre os SOCs para servir todos os clientes independentemente da sua localização;
- Prestação de serviços de qualidade com uma abordagem global:
    - Homogêneo;
    - Serviços globais para responder a ameaças globais.

Entre as muitas vantagens de contratar este serviço com a Vivo Empresas, o cliente poderá usufruir da rede iSOC e inteligência patenteada da Telefónica TECH.

1.2 SOBRE O SERVIÇO

Clean Email é um serviço em nuvem que oferece proteção para e-mail contra ameaças como spam, malware ou phishing. Bloqueia os emails suspeitos endereçados pelo Cliente e permite cumprir as políticas estabelecidas para o uso adequado do e-mail que o Cliente definir. Detecta vírus, lixo eletrônico ou conteúdo impróprio e, nesses casos, impede que cheguem pelo e-mail, parando-os antes que entrem nos sistemas da empresa. Ele também pode interceptar emails de saída potencialmente perigosos antes de serem distribuídos pela Internet fora dos sistemas da empresa.

Este serviço de filtragem de e-mail é independente das plataformas de correio das empresas e de fácil implementação, o que permite às empresas complementarem os seus atuais serviços de e-mail com funcionalidades de antivírus, antispam e filtragem de conteúdos, sem necessidade de investimento em tecnologia, nem na sua manutenção e em conhecimentos avançados na referida tecnologia, visto que o serviço inclui a administração da ferramenta pela equipe do SOC da Telefónica Tech.

Ele é implementado como um gateway de entrada e saída ou gateway para o e-mail do cliente, filtrando-o quanto a spam e malware antes de encaminhá-lo ao seu destino. O e-mail recebido no domínio protegido, coberto pelo Serviço, será verificado usando vários métodos de detecção diferentes para determinar se é spam, por meio de filtros, como alguns dos listados abaixo:

- Antispam.
- Anti-malware.
- Métodos de filtragem de conexão com White / black list, listas de reputação de IP e outros tipos de listas.
- Validação de domínio do remetente.

1.3 BENEFÍCIOS AO CLIENTE

É uma solução para a proteção integral do e-mail corporativo, dispensando a necessidade de infraestrutura nas dependências do cliente.

As organizações geralmente selecionam a segurança de e-mail oferecida por este serviço para proteger os usuários e, em última instância, os dados, contra uma ampla gama de ameaças cibernéticas.

Isso inclui: volumes cada vez maiores de spam, falsificação de engenharia social e comprometimento de e-mail comercial, variantes aceleradas de ransomware e outros malwares, ataques cada vez mais direcionados de adversários de todos os tipos e muito mais. Ao mesmo tempo, o serviço pode ser usado para proteger dados confidenciais de todos os tipos, reduzindo o risco de perda inadvertida e não conformidade com regulamentações como HIPAA, PCI, LGPD e muito mais.

Essa segurança de e-mail usa as tecnologias e serviços de segurança mais recentes para fornecer proteção consistente de primeira classe contra ameaças comuns e avançadas, enquanto integra recursos robustos de proteção de dados para evitar perda de dados.

O serviço se destaca pelos seguintes dados:

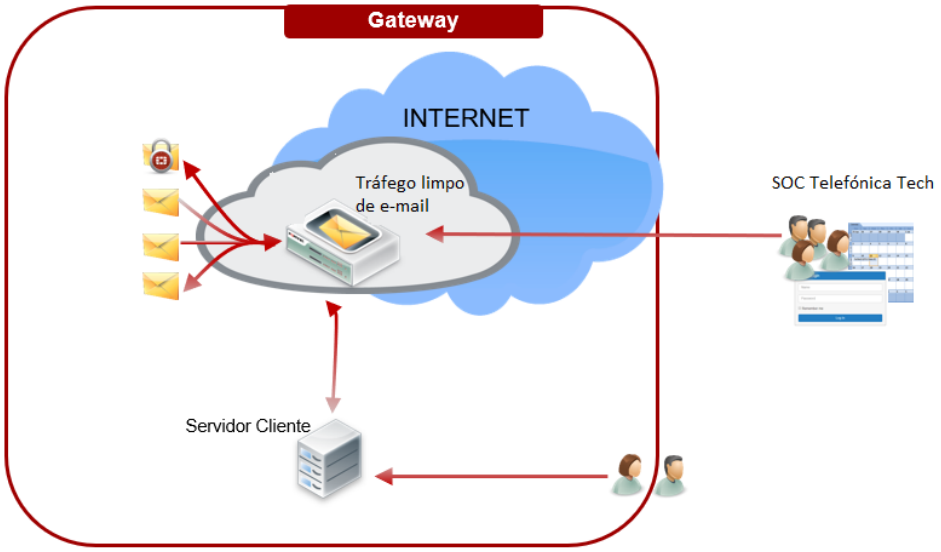
- Inteligência de ameaças baseada em inteligência artificial, em spam, phishing, malware, ransomware e muito mais ..., para acompanhar o cenário de ameaças em constante mudança.
- A maioria dos recursos recomendados do Gartner para Defesa Avançada contra Ameaças (conforme descrito no Guia de Mercado de Segurança de E-mail do Gartner de junho de 2019).
- Controles administrativos robustos para roteamento de e-mail, gerenciamento de quarentena, personalização de mensagens junto com controles de usuário final para autoatendimento.
- Tudo com alto desempenho e confiabilidade para esta ferramenta crítica de negócios.

1.4 ARQUITETURA DO SERVIÇO

Após a contratação do serviço, o domínio do Cliente será disponibilizado pela Vivo Empresas em uma plataforma e a disponibilidade para o seu uso será comunicada ao número de usuários contratados.

A partir desse momento, o Cliente deverá redirecionar seu e-mail para a plataforma de nuvem, alterando os registros MX no Servidor de Nomes de Domínio (DNS) para apontá-lo. O servidor de e-mail do Cliente deve ser configurado para aceitar apenas e-mails vindos da plataforma em nuvem.

Da mesma forma, o Cliente deverá também enviar para a plataforma toda a sua correspondência de saída, de forma a garantir o correto funcionamento do serviço de correio e que, por exemplo, não ocorra o uso malicioso do servidor de e-mail do Cliente.



Arquitetura apenas de referência

1.5 PRINCIPAIS FUNCIONALIDADES

Antivírus

Este antivírus protege contra os vírus mais recentes, spyware e outras ameaças a nível de conteúdo. Utiliza mecanismos de detecção avançados líderes de mercado para evitar que novas ameaças novas e em evolução obtenham uma posição estabelecida em sua rede e acessem conteúdo valioso.

Outbrake Protection

Preenche a lacuna entre as atualizações de antivírus com a varredura Sandbox para detectar e impedir ameaças de malware descobertas entre as atualizações de assinatura antes que possam se espalhar por toda a organização. O sistema operacional inicia uma pesquisa em tempo real em nosso banco de dados de inteligência global contra ameaças.

Desarme e reconstrução de conteúdo

Remove todo o conteúdo ativo dos arquivos em tempo real, criando um arquivo limpo e plano. Todo o conteúdo ativo é tratado como suspeito e removido. Processa todos os arquivos recebidos, os desconstrói e remove todos os itens que não correspondem às políticas do firewall.

Cloud Sandboxing

É uma solução avançada de detecção de ameaças que realiza análises dinâmicas para identificar malware anteriormente desconhecido. A inteligência acionável gerada pelo serviço Sandbox retroalimenta os controles preventivos em sua rede, desarmando a ameaça.

1.6 CARACTERÍSTICAS

Características
Antispam
Anti-malware
Filtragem de entrada e saída
Integração com LDAP do cliente
Entrega de mensagens segura (TLS)
Rastreamento de mensagens
Virus Outbreak Service
Relatórios
Criptografia baseada em identidade (IBE)
Desarmamento e reconstrução de conteúdo
URL Click Protection
Análise de falsificação de identidade
Cloud Sandboxing

1.7 PREMISSAS E PRÉ-REQUISITOS

Para que o serviço seja ativado, alguns requisitos devem ser atendidos e a correta identificação destes requisitos é essencial para o correto funcionamento do serviço.

- O Cliente deve ter contratado um serviço de e-mail. As caixas de correio não estão incluídas no serviço, mas uma solução para remover vírus e malware dele.
- Para utilizar este serviço, o Cliente deve possuir domínio próprio corporativo, ou seja, **não aplicável** a contas de e-mails genéricas de mercado como por exemplo, @gmail.com. @yahoo.com e etc.
- Aplica-se somente a contas de e-mail que possam ter o registro MX do DNS alterado para o endereço IP da plataforma em nuvem do serviço provido pela Vivo Empresas.
- O Cliente deve contratar o serviço para todas as caixas de correio que possui no domínio que deseja analisar com a plataforma do serviço.
- A contratação de 1 usuário em um pacote garante usufruir do serviço para uma única caixa de correio em um único domínio. Duas caixas de correio do mesmo usuário em domínios diferentes exigiriam a contratação de caixas de correio adicionais.
- A utilização da plataforma Vivo Clean Email não permite o envio de e-mails de saída de domínios que não sejam o domínio protegido através da contratação do serviço.
- Não é permitido enviar e-mails em massa usando este serviço para evitar que o serviço Vivo Clean Mail seja incluído nas black lists de spam.
- Administração da plataforma é realizada somente através do SOC da Telefónica Tech, e poderá ser compartilhada com o cliente apenas no modo leitura.
- Para essa solução não será permitida a customização de prazos, SLA ou características diferentes descritas nesse documento.
- A implantação do serviço será realizada em dias úteis, das 08:00 às 17:00 horas.
- O cliente 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.
- O Cliente será responsável por danos causados como resultado da ação tomada pelo próprio Cliente em relação a e-mails de spam e por danos causados pela exclusão de tais e-mails.

- Caso o Cliente opte por divulgar um e-mail infectado ou marcado como potencialmente infectado por malware, a Vivo Empresas não será responsável pelos danos causados.

1.8 ITENS FORA DO ESCOPO

Os seguintes itens estão expressamente excluídos:

- A configuração dos servidores DNS do Cliente.
- Alteração ou configuração de equipamentos e/ou softwares já instalados na rede do cliente.
- Será da responsabilidade do cliente fazer as mudanças na configuração dos registros MX de seu domínio de e-mail para começar a desfrutar do serviço, uma vez que a disponibilidade do mesmo seja comunicada a ele pela Vivo Empresas.
- Alterações de configuração nos servidores de e-mail do Cliente e / ou nos firewalls de propriedade do Cliente (para o estabelecimento de regras que permitem o tráfego de e-mail de e para a plataforma Vivo Clean Mail).
- Definição das políticas de Segurança.
- Passagem de conhecimento do serviço ou treinamento para equipe interna do cliente.
- Confecção de manual de uso para usuários, administradores e gestores.

1.9 INSTALAÇÃO E CONFIGURAÇÃO DO SERVIÇO

A Vivo Empresas será responsável pela instalação e configuração da solução referente a essa proposta. As seguintes atividades e premissas estão sendo consideradas:

- Planejamento interno (alocação Gerente de Projeto, kick-off interno com equipes), preparação de material (cronograma, apresentação), reunião inicial, apresentação equipes, reunião para listar demandas, apresentar planejamento;
- A implantação será realizada em horário comercial. Caso cliente necessite que essa atividade seja realizada em janelas operacionais ou finais de semanas (dias não úteis), deverá sinalizar para Vivo Empresas antecipadamente, na fase de elaboração do projeto.

É imprescindível para o avanço das atividades de instalação do serviço o comprometimento do cliente em disponibilizar os recursos listados abaixo:

- O cliente 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 acompanhar todo o processo de instalação e ativação do serviço;
- Não está contemplado a instalação, configuração, atualização de nenhum outro equipamento e/ou software de TI que não seja o escopo de serviço contratado nesse documento.

1.10 PRAZO DE INSTALAÇÃO

O prazo previsto para instalação do serviço é de até 60 (sessenta) 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.

1.11 SUPORTE

A Telefónica Tech prestará desde o SOC o serviço de suporte, manutenção e administração de todos os produtos contratados pelo cliente que seja escopo da oferta.

O registro de solicitações, incidentes e consultas pode ser efetuado a qualquer hora e em qualquer dia da semana, através dos canais de atendimento colocados à disposição do cliente e de acordo com as características descritas no acordo de nivel de serviços.

O serviço em questão inclui a operação remota pelo SOC do software de segurança fornecido e implantado nos devices do Cliente ou em plataformas de nuvem com o seguinte escopo:

- Participação em incidentes de segurança. o SOC participará na descoberta das origens e mitigação no âmbito da visão proporcionada pelos equipamentos / software geridos dos incidentes de segurança, não sendo em caso algum responsável pela coordenação da gestão ou resposta aos referidos incidentes.
- Participação na resolução de Incidentes. o SOC colaborará na revisão da configuração e ocorrências dos equipamentos / software que gere para ajudar o Cliente a resolver quedas em serviços críticos de seus processos de negócio. Caso a origem do problema seja um Sistema Monitorado, o SOC ativará todos os mecanismos de resolução dentro das limitações dos produtos e sistemas implantados para resolver ou mitigar o problema.
- Resolução de solicitações. contempla o desempenho das tarefas de operação solicitadas pelo Cliente e tipificadas dentro do serviço.

São compreendidas como tarefas tipificadas, as seguintes, classificadas em dois tipos:

a. Incidentes: falhas ou mau funcionamento nos serviços.
b. Solicitações: solicitações feitas pelo Cliente quanto à configuração do serviço. Alguns exemplos:
    - Configurações de black list e lista de permissões de e-mail.
    - Configurações relacionadas às black / white lists de domínios e urls.

- Identificação proativa de riscos. o Cliente será informado de forma proativa se, no desempenho de suas funções, os administradores detectarem riscos de segurança óbvios.

As ferramentas das soluções implantadas irão gerar alertas ou indicadores de segurança que serão analisados pelo SOC de acordo com os critérios de segurança e determinando se são capazes de uma atuação manual bem automatizada. Será limitado apenas ao número de dispositivos / ferramentas / capacidades contratadas e desde que devidamente implantadas de acordo com os critérios pré-acordados.

- Correção de vulnerabilidades identificadas no software fornecido. o serviço participará da realização das alterações necessárias para corrigir as vulnerabilidades encontradas no software fornecido.
- Registro e controle de solicitações de serviço. o Cliente poderá fazer um pedido por qualquer um dos meios que lhe são disponibilizados para tal.
- Comunicações / relatórios: relatórios disponíveis no portal do serviço.
- Updates e patches: atualização de serviços por meio de atualizações e patches gerados pelos fabricantes / prestadores de serviços.

1.12 ACORDO DE NÍVEL DE SERVIÇO

Serviço	Incidentes	Solicitações e Consultas
Operação SOC	24x7	8x5

O horário comercial 8x5 será das 8h00 às 17h00, de segunda a sexta-feira, horário de funcionamento de acordo com o calendário comercial do Brasil.

As diferentes ações que o Cliente pode executar como parte dos serviços são estabelecidas como Solicitações, Consultas ou Incidentes. Incluiremos as consultas como solicitações, pois não são consultivas. Além disso, existem atividades que, por sua própria natureza, são iniciadas pelo SOC. Eles estão definidos da seguinte forma:

- Incidentes: falha, degradação ou comportamento inesperado do serviço informado pelo Cliente ou detectado pela Telefónica Tech.
- Solicitações: solicitação de execução de atividade de prestação de serviço ou consulta de parâmetros próprios extraídos das ferramentas.
- Consulta: pedido de informação sobre o estado ou configuração dos serviços, de forma genérica ou específica para um dispositivo no qual o serviço está sendo prestado.
- Atividade de serviço: atividade de entrega de serviço iniciada pelo SOC.

Tempo alvo de resposta

Período de tempo que decorre desde o momento em que um usuário enviou a solicitação ou incidente até receber uma resposta da Telefónica Tech, uma vez realizada a triagem inicial.

O SOC trabalha com um tempo de resposta alvo de até 90 minutos.

Tempo alvo para resolução de Solicitações e Consultas

Este indicador mede o tempo de resolução de solicitações em 8x5.

Níveis de severidade	Tempo alvo	Horário atuação
Urgente	12 horas	Solicitações e consultas em 8x5
Normal	24 horas	Solicitações e consultas em 8x5

Tempo alvo para resolução de incidentes

A severidade de cada uma das demandas abertas pelo Cliente ou pelo próprio SOC terá, via de regra, uma severidade de acordo com o nível de impacto no serviço prestado pelo SOC, conforme demonstrado na tabela a seguir:

Níveis de severidade	Definição
Crítico	Aqueles incidentes em que há paralização do serviço
Alto	Aqueles incidentes em que há degradação do serviço
Médio-Baixo	Incidentes com impacto no serviço

Este indicador mede o tempo objetivo para resolver incidentes 24x7.

Níveis de severidade	Tempo alvo	Horário atuação
Crítico	<8 horas*	Incidentes em 24x7
Alto	<24 horas*	Incidentes em 24x7
Médio-Baixo	<72 horas*	Incidentes em 24x7

* Estes tempos serão aumentados no caso de o incidente envolver algum tipo de desenvolvimento por parte do fabricante (para resolver, por exemplo, um bug do produto).

Os valores alvo dos níveis Crítico e Severidade Alta referem-se ao tempo de resolução do incidente relacionado à falta de disponibilidade ou degradação da plataforma. Posteriormente, será feito um diagnóstico da origem que causou o incidente, não computando a duração desse diagnóstico na medição do tempo alvo.

O tempo objetivo considera apenas o tempo que a tarefa esteve sob responsabilidade do pessoal da Telefónica Tech. Portanto, são excluídos os períodos de tempo em que esteve à espera de dados, instruções ou ações solicitadas ao Cliente.

Os tempos alvo de resposta e resolução do serviço são comunicados aos Clientes a título informativo, mas o seu incumprimento não acarreta penalizações.

Exclusões

Ao calcular os tempos alvo em uma base mensal, as seguintes exclusões serão levadas em consideração:

- Problemas derivados de elementos não incluídos no serviço não serão levados em consideração.
- Não serão considerados no cálculo os tempos que coincidam com os períodos de inatividade programados, que são janelas programadas para a realização das atividades destinadas a manter a disponibilidade acordada. Os tempos de parada planejados serão pré-definidos e comunicados com no mínimo 48 horas e ocorrerão no horário de menor impacto para o Cliente.
- Os correspondentes às seguintes tarefas consideradas como tempos desculpáveis não serão considerados no cálculo:
    - Períodos de desconexão não programados solicitados pelo Cliente, geralmente associados a emergências.
    - Ataques a serviços com entrada não autorizada, desastres naturais, mudanças devido a ações governamentais, políticas ou outras ações regulatórias, ordens judiciais, greves ou disputas trabalhistas, atos de desobediência civil, atos de guerra, e outros elementos de força maior.
    - Instalação de patch.

1.12.1 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.

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

1.12.2 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 (ex: desastres naturais).

1.12.3 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.

1.12.4 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.

1.12.5 atendimento ao cliente

Após a contratação do serviço, a Vivo Empresas coloca à disposição do cliente os seguintes canais de comunicação com o SOC da Telefónica Tech.

ABERTURA E FECHAMENTO DE CHAMADOS

As solicitações sobre o serviço deverão ser efetuadas a Central de Relacionamento da Vivo Empresas pelo telefone 10315 código 1629 ou via servicosdigitais@vivo.com.br. 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, 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.

HORÁRIO E FLUXO DE ATENDIMENTO

Para os serviços na modalidade 8x5, o horário de atendimento é das 08:00 às 17:00 horas, de segunda a sexta. Para os serviços na modalidade 24x7, não há interrupção no horário 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 CONTRATADA, 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 na sua infraestrutura de segurança, 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 1), seja para abrir novas solicitações, reportar incidentes ou consultar o status de chamados abertos. A Central de Relacionamento é responsável por registrar todos os chamados dos clientes. Uma vez que se identificou que o caso está além das possibilidades de resolução pela própria Central, o chamado é direcionado para o Centro Técnico/SOC (nível 2) que, se necessário, aciona seus parceiros tecnológicos (nível 3) para atender o cliente.

NÍVEIS DE SUPORTE

O SOC disponibiliza 3 (três) níveis de suporte para atendimento aos serviços contratados pelo cliente:

- Suporte 1º Nível: realizado pela equipe do SOC que trabalha 24x7 (vinte e quatro horas por dia, sete dias por semana) para atendimento a qualquer grau de severidade de incidentes ou solicitações.
- 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, desde que aplicável.

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

1.13 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.

1.14 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.

1.15 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.