1 ESCOPO DO PROJETO

Todas as atividades previstas e os entregáveis dos serviços de segurança contemplados nessa proposta técnica e comercial para o cliente estarão descritos nesse item.

1.1 INFORMAÇÕES DO CLIENTE

A solução apresentada nessa proposta técnica e comercial foi baseada nas informações e visibilidade do ambiente de T.I. fornecidas pelo (a) <NOME DO CLIENTE>.
Caso em qualquer momento do processo de venda, implantação ou operação encontre alguma necessidade adicional decorrente de uma nova informação enviada pelo (a) <NOME DO CLIENTE>, será necessário a avaliação e poderá ter custos adicionais.

1.2 ATIVAÇÃO E CONFIGURAÇÃO DO SERVIÇO

A VIVO EMPRESAS disponibilizará um especialista em segurança da informação para conduzir as etapas necessárias para a ativação do serviço de forma remota, a partir do nosso SOC – Security Operation Center localizado no Brasil.

2 DESCRIÇÃO DO SERVIÇO – VIVO WAF

2.1 SOBRE O SERVIÇO

O **VIVO - WAF** é uma solução em Cloud que aplica diferentes funcionalidades de segurança visando proteger e possibilitar a evolução dos negócios atuais e futuros do cliente, tudo isto suportado nos serviços profissionais do nosso SOC (Security Operation Center – Centro Operacional de Segurança). O produto oferece proteção das aplicações web do cliente tais como Lojas Virtuais, Web Mail, Intranet, Extranet, dentre outras.

2.2 VIVO WAF

- O WAF funciona como um filtro que aplica regras de segurança para comunicações HTTP seguras.

- A solução analisa o tráfego HTTP/0.9, HTTP/1.0 e HTTP/1.1, detectando ataques conhecidos em diferentes camadas, incluindo rede, sistema operacional, servidor HTTP e camada de aplicação.

- Ao detectar um ataque ou qualquer atividade não autorizada, o WAF está em capacidade de:

    - Derrubar (drop) requisições e respostas evitando ataques DDOS (ataque de negação de serviço) em camada sete,
    - Bloquear uma sessão TCP,
    - Bloquear um determinado usuário,
    - Bloquear um determinado IP,
    - Bloquear um determinado IP durante um determinado intervalo de tempo.

- A solução oferece um serviço baseado na reputação do IP de origem, evitando que as aplicações do cliente sejam acessadas Botnets, ou ainda, acessos originados por endereços IPs de baixa reputação, desta maneira o WAF diferencia de forma efetiva o tráfego legítimo do tráfego malicioso.

- A solução possui mecanismos de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, campo obrigatório ou não, campo de leitura ou não, etc.) sendo capaz de diferenciar entre bots e usuários humanos protegendo contra ataques automatizados.

- O WAF executa o bloqueio através da intermediação e interrupção da conexão, ou seja, o tráfego é interceptado e a comunicação é finalizada no firewall de aplicação, não alcançando assim os aplicativos web.

2.3 AMEAÇAS AVANÇADAS

O WAF tem a capacidade de proteger as aplicações web de diferentes ameaças avançadas:

Ataque de Força Bruta	A maioria das aplicações Web oferece aos usuários vários métodos de autenticação (geralmente usuário e senha). Os ataques de força bruta estão orientados a devolver um usuário e senha a través de várias tentativas de possíveis combinações. Uma vez que o ataque tiver sucesso o usuário malicioso terá acesso a: a) Informação confidencial: documentos, perfis de usuários, status financeiros, dados bancários, etc. b) Paneis administrativos: usados pelos webmasters para administrar (alterar, excluir ou adicionar) conteúdo na aplicação web, ativar/desativar usuários, assignar diferentes permissões para usuários, etc. c) Outros vetores de ataques: o acesso a áreas privadas da aplicação web pode esconder outras vulnerabilidades ou conter funcionalidades avançadas não disponíveis para o público.
Botnets	São grupos de computadores infectados que são controlados remotamente por atacantes maliciosos com o objetivo de serem utilizados para coletar informações pessoais e cometer fraudes e roubo de identidade, realizar ataques em massa de negação de serviço em sites e empresas específicas, ou simplesmente enviar grandes quantidades de e-mail não solicitadas (spam).
Sites Legítimos Infectados	Antes era possível reduzir a ameaça de infecção simplesmente não navegando em sites de baixo renome. No entanto, atualmente, os atacantes também controlam de forma regular sites de renome e os usam para espalhar Malwares clandestinamente para os usuários desavisados da web, através de, por exemplo, código malicioso injetado dentro de sites legítimos.

Falhas de Injections (Cross-site scripting, SQL injection, File injection, etc.)	Esta ameaça incorpora links para sites maliciosos dentro de conteúdos ou sites legítimos. Assim, quando um usuário web acessa este conteúdo ou site fará o download do código malicioso hospedado nos sites ilícitos. Este processo acontece automaticamente, sem qualquer tipo de conhecimento ou intervenção do usuário.
DDOS em camada de aplicação	Este tipo de ataque tem na maioria das vezes o propósito de interromper transações ou acessar banco de dados das aplicações web. O ataque é camuflado como trafego legítimo exceto quando esta orientado para os targets na camada de aplicação. Como consequência do ataque funções como busca, navegação ou e-mail são interrompidos.

2.4 SOLUÇÃO TÉCNICA

A **Telefônica | Vivo** entende que o cliente precisa de um serviço de monitoramento e proteção de aplicações Web.

O **VIVO WAF** funciona baseado numa arquitetura Full Proxy o que garante uma proteção robusta da aplicação web. O modelo de arquitetura full-proxy estabelece duas conexões distintas entre o usuário e a aplicação uma conexão "user-side" (entre o usuário e o WAF) e outra conexão "server-side" (entre o WAF e a aplicação) oferecendo um isolamento completo entre usuário e aplicação, isso permite que o WAF aplique políticas específicas focadas em corrigir problemas peculiares no lado do usuário assim como no lado do servidor.

O modelo Full Proxy também permite o monitoramento não só das requisições dos usuários como também das respostas dos servidores conforme diagrama abaixo:

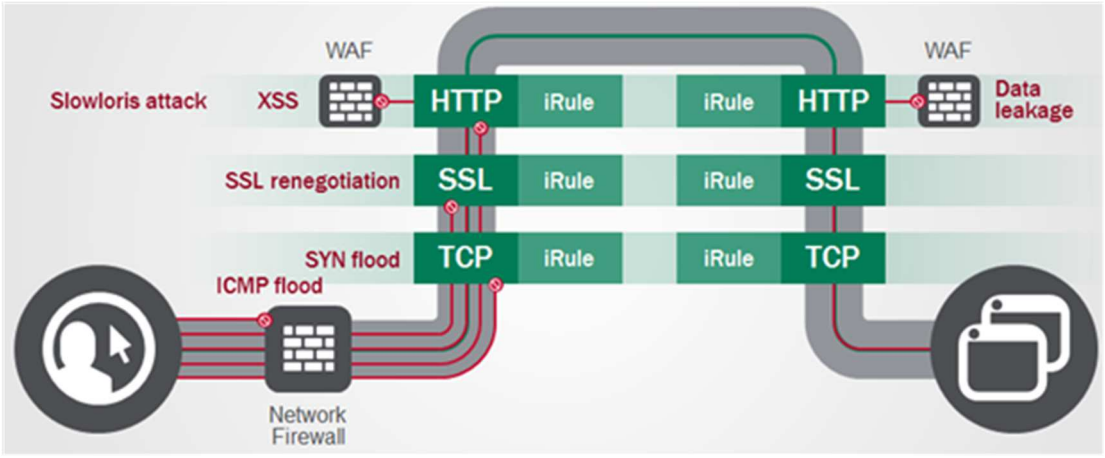

Gráfico 1: Arquitetura do Produto

O WAF garante uma comunicação HTTP segura entre usuário e servidor a partir de um conjunto de regras definidas as quais são retroalimentadas:

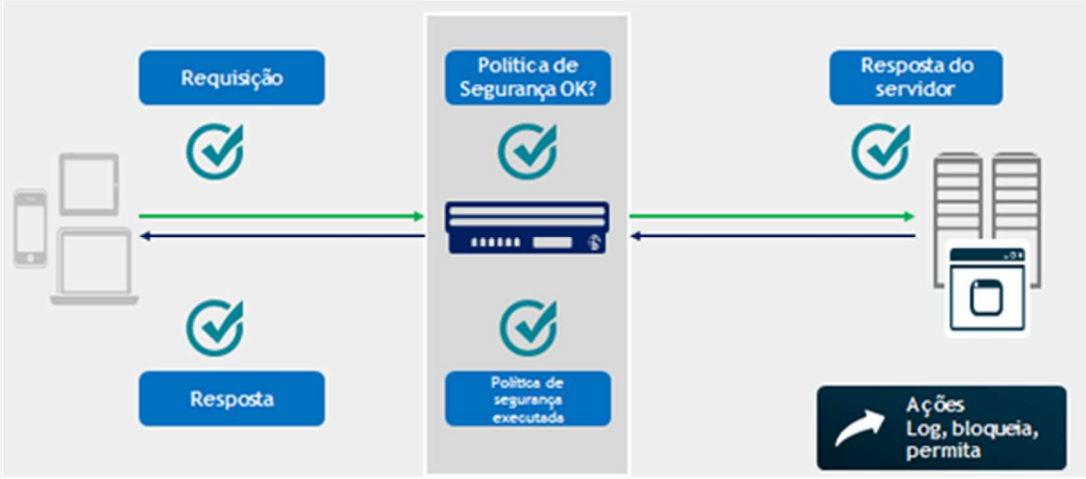

Gráfico 2. Exemplo do funcionamento do WAF

A solução recebe e verifica as requisições iniciadas pelos usuários, aplica as políticas de segurança pré-definidas, estabelece a comunicação com o servidor, analisa as respostas do

servidor, aplica as políticas de segurança pertinentes ao lado do servidor e entrega o conteúdo ao usuário, garantindo assim o máximo de segurança na camada da aplicação.

3 CONDIÇÕES DE PRESTAÇÃO DE SERVIÇO

3.1 FECHAMENTO DE CHAMADO

O chamado somente será concluído, pela Central de Relacionamento, com o "de acordo" dado por um dos dois três (3) administradores designados previamente pelo cliente, sendo o contato efetuado por telefone ou e-mail. Caso o administrador não responda ao e-mail ou retorne contato telefônico em até 72 horas o SOC entenderá que o chamado está adequadamente atendido fechando o chamado automaticamente.

3.2 HORÁRIO DE ATENDIMENTO

- A prestação do serviço para atendimento e mitigação de problemas ou ataques ocorre 24x7.
- O atendimento a consultas e solicitações ocorre na modalidade 8x5

3.3 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 **Telefônica | Vivo**, sendo tal atividade atribuída apenas à equipe de suporte do cliente (contatos autorizados pelo Cliente).

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

O ponto de contato do cliente para abertura de Novas Incidentes, Solicitações e Consultas, assim como também para consultar o status dos chamados abertos, será a Central de Relacionamento (nível 1). A Central de Relacionamento é responsável por registrar 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 de Clientes (nível 2) que, se necessário, aciona o SOC de Redes ou Fabricante (nível 3) para atender o cliente.

Para reportar incidentes, o cliente poderá acionar diretamente o Centro Técnico/SOC de Clientes (nível 2).

Gráfico 3: Fluxo de Atendimento

3.4 SUPORTE

O serviço contempla suporte com disponibilidade 24x7, para atender as consultas e solicitações do cliente. Após a contratação do serviço, o cliente receberá o procedimento de ação para casos de eventos e os telefones e correios eletrônicos destinados a qualquer solicitação e eventos no serviço.

3.5 ACORDOS DE NÍVEL DE SERVIÇO (SLA)

Este item tem como objetivo estabelecer e fornecer informações a respeito do acordo de nível de serviço que irá definir os padrões de qualidade para o **VIVO APLICAÇÃO WEB SEGURA - WAF** oferecido pela **Telefônica | Vivo**.

3.5.1 DESCRIÇÃO DAS SEVERIDADES

As severidades são definidas de acordo com impacto do evento, conforme tabela 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 indisponibiliza os 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, pouco ou nenhum impacto na operação.

Tabela 1: Critérios de Severidade – Incidentes

3.5.2 SLO DE PRESTAÇÃO DE SERVIÇOS

O **VIVO APLICAÇÃO WEB SEGURA - WAF** é prestado considerando os seguintes objetivos de atendimento:

3.5.3 SLO DE INCIDENTES

Serviço	Definição	Crítico	Alto	Médio	Baixo
Todos	**Tempo de atendimento** a partir da comunicação do cliente até a atribuição do ticket a um analista do SOC	30 min.	45 min.	1,5h (8X5).	2,5h. (8X5)
Todos	**Tempo de resposta** a partir da comunicação do cliente até que SOC faça o primeiro diagnóstico	1,5h.	2h.	3,5h. (8x7)	6,5h. (8x5)
Todos	**Tempo de resolução** a partir da comunicação do cliente até que o SOC comunique a resolução do mesmo	4,5h.	6,5h.	24h. (8x7)	36h. (8x5)

Tabela 2: SLO de Incidentes.

O SLO de incidentes é medido em 24x7 (horas por dia x dias por semana), exceto quando explicitamente atendimento em horário comercial (8x5) ou horário comercial estendido (8x7).

3.5.4 SLO DE APRESENTAÇÃO DOS RELATÓRIOS

Serão gerados os seguintes tipos de relatório segundo o definido junto ao cliente e atendendo o seguinte SLO:

- Relatório Padrão: O serviço inclui a entrega de relatório mensal padrão.

- Relatório Sob Demanda: O cliente poderá solicitar relatórios sob demanda desde que tenha contratado o complemento respectivo segundo item 3.5

Quando o cliente contratar o pacote de Relatório Sob Demanda, será enviado junto com o formulário de ativação do WAF o formulário de geração de relatórios. Este relatório deverá ser entregue junto com o formulário de ativação dentro dos prazos acordados dentro desta proposta.

Uma vez definidos o(s) relatório(s) segundo necessidade do cliente o SLO para apresentação destes relatórios será o mesmo que o definido para o relatório padrão mensal.

Serviço	Definição	Prazo
VIVO APLICAÇÃO WEB SEGURA - WAF	**Tempo de entrega** de relatórios mensais	Até o 10º dia útil do mês subsequente

Tabela 3: SLO de Apresentação de relatórios

3.5.5 SLO DE SOLICITAÇÕES E CONSULTAS

Todas as Solicitações e Consultas serão registradas pela Telefônica | Vivo com severidade "Baixa" e atendidas em regime de 8x5 e terão seu SLO medido em horas comerciais (úteis).

Considera-se que as Solicitações e Consultas utilizarão os mesmos valores de SLO's que os incidentes de severidade baixa.

a) Indicadores de Consultas

São previstas as seguintes consultas para este serviço:

- Trafego da aplicação
- Aplicações mais acessadas
- Usuários que mais utilizaram serviços
- Latência da aplicação
- Principais ataques

b) Indicadores de Solicitações

Para atendimento de solicitações será solicitado ao cliente o envio de formulário específico, corretamente preenchido. Em caso de falta do mesmo, ou de erro no preenchimento, o SOC devolverá o formulário ao solicitante com a indicação do problema e aguardará o seu retorno. Este período não será contabilizado no cálculo do SLO.

São previstas as seguintes solicitações para este serviço:

- Modificação da lista de contatos autorizados do cliente.
- Inclusão/Alteração/Remoção de aplicações web, em acordo com o plano contratado.

Serviço	Definição	Severidade Baixa	
WAF	**Tempo de atendimento** de solicitações e consultas: A partir da comunicação do cliente até a atribuição do ticket a um analista do SOC.	2h.	úteis
WAF	**Tempo de resolução** de consultas: A partir da comunicação do cliente até que o SOC comunique a resolução do mesma.	8h.	úteis
WAF	**Tempo de resolução** de solicitações: A partir da comunicação do cliente até que o SOC comunique a resolução da mesma.	16h	úteis

Tabela 4: SLO de Solicitações e Consultas

3.5.6 SLA DE PRESTAÇÃO DE SERVIÇO

a) **Objetivo:** Garantir o atendimento de 95% dos SLOs por mês.

b) **SLA de disponibilidade do produto:** A disponibilidade do serviço seguirá o seguinte modelo:

Serviço	Disponibilidade
Vivo Aplicação Web Segura	99,99%

Tabela 5: Disponibilidade do Serviço

Somente se considera para efeitos de penalização:

- Incidentes Críticos e Altos
- As requisições categorizadas como Altas pelo cliente na abertura do chamado

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

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

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

Tabela 6: Índices de descontos

3.5.7 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 comprometido a facilitar o acesso a suas dependências, das pessoas designadas pela **Telefônica | Vivo**, para a resolução dos problemas, ou a operação do serviço que seja necessária. O tempo necessário para obter esta permissão está fora do cálculo da disponibilidade;
- A **Telefônica | Vivo** 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 ou de força maior).

3.5.8 PERIODOS DE MANUTENÇÃO

Por necessidade de manutenção, pode ser necessário deixar sem serviço a rede do Cliente, com o objetivo de executar reconfigurações, atividades de manutenção, etc., na rede. Tais atividades serão executadas, necessariamente, durante um período pré-programado de manutenção.

3.5.9 INTERRUPÇÕES PROGRAMADAS

As interrupções programadas de disponibilidade do serviço sejam elas pelas causas motivadas pelo item anterior, de períodos de manutenção, ou motivadas por alguma solicitação do Cliente, não serão contabilizadas para o cálculo da disponibilidade do serviço, constantes no Compromisso de Qualidade do Serviço.

3.6 RESPONSABILIDADES DO CLIENTE

Clientes que por ventura venham a contratar serviços da **Telefônica | Vivo** estarão assumindo as seguintes as responsabilidades:

- Fornecer a **Telefônica | Vivo** as informações necessárias para ativação da solução dentro do prazo estabelecido no ponto **5.7**.
- Informar a **Telefônica | Vivo** 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. O Cliente deverá fornecer informações suficientes com relação às suas necessidades.

- Informar a **Telefônica | Vivo** com antecedência mínima de 30 (trinta) dias, sobre qualquer mudança que possa afetar a prestação de Serviços.
- Zelar pela conservação e correto manuseio da infraestrutura disponibilizada pela **Telefônica | Vivo**, responsabilizando-se pelos eventuais danos, pessoais e materiais, decorrentes de ações e utilizações indevidas por parte de seu pessoal ou de seus equipamentos.
- Definir prioridades/graus de severidade de atendimento
- Informar internamente e aos seus outros prestadores de serviços, o escopo de contrato com a **Telefônica | Vivo**, quando relacionado à suas atividades.
- Não gerenciar diretamente nenhum funcionário ou terceiros da **Telefônica | Vivo** alocados ou em atendimento nos sites do cliente
- Providenciar as autorizações de ingresso do pessoal da **Telefônica | Vivo** às suas instalações para executar o projeto contratado (caso for necessário).
- Designar um único interlocutor como responsável pelo projeto, e definir as pessoas de contato autorizadas a realizar consultas.
- Analisar o produto gerado e aprová-lo quando corresponder, garantindo a continuidade das diversas atividades do projeto e possibilitando seu fechamento quando os requisitos definidos para o projeto forem atendidos.
- Brindar a correspondente diligência nos trabalhos que lhe sejam próprios a executar dentro dos prazos do planejamento proposto.
- Designar o pessoal necessário, especializado nas funções a realizar e com dedicação suficiente a essas tarefas, para coordenar e entregar a **Telefônica | Vivo** a informação necessária para análise e resolução de eventos.
- Proporcionar, conforme corresponda, a infraestrutura necessária para instalação de equipes, cumprindo com as especificações indicadas nesta oferta.
- Manter atualizada junto à **Telefônica | Vivo** a lista de pessoas autorizadas a abrir chamados e solicitações de suporte.

3.7 RESPONSABILIDADES DA TELEFÔNICA | VIVO

A **Telefônica | Vivo** assume as seguintes responsabilidades perante os Clientes que venham a contratar seus serviços.

- Designar um profissional **Telefônica | Vivo** que será ponto focal para o projeto;
- Tornar disponíveis recursos **Telefônica | Vivo** 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 **Telefônica | Vivo** e conforme estabelecido no contrato com o cliente;
- Cumprir os prazos estabelecidos nas atividades do projeto, desde que as responsabilidades do cliente sejam cumpridas;
- Gerenciamento proativo do serviço incluindo o fornecimento da Central de Atendimento.
- Dirigir, organizar e gerenciar o projeto.
- Participar nas reuniões de trabalho combinadas.
- Manter informado o pessoal do cliente sobre ações e resultados nas diferentes atividades.
- Garantir a confidencialidade dos dados informados pelo cliente para o desenvolvimento da atividade.
- O pessoal da **Telefônica|Vivo** que tiver acesso aos escritórios do cliente estará sujeito às normas de segurança que o cliente estabelecer para acesso e permanência em suas instalações.
- Comunicará e solicitará ao cliente, a aprovação explícita de qualquer mudança da equipe de trabalho, com uma antecipação mínima de sete (7) dias corridos.

3.8 CONDIÇÕES DE ACEITAÇÃO DO SERVIÇO

O serviço será implantado nas unidades da **<<NOMECLIENTE>>**, conforme o Cronograma de Implantação acordado previamente entre as partes.

A **<<NOMECLIENTE>>** fará o aceite da configuração dos serviços na nuvem no prazo de 5 (cinco) dias úteis. Ao final deste período, caso a **<<NOMECLIENTE>>** não se manifeste formalmente em contrário, o serviço será considerado aceito.

3.8.1 REUNIÃO TÉCNICA

A **Telefônica | Vivo** irá se reunir com a equipe técnica do cliente no prazo máximo de **30 dias úteis** após a assinatura do contrato, para o planejamento da implantação do serviço a ser fornecido. Nesta reunião deverão ser discutidos e esclarecidos todos os questionamentos técnicos do serviço assim como as definições técnicas de configuração dos serviços e atividades de responsabilidade do cliente.

3.8.2 FORMULÁRIO DE ATIVAÇÃO

Após reunião técnica será disponibilizado um formulário técnico de ativação para identificação dos pré-requisitos e compatibilidades da solução, com as aplicações do cliente. O cliente deve preencher e retornar o formulário de ativação no prazo máximo de **30 dias** corridos caso contrário à solução será configurada conforme o seguinte padrão:

- Nenhuma aplicação web pode ser automaticamente incluída na solução WAF, se contratada;
- Apenas os contatos técnicos ou responsáveis informados nesta proposta podem entrar em contato com o SOC para configurações posteriores.

3.8.3 INSTALAÇÃO DO SERVIÇO

O prazo previsto para instalação do serviço é de até **30 dias corridos**, contados após a disponibilização dos dados necessários para a configuração da solução, através de cronograma a ser estabelecido de comum acordo entre as partes. Este prazo não contempla a disponibilização de equipamentos, no caso de vendas ou locação, assim como os prazos de instalação de links de dados, quando inclusos nos projetos. Limitações ou situações específicas de cada cliente e projeto podem causar variação nos prazos estabelecidos.

Ao finalizar o período de provisão do serviço, o cliente e **Telefônica|Vivo** acordarão testes de configuração para verificar o funcionamento correto de cada uma das funcionalidades do produto. Com o objetivo de customizar os limiares de detecção para aperfeiçoar o serviço ao cliente, a **Telefônica|Vivo** solicitará poderá solicitar ao cliente informações específicas de sua infraestrutura de rede interna e equipamentos de segurança existente. Tais informações serão confidenciais e não poderão ser divulgadas pela **Telefônica|Vivo**.

Estes prazos também são aplicados nos seguintes cenários:

- Solicitação de Upgrade/Dowgrade do produto.
- Solicitação de baixa (cancelamento) do produto.
- Solicitação de reconexão do produto.