

TENURE

DESCRIÇÃO DO PRODUTO

1. SERVIÇO TENURE

O serviço de Big Data Tenure visa verificar o tempo de permanência do usuário que está vinculado a um número de telefone com sua operadora móvel atual.

1.1 VANTAGENS DA SOLUÇÃO

- Tomada de decisão aprimorada: Fornece aos clientes informações cruciais para decisões mais precisas.
- Redução de fraudes: Ajuda a identificar potenciais atividades fraudulentas relacionadas à troca recente de números telefônicos.
- Reforça a segurança e confiabilidade dos produtos de identidade da empresa.
- Maior precisão na verificação de identidade dos usuários.
- Diminuição do risco de fraudes associadas à troca recente de números telefônicos.

1.2 FACILIDADES

A API funcionará mesmo que o dispositivo esteja desligado, fora de cobertura, wi-fi etc.

A API define um serviço de endpoint:

É necessário o identificador de assinatura de rede (por exemplo, MSISDN para redes móveis) e a data mínima de posse especificada para validar a assinatura de rede associada. Este endpoint responderá com uma confirmação se a permanência do assinante da rede é maior que o carimbo de data e hora especificado.

Para chamar esse endpoint, o consumidor da API deve primeiro obter um token de acesso válido com o escopo especificado do endpoint do token especificado, que é então passado para o endpoint por meio do cabeçalho `Authorization`.

200 – informa quando a assinatura móvel identificada tiver tido um período de vigência válido

Ou códigos de erro 400, 401, 403, 404 e 422

As consultas com retorno 200 serão cobradas.

2. SLA DE DISPONIBILIDADE

A VIVO obriga-se a manter uma taxa de disponibilidade dos seus sistemas e serviços em no mínimo 95% (noventa e cinco por cento) das requisições, consideradas as consultas mensais efetuadas pelo PARCEIRO.

- A taxa de disponibilidade é definida como a quantidade de requisições e consultas em um dado período de tempo que, obedecendo à especificação de integração, não recebe algum código de erro sistêmico como resposta à chamada.

Serão considerados erros sistêmicos:

- Aquelas requisições cujos códigos de resposta HTTP padrão pertencerem à classe 5XX, a exemplo de (mas não se limitando a): 500 (Internal Server Error), 502 (Bad Gateway), 503 (Service Unavailable) e 504 (Gateway Timeout), etc.
- Aquelas requisições que obtiverem falha na autenticação das credenciais (usuário de login e senha) do PARCEIRO ou falha na permissão de acesso aos serviços/produtos da VIVO (a exemplo dos códigos de erro 400-Bad Request, 401-Unauthorized e 403-Forbidden), nos casos em que houver alguma alteração por parte da VIVO - seja nas características de acesso do PARCEIRO ou nas características dos produtos/serviços - sem comunicação prévia realizada pela VIVO com antecedência de 15 dias e formalizada por escrito.
- Aquelas requisições cujo retorno não estiver previsto como HTTP padrão.

Não serão erros sistêmicos aqueles MSISDNs e/ou IPs não presentes na base de dados da VIVO.

3. SLA DE REPARO

Aplicam-se aos serviços de Suporte e atendimento providos pela VIVO, o SLA previsto abaixo.

Suporte N1 e N2:

Severidade	Disponibilidade do Serviço	Tempo de Atendimento	Tempo de Restabelecimento	Tempo de Solução Definitiva
Crítica	24x7	15 minutos	12 horas	2 dias úteis
Alta	24x7	30 minutos	24 horas	4 dias úteis
Média	24x7	3 horas	36 horas	5 dias úteis
Baixa	24x7	24 horas	48 horas	7 dias úteis

Suporte N3: Disponibilidade 8x5.

Será passível de expurgo de SLA:

- Manutenções emergenciais solicitadas pela área de Segurança da Informação, com notificação de até uma hora após a interrupção, contendo a razão que gerou a demanda.
- Manutenções corretivas, acordadas e agendadas previamente entre as ambas as partes.

Para fins de aplicação dessa cláusula, serão considerados os seguintes critérios para classificação da severidade:

Severidade 1 – Crítico: Os chamados nessas condições são aqueles nos quais o PARCEIRO encontra-se impossibilitado de realizar com sucesso (sem retorno de erro) qualquer requisição/consulta sistêmica aos serviços e produtos da VIVO e não possui solução de contingência.

Exemplos:

- Usuário ou senha do PARCEIRO foram bloqueados, impedindo a consulta por API
- Kernel está indisponível, fora do ar ou retornando erros para todas as requisições/consultas.

Severidade 2 - Alta: Os chamados nessas condições são aqueles nos quais o PARCEIRO encontra-se impossibilitado de realizar com sucesso (sem retorno de erro) requisições/consultas sistêmicas às APIs do Open Gateway porém possui uma solução de contingência manual ou por outro meio que não anteriormente previsto, implicando em esforço operacional do lado do PARCEIRO para manter a operação.

Encontram-se nessa categoria também os chamados relacionados a potenciais desvios de qualidade dos dados de forma não localizada, ou seja, que impactem de forma generalizada a maioria das requisições/consultas realizadas pelo PARCEIRO às APIs do Open Gateway.

Exemplo:

- Plataforma do PARCEIRO está retornando erros para a maioria das consultas realizadas em um determinado período de tempo.

Severidade 3 - Média: Os chamados nessas condições são aqueles nos quais o PARCEIRO encontra alguma dificuldade de estabilidade na realização de requisições/consultas sistêmicas pelos meios previstos, bem como os potenciais desvios de qualidade localizados e que impactem um subconjunto limitado das requisições/consultas realizadas pelo PARCEIRO às APIs do Open Gateway. Em ambos os casos, o impacto deve estar limitado a um subconjunto minoritário do total de requisições/consultas realizados - caso impactem um subconjunto majoritário, o problema é classificado como severidade 2.

Exemplos:

- Plataforma do PARCEIRO está retornando erros para uma quantidade minoritária de consultas realizadas em um determinado período de tempo.
- Requisições estão recebendo um tratamento não esperado para um tipo específico de consumidor.

Severidade 4 - Baixa: Os chamados nessas condições são referentes às solicitações nas quais se trata de

um problema menor que requer ação, mas não afeta a capacidade do PARCEIRO de usar as APIs do Open Gateway sem impacto operacional por parte do PARCEIRO.

Exemplos:

- Correções de usabilidade do Software, como, por exemplo, bugs de baixo impacto.

A VIVO disponibilizará o atendimento para o PARCEIRO por meio de canais descritos abaixo, destinados para atendimento de demandas de suporte, disponível todos os dias da semana, 24h por dia, inclusive feriados. Por meio do qual a solicitação do PARCEIRO será tratada individualmente.

Canais de contato:

Envie e-mail para missaocritica@vivo.com.br ou ligue para 0800 0151551 (opção 8)

A confirmação pela VIVO do recebimento da solicitação se dará através de envio de recibo/notificação de entrega com sucesso do e-mail para o remetente.

MANUTENÇÕES TÉCNICAS

A VIVO possui janelas de manutenções. As manutenções técnicas emergenciais não programadas devem ser comunicadas ao PARCEIRO em até 1h a partir do seu início.

6) CONSIDERAÇÕES:

Todas as cláusulas e premissas desse anexo poderão ser revisadas e alteradas a qualquer tempo, uma vez que o programa EAP trata-se de período de Prova de Conceito, no qual, inclusive, todos os itens referentes ao nível de serviço (SLA) também serão analisados. As alterações e revisões neste Anexo II deverão ter consentimento mútuo entre as partes e formalizadas através de instrumento particular devidamente assinado ou comunicação por e-mail entre as partes.