Monitor da 2N5

Documentação

O guia do usuário, o produto, a referência de telefonia, os guias e os termos em vigor, num só documento.

Versão	25 de outubro de 2026
Publicado por	2N5
Site	monitor.2n5global.com

Sumário

Guia do usuário

- Primeiros passos
- O painel
- A página de um circuito de voz
- Circuitos de dados e o agente
- Sites e e-mail
- Incidentes e alertas
- Relatórios
- Pessoas e organizações
- Configurações
- Perguntas e ajuda

O produto

- Como funciona o monitoramento VoIP gerenciado da 2N5
- Monitoramento de troncos SIP e VoIP com chamadas reais
- Teste e monitoramento de 0800 e URA
- Qualidade de voz VoIP medida com MOS-LQO
- Alerta de queda de linha e escalonamento
- Relatório de SLA da operadora, mensal e anual
- Monitoramento de link de internet de cada filial
- Monitoramento de sites e conteúdo
- Monitoramento de e-mail e caixa cheia
- Segurança e LGPD no monitoramento VoIP da 2N5
- Planos e preços do monitoramento de 0800, URA e troncos SIP

Referência

- Códigos SIP
- Causas Q.850
- Glossário

Guias

- 0800 não completa? Como monitorar 0800 e URA
- Alerta de queda de linha sem falso alarme
- Chamadas falhando: diagnóstico por código SIP e Q.850
- Como cobrar o SLA da operadora com provas
- Decreto do SAC e RGC: como provar que o 0800 estava no ar
- Ligação muda e áudio de um lado só no VoIP
- Monitoramento de troncos SIP, 0800 e URA: guia
- Monitoramento passivo vs chamadas de teste ativas
- O que é monitoramento sintético de chamadas
- Por que um 0800 não completa do celular?
- Qualidade de voz: MOS e MOS-LQO na prática
- SLA de telefonia: cálculo anual e mensal

Termos e privacidade

- Termos de Uso
- Política de Privacidade

Guia do usuário

GUIA DO USUÁRIO · CAPÍTULO 1

Primeiros passos

Para começar a usar o Monitor da 2N5, abra o convite que a 2N5 enviou por e-mail, crie a sua senha e entre. Este capítulo mostra a primeira entrada, a verificação em duas etapas, como recuperar a senha e onde trocar o idioma e o tema.

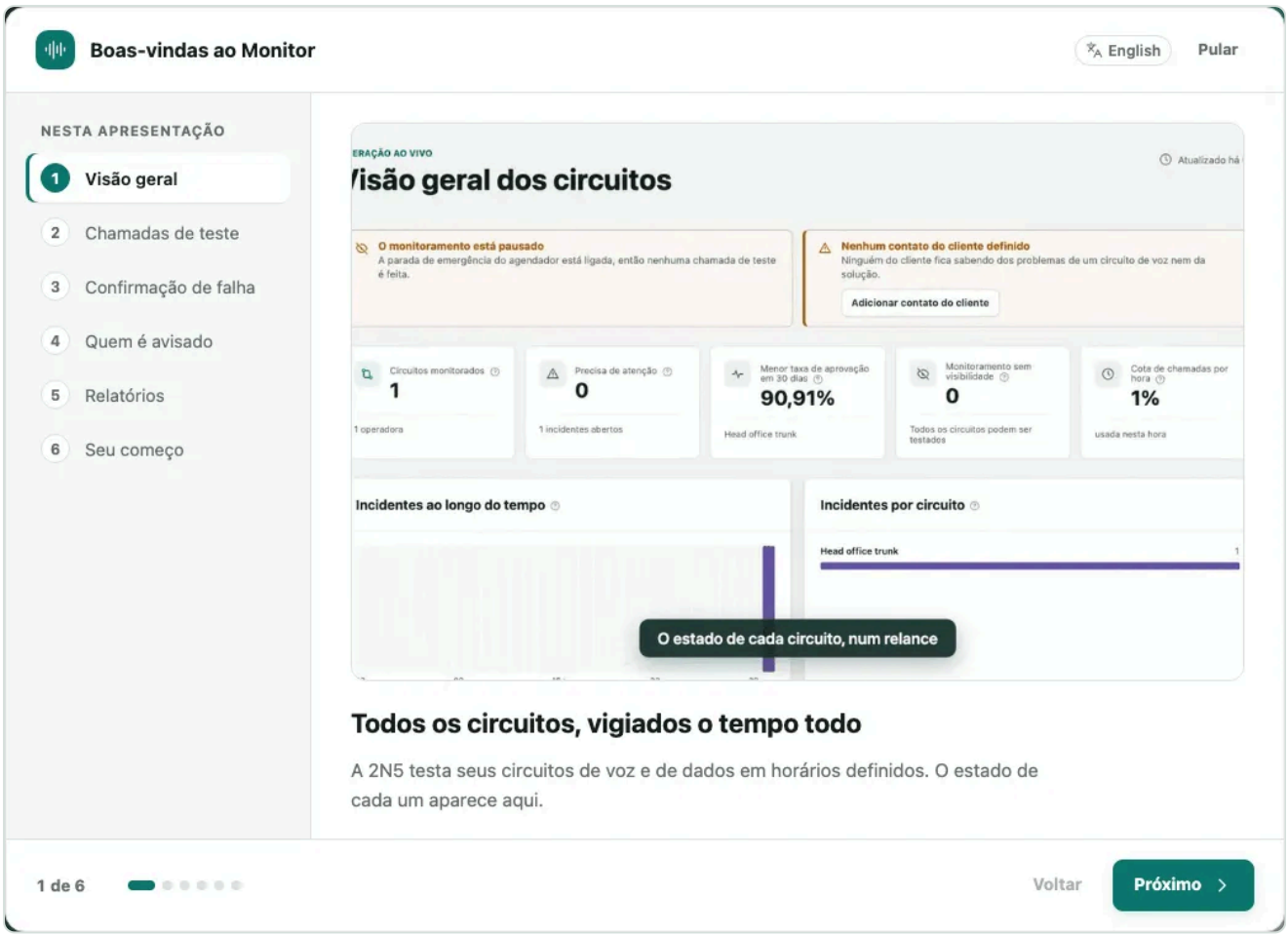
Por Equipe 2N5 Atualizado em 14 de outubro de 2026

Entrar pela primeira vez

Você não precisa criar uma conta: a 2N5 cadastra a sua organização e envia um convite para o seu e-mail.

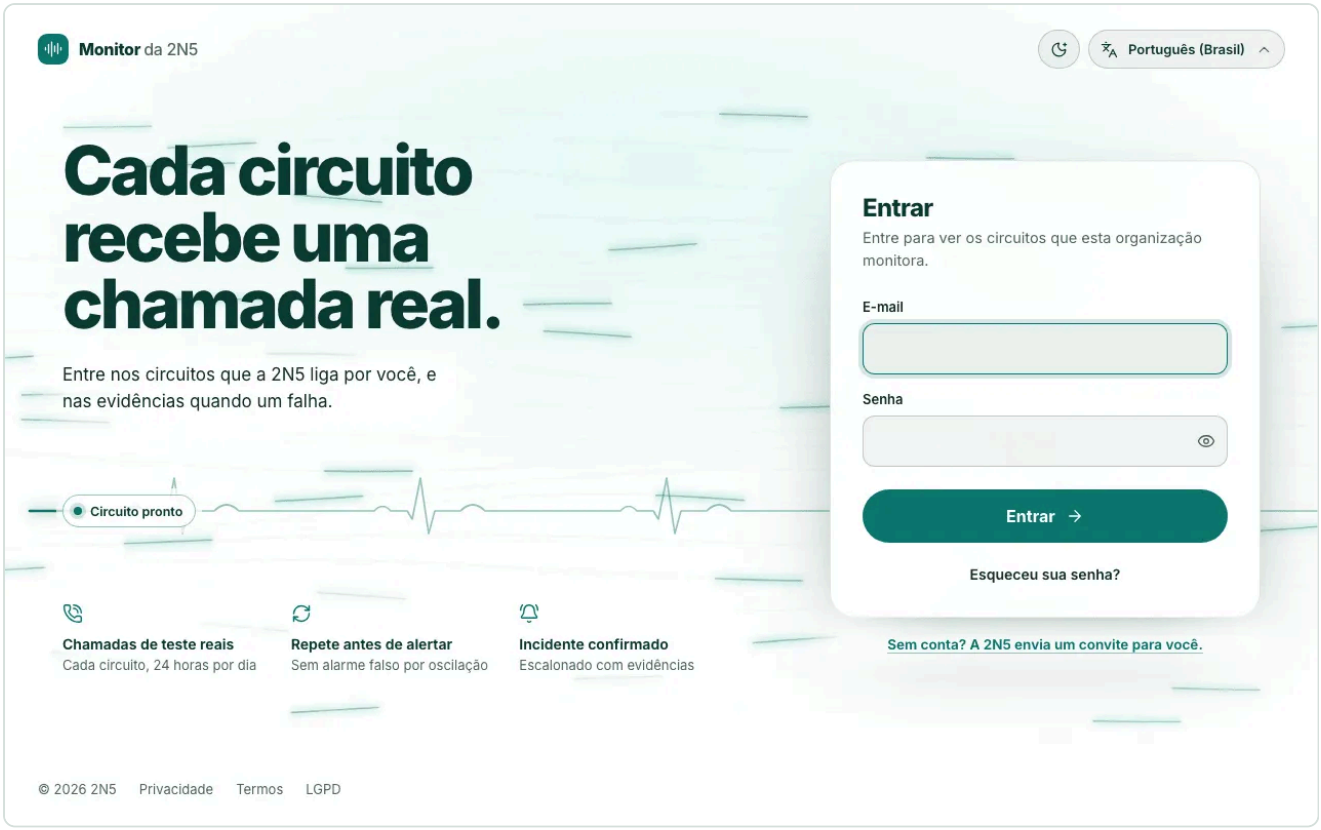
1. Abra o e-mail de convite e clique no link. A página **Gerenciar** mostra o nome da sua organização e o seu nome, que já vem preenchido.
2. Digite a sua senha em **Senha** e repita em **Confirme a senha**.
3. Marque a caixa que aceita os Termos de Uso e confirma a leitura da Política de Privacidade.
4. Clique em **Começar a gerenciar**. O Monitor abre o painel da sua organização.

Na primeira entrada, uma apresentação curta, **Boas-vindas ao Monitor**, explica em seis passos como o Monitor trabalha. Use **Próximo** para avançar ou **Pular** para fechar. No último passo você pode começar o tour guiado, que para uma vez em cada página.



Nas próximas vezes, entre pelo endereço do Monitor:

1. Digite o seu **E-mail** e a sua **Senha**.
2. Clique em **Entrar**.



Proteger a conta com a verificação em duas etapas

A verificação em duas etapas pede, além da senha, um código de seis dígitos gerado por um aplicativo autenticador no seu celular. Recomendamos ativar. A sua organização pode torná-la obrigatória para todos os gestores; nesse caso o Monitor pede a configuração logo depois da senha.

1. No canto inferior esquerdo, clique no seu nome e escolha **Configurações da conta**.
2. No quadro **Verificação em duas etapas**, clique em **Configurar**, e de novo em **Configurar** na janela que abre.
3. Escaneie o QR code com o aplicativo autenticador. Se preferir, copie a **Chave de configuração** com **Copiar chave** e cole no aplicativo.
4. Digite em **Código do aplicativo autenticador** o código que o aplicativo mostra e clique em **Ativar**.
5. Guarde os códigos de recuperação com **Copiar** ou **Baixar** e clique em **Concluir**. Cada código substitui o aplicativo uma vez, se você perder o celular.

Daqui em diante, depois da senha, o Monitor pede o código do aplicativo. Digite o código e clique em **Verificar**. Sem o celular, escolha **Usar um código de recuperação**.

Esqueceu a senha

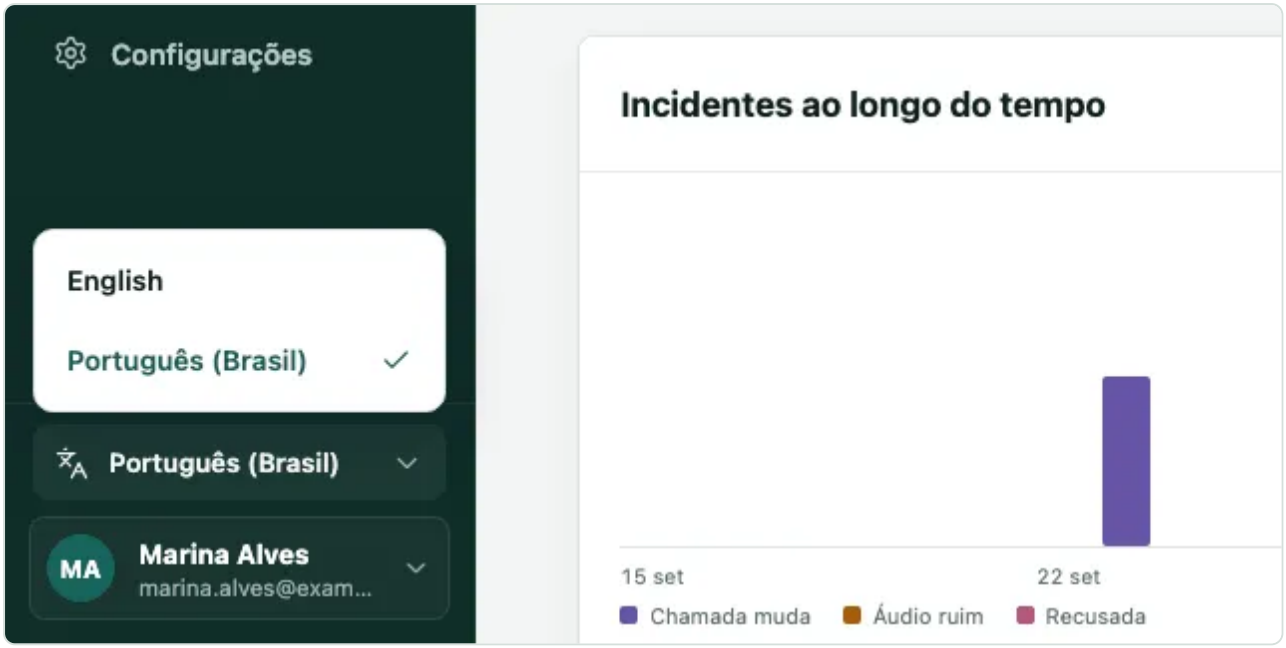
1. Na tela de entrada, digite o seu e-mail em **E-mail**.
2. Clique em **Esqueceu sua senha?**. Se o endereço tiver uma conta, um link de redefinição chega por e-mail.
3. Abra o link. Na página **Defina uma nova senha**, digite a nova senha em **Nova senha** e em **Confirme a nova senha**.
4. Clique em **Definir senha** e depois em **Ir para o login**.

Trocar a senha encerra todas as sessões que estavam abertas na sua conta, em qualquer computador. Para trocar a senha sem esquecê-la, use o quadro **Senha** em **Configurações da conta**.

Idioma

O Monitor fala português do Brasil e inglês. O idioma escolhido fica salvo na sua conta.

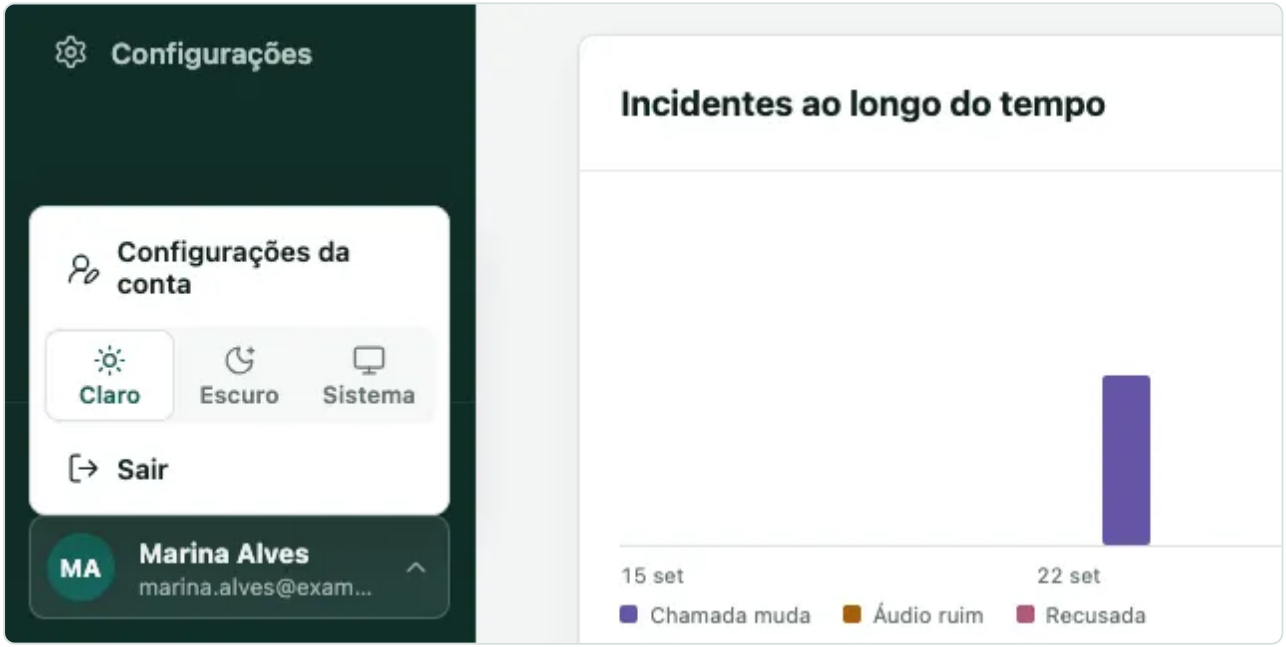
1. No menu lateral, clique no idioma atual, logo acima do seu nome.
2. Escolha **English** ou **Português (Brasil)**.



A tela de entrada também tem o seletor de idioma, no canto superior direito.

Tema claro ou escuro

1. Clique no seu nome, no canto inferior esquerdo.
2. Escolha **Claro**, **Escuro** ou **Sistema**. **Sistema** acompanha o tema do seu computador.



No mesmo menu, **Sair** encerra a sessão neste computador. Para encerrar em todos, use **Sair de todos os dispositivos** em **Configurações da conta**.

Perguntas frequentes

Não recebi o convite. O que faço?

Confira a caixa de spam e as abas de promoções do seu e-mail, procurando uma mensagem da 2N5. Se não encontrar, peça à 2N5 que reenvie o convite: o link vale por sete dias e um convite novo substitui o anterior. Quem já é gestor da sua organização também pode convidar você pela tela Gestores, com o botão Convidar gestor.

Perdi o celular com o aplicativo autenticador. Como entro?

Na tela do código, escolha Usar um código de recuperação e digite um dos códigos que você guardou quando ativou a verificação em duas etapas. Cada código vale uma vez. Se não tiver mais nenhum, peça à 2N5 ou a outro gestor da sua organização que redefina a sua verificação em duas etapas; depois você a configura de novo no celular novo.

O idioma que eu escolho vale para os alertas também?

Não. O idioma do menu lateral vale para as telas que você vê e fica salvo na sua conta, então outro computador abre no mesmo idioma. O idioma de cada alerta por e-mail é o do contato que o recebe, definido no cadastro dele na tela Escalonamento, e o dos relatórios é escolhido na hora de enviar.

GUIA DO USUÁRIO · CAPÍTULO 2

O painel

O painel é a primeira tela depois da entrada e responde a uma pergunta: está tudo funcionando agora? A aba Circuitos mostra os circuitos de voz e de dados, e a aba Serviços online mostra os sites e as caixas de e-mail.

Por Equipe 2N5 Atualizado em 21 de outubro de 2026

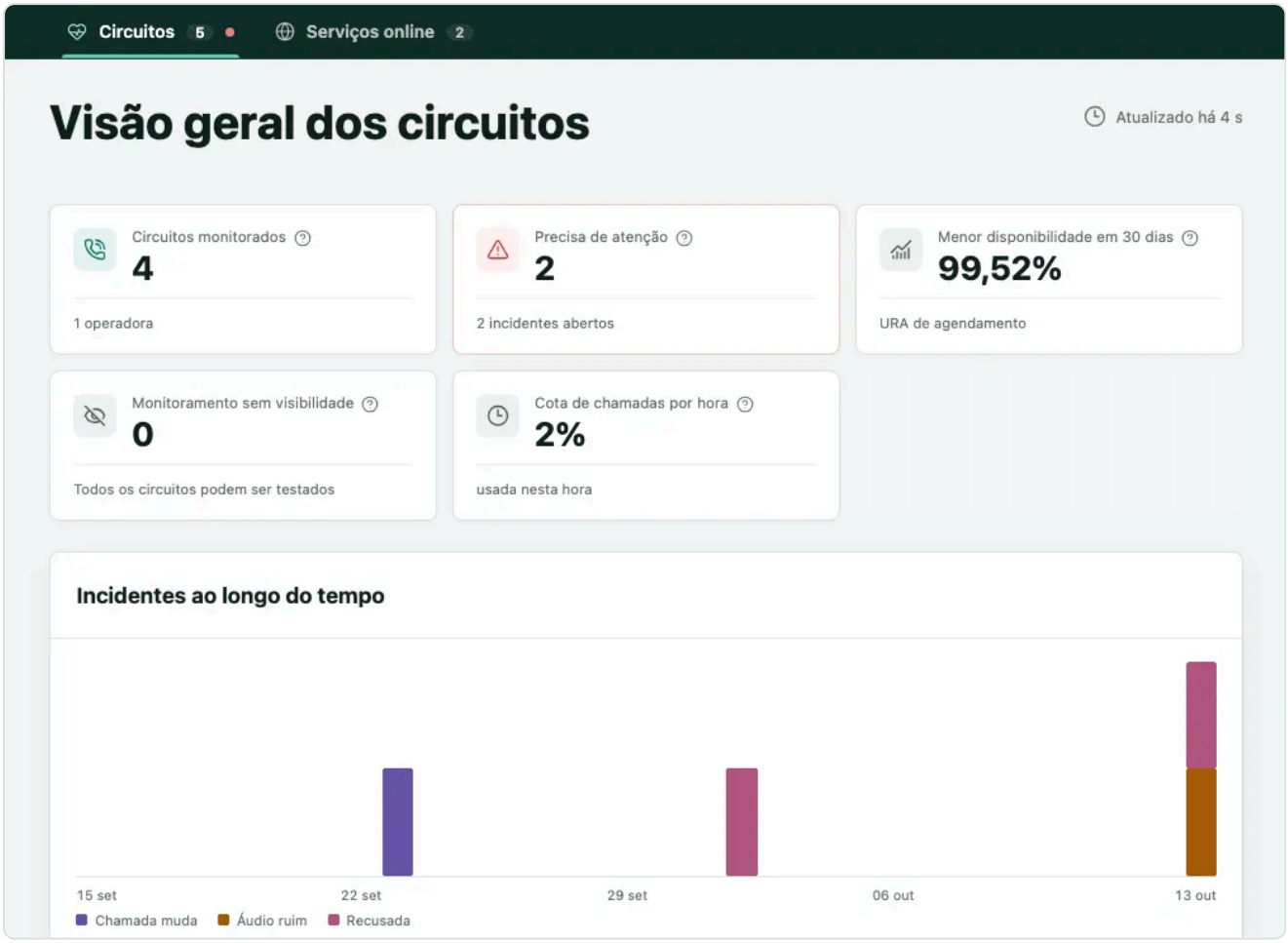
O que o painel mostra

1. No menu lateral, clique em **Painel**.
2. No topo, escolha a aba **Circuitos** ou **Serviços online**. O número em cada aba é quantos itens ela mostra; um ponto vermelho avisa que algo está fora do ar.

Na aba **Circuitos**, a página **Visão geral dos circuitos** abre com cinco números:

- **Circuitos monitorados**: quantos circuitos de voz a sua organização acompanha.
- **Precisa de atenção**: circuitos fora do ar, degradados ou suspeitos, e quantos incidentes estão abertos.
- **Menor disponibilidade em 30 dias**: o circuito com a pior disponibilidade do último mês, e o valor dela.
- **Monitoramento sem visibilidade**: circuitos que o Monitor não conseguiu testar. Isso é um problema da 2N5, não uma queda sua.
- **Cota de chamadas por hora**: quanto da cota de chamadas de teste desta hora já foi usada.

Abaixo, o gráfico **Incidentes ao longo do tempo** mostra os incidentes dos últimos 30 dias, com uma cor para cada tipo de falha.



Estados e cores

A tabela **Circuitos de voz e de dados** lista cada circuito com o seu estado atual:

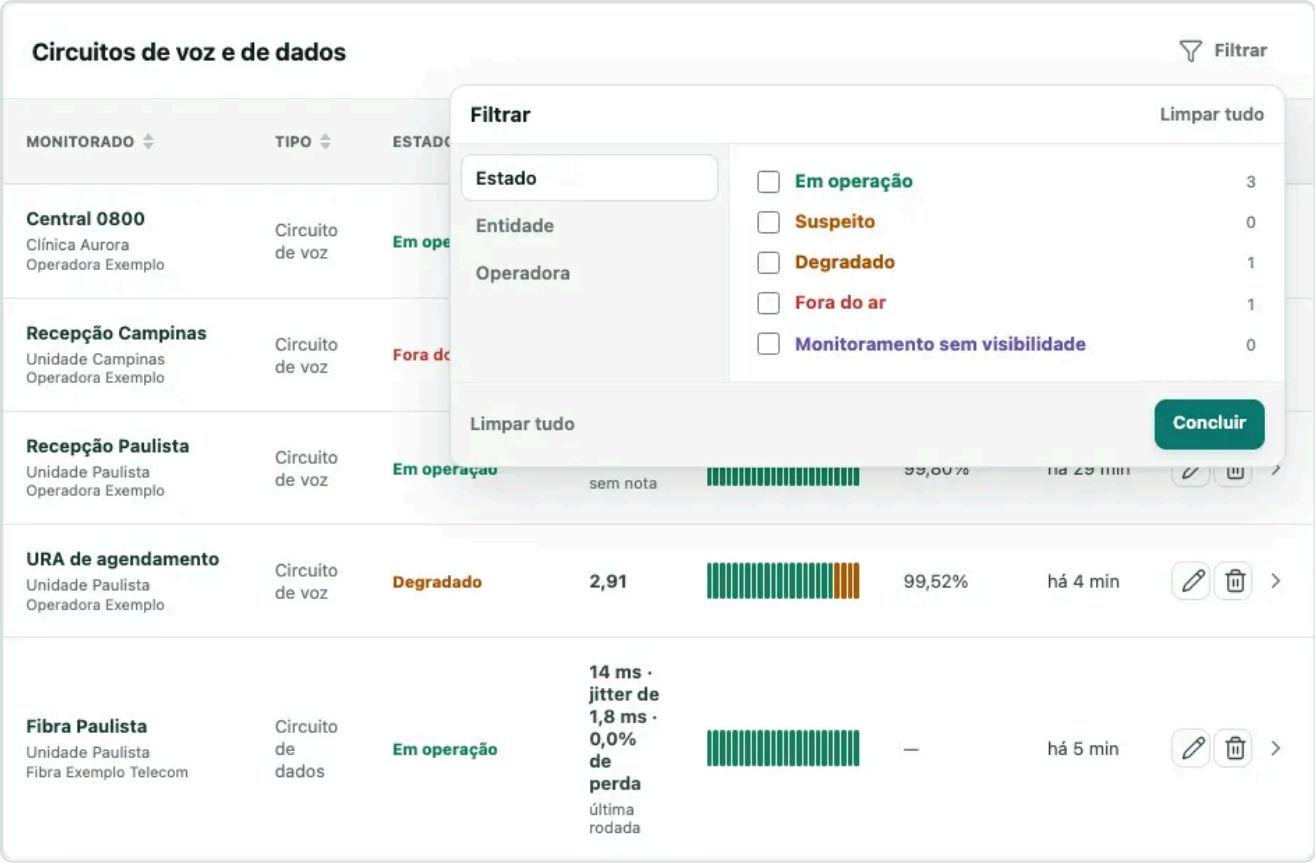
Estado	O que quer dizer
Em operação	O último teste passou.
Suspeito	Um teste falhou e está sendo repetido antes de avisar alguém.
Degradado	O circuito atende, mas a qualidade ficou abaixo do limite em testes seguidos.
Fora do ar	A queda foi confirmada depois de quatro testes com falha seguidos e há um incidente aberto.
Monitoramento sem visibilidade	O Monitor não conseguiu testar; o período não conta como queda.

A coluna **Últimas 24 horas** mostra uma barra por hora. Verde é **Em operação o tempo todo**, laranja é **Degradado**, laranja-avermelhado é **Fora do ar por pouco tempo**, vermelho é **Fora do ar boa parte do tempo**, roxo é **Monitoramento sem visibilidade** e cinza claro é **Não observado**. A coluna **Qualidade** mostra a última nota de MOS-LQO medido dos circuitos que atendem com uma gravação, e **Disponibilidade em 30 dias** mostra a parte do último mês em que o circuito esteve no ar.

Clique no nome de um circuito para abrir a página dele, explicada no capítulo A página de um circuito de voz.

Filtrar e ordenar

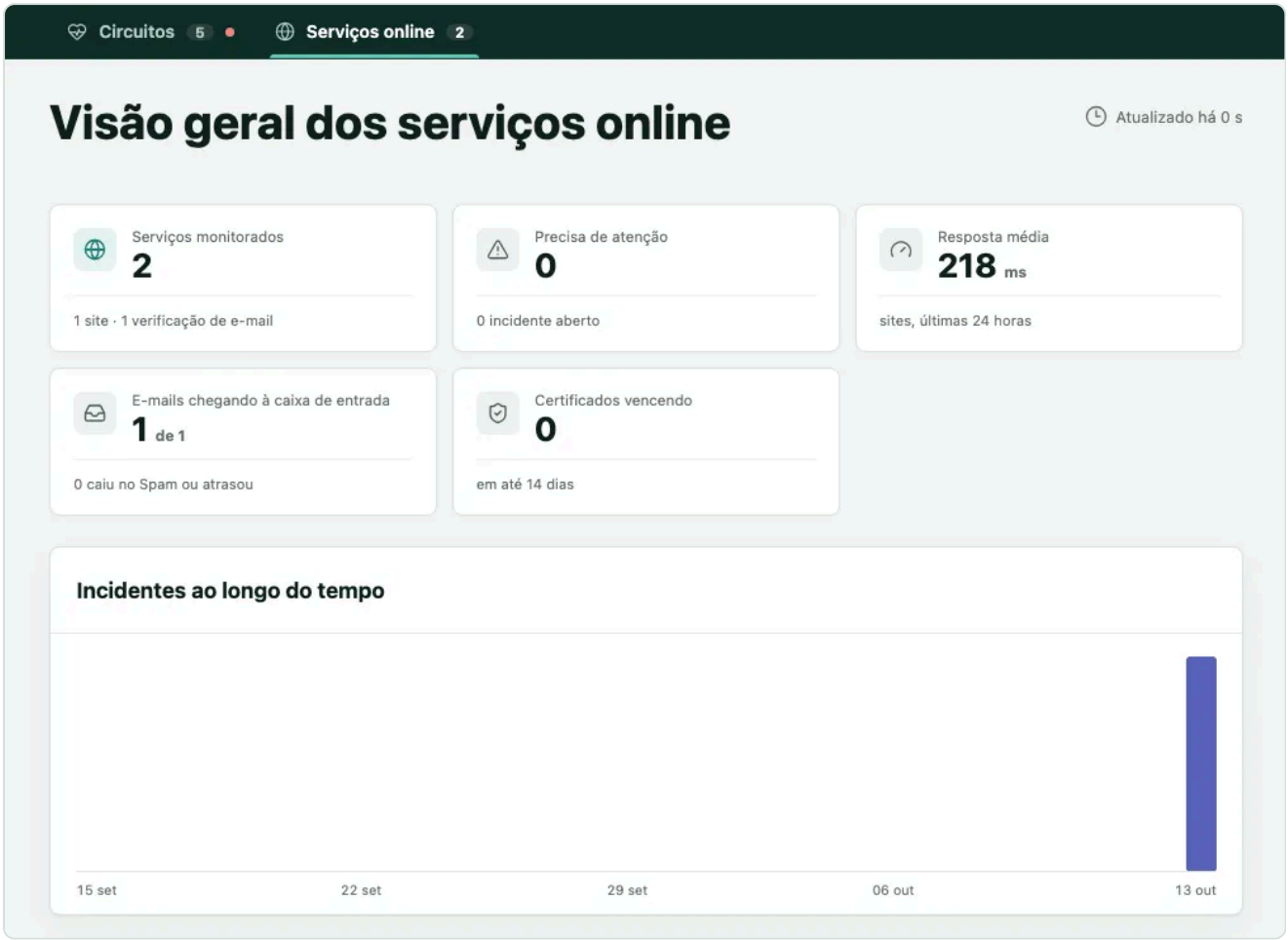
1. Na tabela, clique em **Filtrar**.
2. À esquerda, escolha o que filtrar: **Estado**, **Entidade** ou **Operadora**.
3. À direita, marque as opções. O número ao lado de cada uma diz quantos circuitos ela tem.
4. Clique em **Concluir**. Para voltar a ver tudo, use **Limpar tudo**.



Para ordenar, clique no título de uma coluna que tem o triângulo, como **Monitorado**, **Estado** ou **Último teste**. Um segundo clique inverte a ordem.

A aba Serviços online

A aba **Serviços online** faz o mesmo para os sites e as caixas de e-mail que a 2N5 monitora para você. Os números do topo são **Serviços monitorados**, **Precisa de atenção**, **Resposta média** dos sites nas últimas 24 horas, **E-mails chegando à caixa de entrada** e **Certificados vencendo** nos próximos 14 dias.



Mais abaixo ficam as tabelas **Sites** e **E-mail**, com o mesmo filtro e a mesma ordenação. O capítulo Sites e e-mail explica cada uma.

Perguntas frequentes

Por que um circuito aparece como Suspeito sem que ninguém tenha sido avisado?

Suspeito quer dizer que um teste falhou e o Monitor está repetindo antes de avisar alguém. Uma falha isolada nunca vira alerta. O incidente só abre depois de quatro testes com falha seguidos, o primeiro e três novas tentativas. Se a nova tentativa passar, o circuito volta para Em operação e ninguém recebe mensagem.

O que significa Monitoramento sem visibilidade?

Significa que o próprio Monitor não conseguiu testar o circuito, por exemplo porque a conexão da 2N5 falhou naquele momento. Esse período não é contado como queda do seu circuito e fica fora da disponibilidade dos relatórios. A 2N5 é avisada e cuida do problema; você não precisa fazer nada.

O painel se atualiza sozinho?

Sim. O painel recebe as mudanças ao vivo, sem recarregar a página, e mostra no canto superior direito há quanto tempo foi atualizado. No topo da tela, Monitoramento ativo indica que os testes estão rodando normalmente. Se a conexão cair, o painel avisa e mantém os últimos dados bons visíveis enquanto se reconecta.

GUIA DO USUÁRIO · CAPÍTULO 3

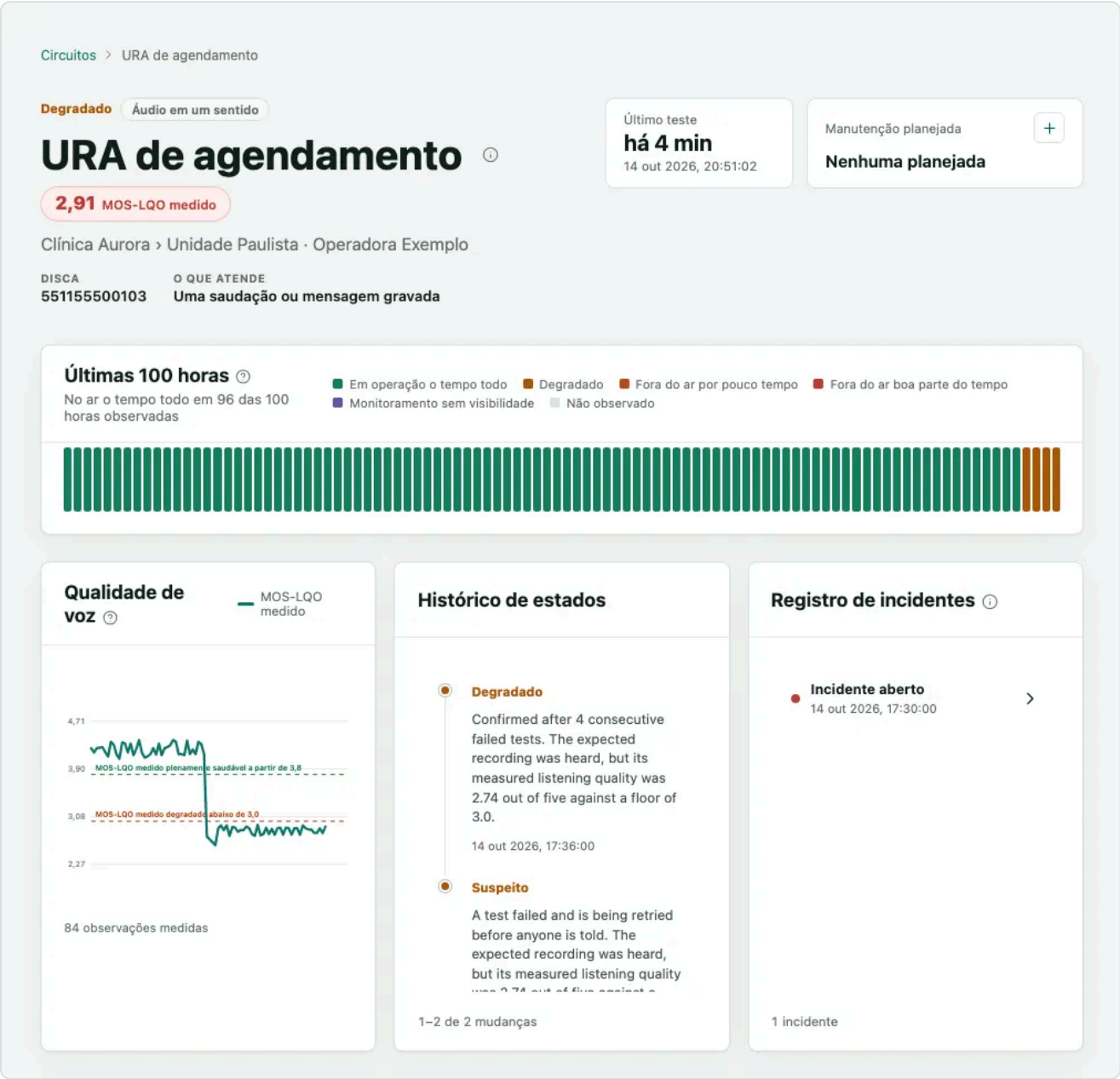
A página de um circuito de voz

Cada circuito de voz tem uma página com tudo o que o Monitor sabe sobre ele: o estado agora, as últimas 100 horas, a qualidade de voz medida, os incidentes e cada chamada de teste. É aqui também que você avisa a 2N5 de uma manutenção planejada.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

Abrir a página do circuito

1. No **Painel**, na tabela **Circuitos de voz e de dados**, clique no nome do circuito.
2. Para voltar, use **Circuitos** no caminho acima do nome.



No topo da página você encontra:

- O **estado** do circuito, como **Degradado**, e o quanto da chamada foi comprovado, como **Áudio em um sentido** ou **Áudio nos dois sentidos**.

- A nota de **MOS-LQO medido** da última chamada com nota, em vermelho quando está abaixo do limite.
- A organização, a entidade e a operadora do circuito, o número que o Monitor **Disca** e **O que atende**: **Uma saudação ou mensagem gravada**, **Um tom de teste ou serviço de eco** ou **Outro: pode tocar ou ser atendido**.
- **Último teste**: quando foi a última chamada de teste.
- **Manutenção planejada**: a próxima janela cadastrada, se houver.

As últimas 100 horas

O quadro **Últimas 100 horas** tem uma barra por hora e mostra o que a sequência de testes concluiu em cada hora, com as mesmas cores do painel. Passe o mouse sobre uma barra para ver a hora e o que aconteceu; uma barra com incidente leva até ele.

Qualidade de voz: MOS e MOS-LQO

MOS (Mean Opinion Score) é a escala de 1 a 5 usada em telefonia para dizer como uma chamada soa a quem escuta: perto de 4,5 é excelente, abaixo de 3 a conversa fica difícil. MOS-LQO é a mesma escala calculada a partir do áudio, sem ouvintes: o Monitor compara o áudio que cada chamada de teste recebeu com a gravação esperada, usando um modelo perceptual de qualidade de escuta com referência que devolve MOS-LQO (ITU-T P.800.1).

O gráfico **Qualidade de voz** mostra a nota de cada chamada atendida nas últimas horas e duas linhas:

- **degradado abaixo de 3,0**: chamadas abaixo desta linha contam como degradadas. Se isso se repetir em testes seguidos, o circuito fica **Degradado** e abre um incidente.
- **plenamente saudável a partir de 3,8**: acima desta linha a chamada é considerada plenamente saudável.

Esses limites são da sua organização e ficam em **Configurações**, na aba **Limites de qualidade**. Circuitos que não atendem com uma gravação aparecem como **sem nota**. O glossário explica MOS e MOS-LQO em mais detalhe.

Histórico de estados e incidentes

- **Histórico de estados** lista cada mudança de estado, da mais recente para a mais antiga, com o motivo e a hora. Uma queda aparece primeiro como **Suspeito**, quando o primeiro teste falha, e depois como **Fora do ar** ou **Degradado**, quando é confirmada depois de quatro testes com falha seguidos.
- **Registro de incidentes** mostra só as falhas confirmadas. Clique em um incidente para abrir a página dele, explicada em Incidentes e alertas.

Registro de observações: cada chamada de teste

Mais abaixo, o **Registro de observações** guarda cada chamada de teste, da mais recente para a mais antiga:

- **Testado**: quando a chamada foi feita, e quando estava prevista.
- **Veredito**: o que a chamada concluiu.
- **SIP**: o código de resposta da operadora, como 200 para atendida.

- **Atendimento**: quanto tempo a chamada levou para ser atendida.
- **RTP enviado / recebido**: os pacotes de áudio enviados e recebidos.
- **MOS-LQO** e **Ouvido**: a nota da chamada e se a gravação esperada foi ouvida.

Registro de observações Filtrar Baixar CSV

TESTADO	VEREDITO	SIP	ATENDIMENTO	RTP ENVIADO / RECEBIDO	MOS-LQO	OUVIDO	TONS EN
14 out 2026, 20:30:06 previsto 14 out 2026, 20:30:00	Em operação pela 2N5	200	1405 ms	493 / 493	4,13	Gravação esperada ouvida	—
14 out 2026, 20:00:04 previsto 14 out 2026, 20:00:00	Em operação pela 2N5	200	3238 ms	485 / 479	4,18	Gravação esperada ouvida	—
14 out 2026, 19:30:06 previsto 14 out 2026, 19:30:00	Em operação pela 2N5	200	1972 ms	508 / 504	4,37	Gravação esperada ouvida	—
14 out 2026, 19:00:08 previsto 14 out 2026, 19:00:00	Em operação pela 2N5	200	1405 ms	513 / 508	4,10	Gravação esperada ouvida	—

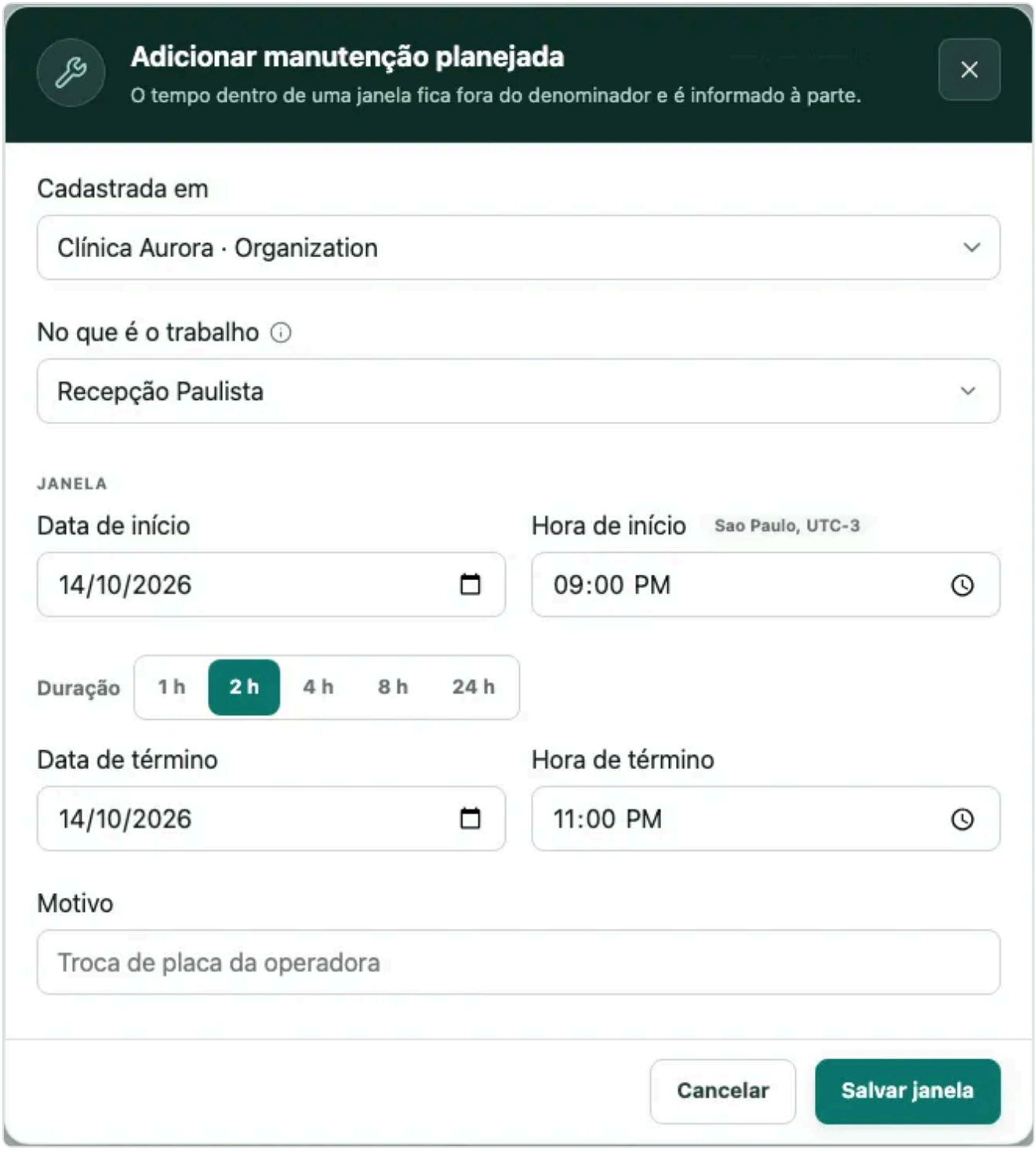
1–20 de 2106 observações 1 de 106

Use **Filtrar** para ver só um tipo de resultado e **Baixar CSV** para levar o registro para uma planilha. As setas no rodapé passam as páginas.

Cadastrar uma manutenção planejada

Se a sua operadora ou a sua equipe vai mexer no circuito, cadastre uma janela de manutenção. Falhas dentro da janela não abrem incidente e o tempo fica fora da disponibilidade.

1. Na página do circuito, no quadro **Manutenção planejada**, clique em **+** (**Adicionar janela**).
2. Em **No que é o trabalho**, confira o circuito. Você pode escolher outros circuitos da mesma entidade.
3. Em **Data de início** e **Hora de início**, informe quando o trabalho começa. O horário é o do fuso da sua organização, mostrado ao lado.
4. Escolha a **Duração** (1 h, 2 h, 4 h, 8 h ou 24 h) ou preencha **Data de término** e **Hora de término**.
5. Escreva o **Motivo**, por exemplo a troca de um equipamento.
6. Clique em **Salvar janela**.



A janela aparece no quadro **Manutenção planejada** e pode ser excluída ali mesmo, enquanto não tiver acontecido.

Perguntas frequentes

Por que o meu circuito mostra sem nota na qualidade?

A nota MOS-LQO só é medida quando o circuito atende com uma saudação ou mensagem gravada, porque ela compara o áudio que a chamada recebeu com a gravação esperada. Um circuito que toca ou é atendido por uma pessoa é testado pela chamada em si, sem nota. Se quiser a nota, peça à 2N5 para configurar a gravação de referência do circuito.

Uma falha durante a manutenção planejada conta contra a disponibilidade?

Não. O tempo dentro de uma janela de manutenção fica fora do cálculo da disponibilidade e aparece à parte nos relatórios, e uma falha nesse período não abre incidente nem avisa ninguém. Cadastre a janela antes do trabalho começar: uma janela não muda o que já foi registrado antes de ela existir.

Posso mudar com que frequência o circuito é testado?

Cada circuito guarda os valores com que foi adicionado: o intervalo entre testes, o intervalo das novas tentativas e quantas tentativas fazer antes de confirmar a queda. Para mudar os de um circuito existente, peça à 2N5. Os valores da tela Configurações valem para os circuitos adicionados depois.

GUIA DO USUÁRIO · CAPÍTULO 4

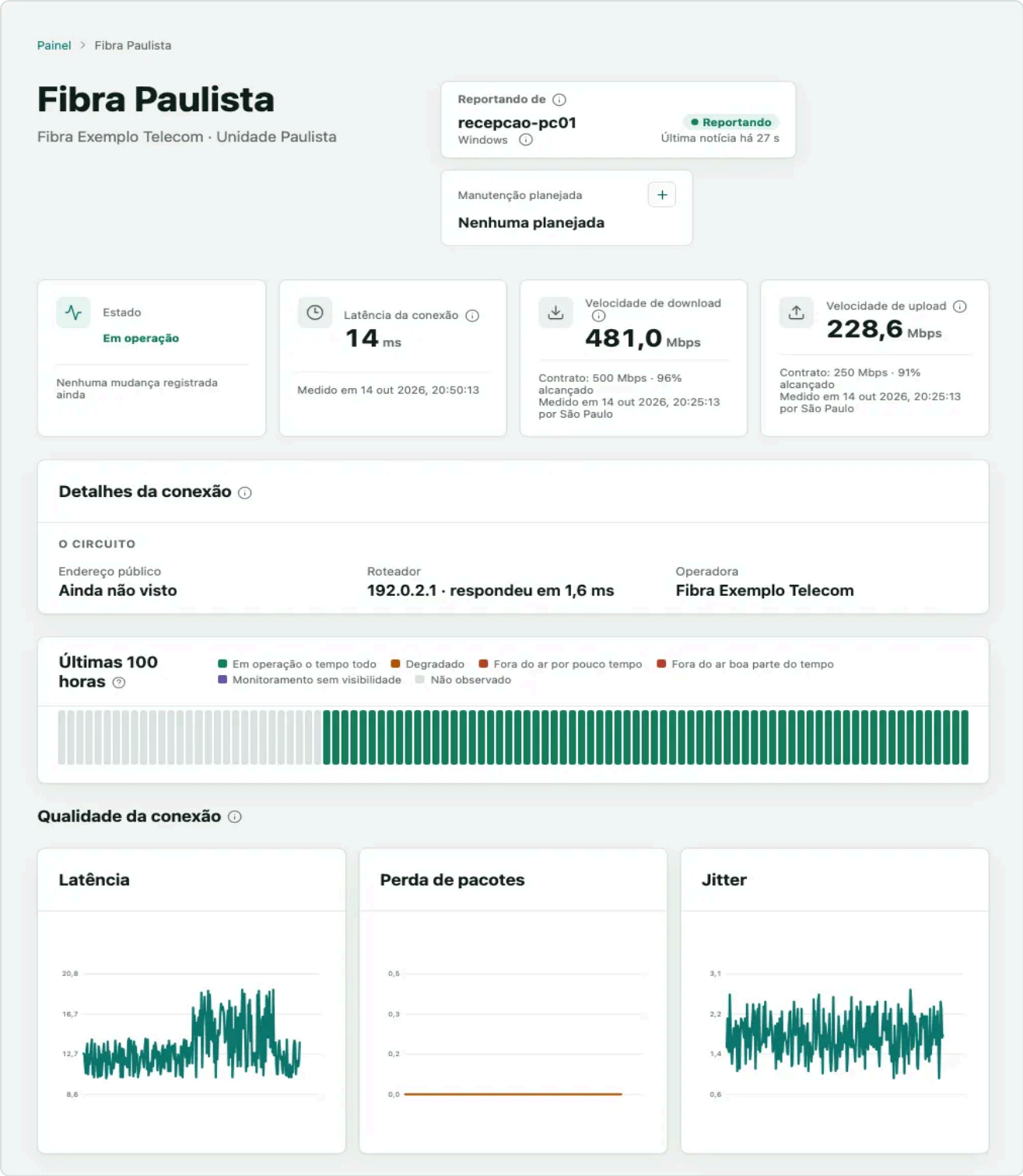
Circuitos de dados e o agente

Um circuito de dados é o link de internet de um local, medido por um agente: um pequeno serviço que roda em segundo plano em um computador do próprio local. A página do circuito mostra se o link está no ar, a qualidade da conexão e a velocidade contratada que de fato chega.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

O que você vê de um circuito de dados

1. No **Painel**, aba **Circuitos**, os circuitos de dados aparecem na mesma tabela dos circuitos de voz, com o **Tipo Circuito de dados**. A coluna **Qualidade** mostra a latência, o jitter e a perda da última rodada.
2. Clique no nome do circuito para abrir a página dele.



Na página do circuito:

- **Reportando de** mostra o computador onde o agente roda, o sistema dele e quando chegou a última notícia. **Reportando** em verde quer dizer que as leituras estão chegando.
- **Estado** é **Em operação**, **Degradado** ou **Fora do ar**. Uma queda do link é confirmada depois de novas medições, como nos circuitos de voz, e só então abre incidente e avisa a escada de escalonamento.
- **Latência da conexão** é o tempo de ida e volta até a internet, em milissegundos.

- **Velocidade de download** e **Velocidade de upload** mostram o último teste de velocidade e quanto do **Contrato** ele alcançou.
- **Detalhes da conexão** mostra o endereço público, o roteador do local (e se ele respondeu) e a operadora.
- **Últimas 100 horas** tem uma barra por hora, com as cores do painel.
- **Qualidade da conexão** traz os gráficos de **Latência**, **Perda de pacotes** e **Jitter**, e **Velocidade da conexão** traz os testes de **Download** e **Upload**.
- **Registro de observações**, no fim da página, guarda cada rodada de medição, com **Filtrar** e **Baixar CSV**.

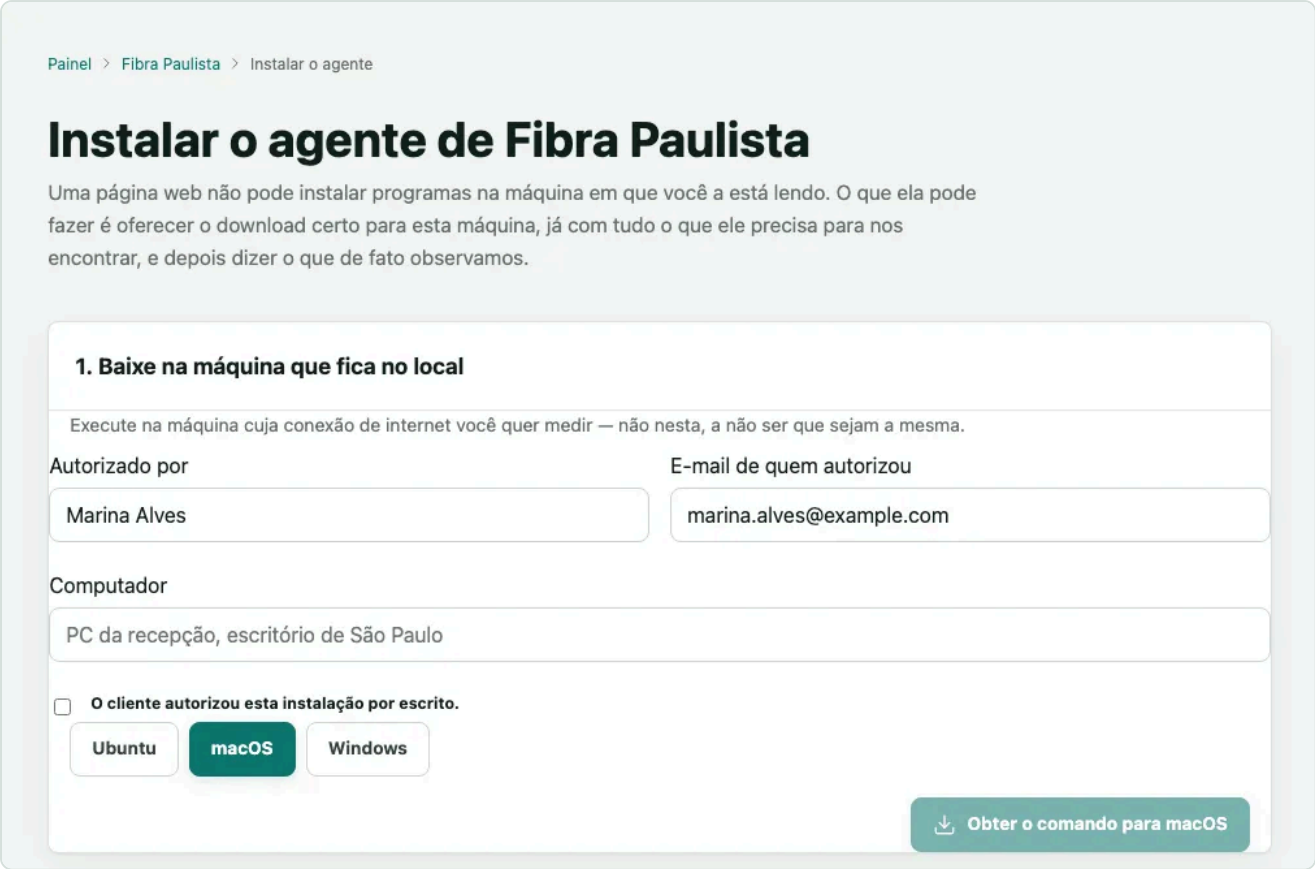
Como o agente também mede o roteador do local, o Monitor consegue separar uma falha do roteador de uma falha da operadora.

Instalar o agente com a ajuda da 2N5

Normalmente a 2N5 instala o agente com você: ela combina o horário, confirma qual computador vai rodar o agente e registra a sua autorização por escrito. Escolha um computador do local que fique sempre ligado e que use o link a ser medido.

Enquanto nenhum agente reportar, a página do circuito mostra **Aguardando seu agente**, com duas opções: **Instalar em outro computador** e **Configurar este computador**. Se for instalar junto com a 2N5:

1. Abra a página do circuito no computador do local e clique em **Configurar este computador**. A página **Instalar o agente de** mostra o nome do circuito.
2. Confira **Autorizado por** e **E-mail de quem autorizou**, que vêm com o seu nome, e escreva em **Computador** qual é a máquina, por exemplo o PC da recepção.
3. Marque **O cliente autorizou esta instalação por escrito.**
4. Escolha o sistema do computador e clique em **Obter o comando para**. Execute o comando nesse computador, como a 2N5 orientar.
5. Acompanhe **2. O que observamos**: os passos avançam sozinhos à medida que o Monitor vê o agente se registrar e enviar as primeiras leituras.



Quando o agente começa a reportar, a página do circuito passa a mostrar as medições. As primeiras horas do quadro **Últimas 100 horas** ficam em cinza, como **Não observado**, porque são anteriores à instalação.

O que só a 2N5 muda

A frequência das medições e dos testes de velocidade, os limites que fazem um link contar como degradado ou fora do ar, o tempo de silêncio que conta como agente parado e a verificação externa são definidos pela 2N5, porque é ela que atende os alertas do link. Para mudar qualquer um deles, peça à 2N5.

Perguntas frequentes

O agente deixa alguma porta aberta no computador?

Não. O agente só faz conexões de saída: ele mede o link do local e envia as leituras para a 2N5, sem abrir nenhuma porta de entrada no computador nem na rede. Ele envia só medições do link, de uma lista fixa. Se a sua equipe de segurança quiser os detalhes, peça à 2N5 a lista do que o agente mede.

O que acontece se o computador do agente for desligado?

As leituras param de chegar e o agente aparece como parado de reportar. Isso, sozinho, não quer dizer que o link caiu, porque um agente em silêncio pode ser só um computador desligado. A 2N5 é avisada quando um agente fica em silêncio e combina com você o que fazer. Por isso o agente deve ficar em um computador que permaneça ligado.

E se o local não tiver um computador para o agente?

Peça à 2N5 a verificação externa. Nesse caso a 2N5 testa de fora se o link responde, no ar ou fora do ar, sem medir velocidade, latência, perda ou DNS. Ela precisa de um endereço público fixo; um link atrás de endereçamento compartilhado (CGNAT) não pode ser verificado assim.

GUIA DO USUÁRIO · CAPÍTULO 5

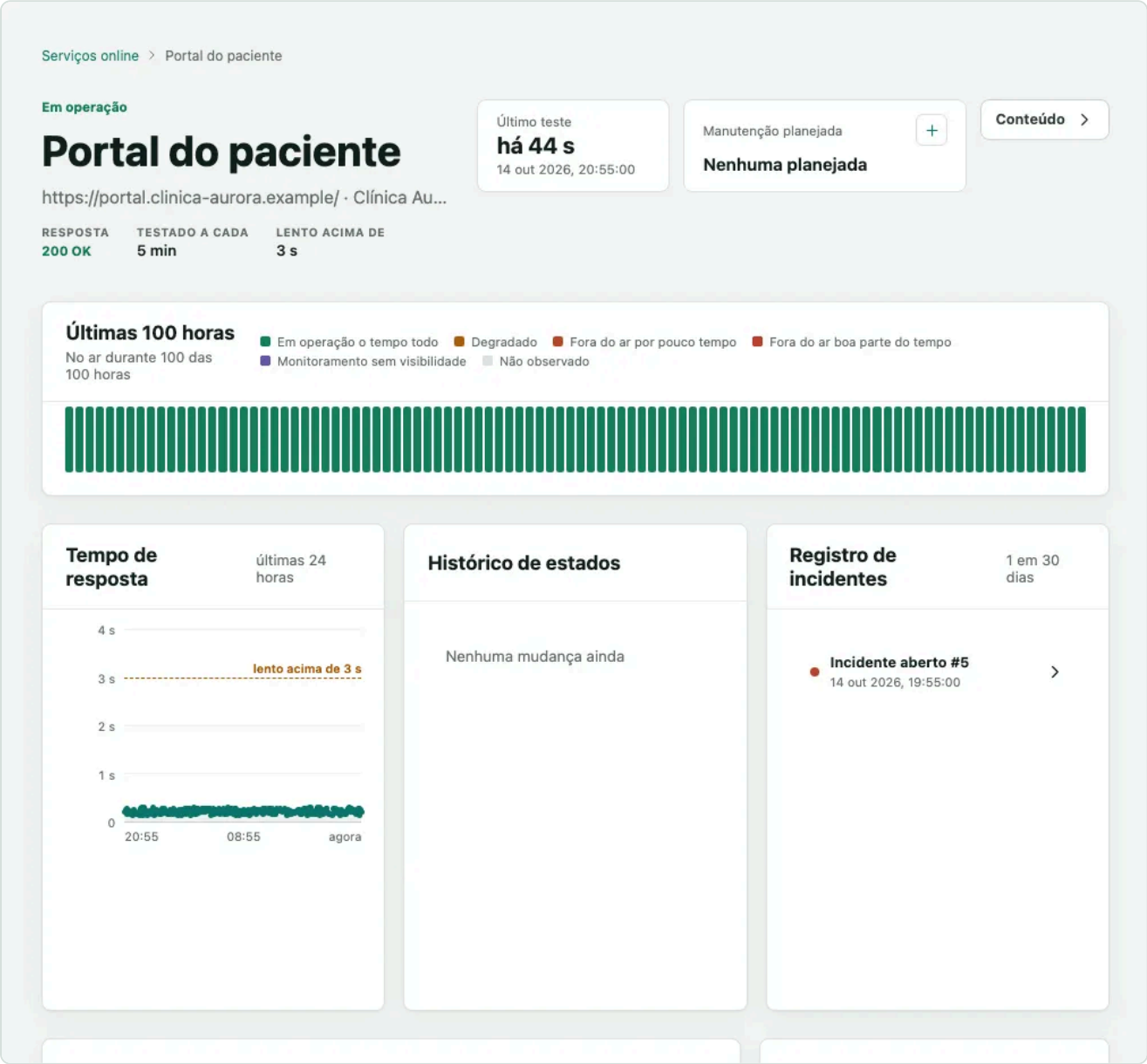
Sites e e-mail

Além dos circuitos, a 2N5 pode monitorar os seus sites e as suas caixas de e-mail. Para um site, o Monitor confere se ele responde, se está rápido, se o certificado está em dia e se o conteúdo mudou; para uma caixa de e-mail, se uma mensagem de teste chega à caixa de entrada a tempo.

Por Equipe 2N5 Atualizado em 21 de outubro de 2026

A página de um site

1. No **Painel**, abra a aba **Serviços online**.
2. Na tabela **Sites**, clique no nome do site.



No topo, o estado do site, o endereço e três números: **Resposta** (o código que o servidor devolveu, como **200 OK**), **Testado a cada** e **Lento acima de**. O site fica:

- **Em operação** quando responde normalmente.

- **Degradado** quando responde, mas mais devagar que o limite de lento, ou quando o certificado de segurança vence em até 14 dias.
- **Fora do ar** quando não responde, responde com erro ou o certificado venceu ou não é confiável. A queda é confirmada depois de novas tentativas, e só então abre incidente.

Abaixo vêm **Últimas 100 horas**, **Tempo de resposta** nas últimas 24 horas, **Histórico de estados** e **Registro de incidentes**. Mais abaixo, **Respostas** resume os códigos dos últimos 30 dias, **Certificado** mostra **Válido até**, **Dias restantes** e **Emitido por**, e o **Registro de observações** guarda cada teste.

Mudanças de conteúdo

Se a chave **Verificar também o conteúdo deste site** estiver ligada, o Monitor compara a página com uma referência: o texto e a estrutura que a página tinha quando a chave foi ligada. Não há nenhuma configuração de conteúdo: a verificação usa limites fixos e o ritmo de teste do próprio site. Uma página montada inteira por JavaScript não pode ser verificada e aparece como ilegível. Assim ele percebe, por exemplo, um menu que sumiu, uma página trocada ou um texto que alguém mudou sem avisar.

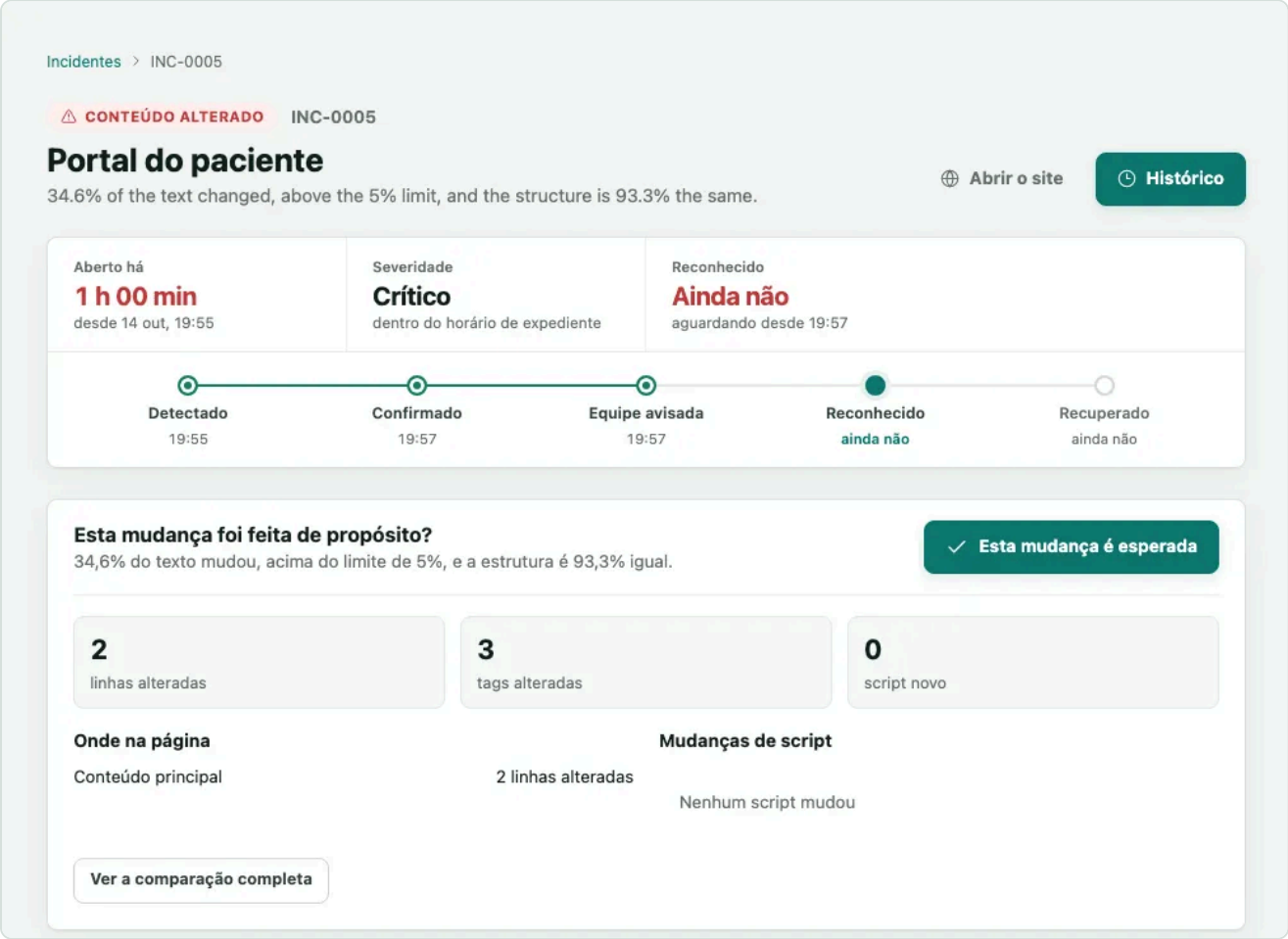
1. Na tabela **Sites**, o site com a página alterada aparece como **Conteúdo alterado**, um estado pior que **Em operação** e melhor que **Fora do ar**. Clique no nome dele.
2. Na página do site, abaixo de **Respostas** e **Certificado**, duas seções mostram o conteúdo: o estado e o que mudou, com o botão **Esta mudança é esperada** e a comparação completa, e as verificações de conteúdo, uma por rodada.

Quando a página muda mais do que o permitido, o Monitor repete a verificação antes de concluir. Se a mudança continua, abre um incidente de **Conteúdo alterado** e avisa a escada de escalonamento. Se o site estiver fora do ar ao mesmo tempo, o incidente é um só, o da queda, e a mudança de conteúdo continua como uma linha do registro de observações. Um site lento e uma mudança de conteúdo são dois incidentes.

Esta mudança é esperada

Se a mudança foi feita de propósito, por exemplo um aviso de horário de feriado, encerre o incidente assim:

1. Abra o incidente pelo **Registro de incidentes** da página do site, ou em **Incidentes** no menu lateral.
2. Leia **Esta mudança foi feita de propósito?**: quantas linhas e tags mudaram, se apareceu script novo e **Onde na página** a mudança está.
3. Para ver exatamente o que mudou, clique em **Ver a comparação completa**. O texto **Removido** e o **Adicionado** aparecem lado a lado.
4. Se a mudança é esperada, clique em **Esta mudança é esperada**. A página de hoje vira a nova referência, o incidente é encerrado e o seu nome fica registrado.



Se ninguém fez a mudança, não clique: trate como um problema no site e fale com quem cuida dele. O que a página deve mostrar e as partes que mudam sozinhas, como um relógio ou uma notícia do dia, são combinados com a 2N5.

A página de uma caixa de e-mail

A verificação de e-mail envia uma mensagem de teste para o endereço da sua caixa, em horários definidos, e confere se ela chegou, onde caiu e em quanto tempo.

1. No **Painel**, aba **Serviços online**, na tabela **E-mail**, clique no nome da verificação.
2. No topo estão **Testado a cada** e **Aguarda até**, o tempo máximo para a mensagem chegar sem contar como atrasada.

A verificação fica **Em operação** quando a mensagem chega à caixa de entrada a tempo, **Degradado** quando cai no Spam ou chega atrasada, e **Fora do ar** quando não chega. O gráfico **Tempo de entrega** mostra os últimos testes. O registro mostra para cada teste quando foi enviado, em quanto tempo chegou, onde caiu, se foi apagado e as verificações do remetente (SPF, DKIM e DMARC). Na tabela **E-mail** do painel, a barra **Caixa** mostra quanto da caixa está ocupado.

Para que a caixa possa ser verificada, a 2N5 envia um link para você conectá-la. Se o link vencer antes de você usá-lo, peça um novo à 2N5.

Perguntas frequentes

Uma mudança de conteúdo derruba a disponibilidade do site?

Não. A mudança de conteúdo mostra o site como Conteúdo alterado e abre um incidente próprio, e nunca conta como tempo fora do ar. Se o site cair ao mesmo tempo, há um só incidente, o da queda. Os relatórios mostram a disponibilidade e as mudanças de conteúdo em separado.

Quem pode clicar em Esta mudança é esperada?

Um gestor da organização ou da entidade onde o site está. Ao clicar, a página de hoje vira a nova referência, o incidente é encerrado e o seu nome fica registrado. Se a mudança não foi feita de propósito, não clique: trate o site como um incidente e fale com quem cuida dele.

A mensagem de teste fica na minha caixa de e-mail?

Normalmente não. Depois de conferir onde a mensagem caiu, o Monitor a apaga, e o registro mostra Apagado para cada teste. Se a conexão da caixa só permite ler, a mensagem fica e o registro diz isso. Para a caixa ser verificada, a 2N5 envia um link para você conectá-la.

GUIA DO USUÁRIO · CAPÍTULO 6

Incidentes e alertas

Um incidente é uma falha confirmada: ele só abre depois de quatro testes com falha seguidos, o primeiro e três novas tentativas. Então o Monitor avisa as pessoas da sua escada de escalonamento, nível por nível, até alguém reconhecer o incidente pelo link da mensagem.

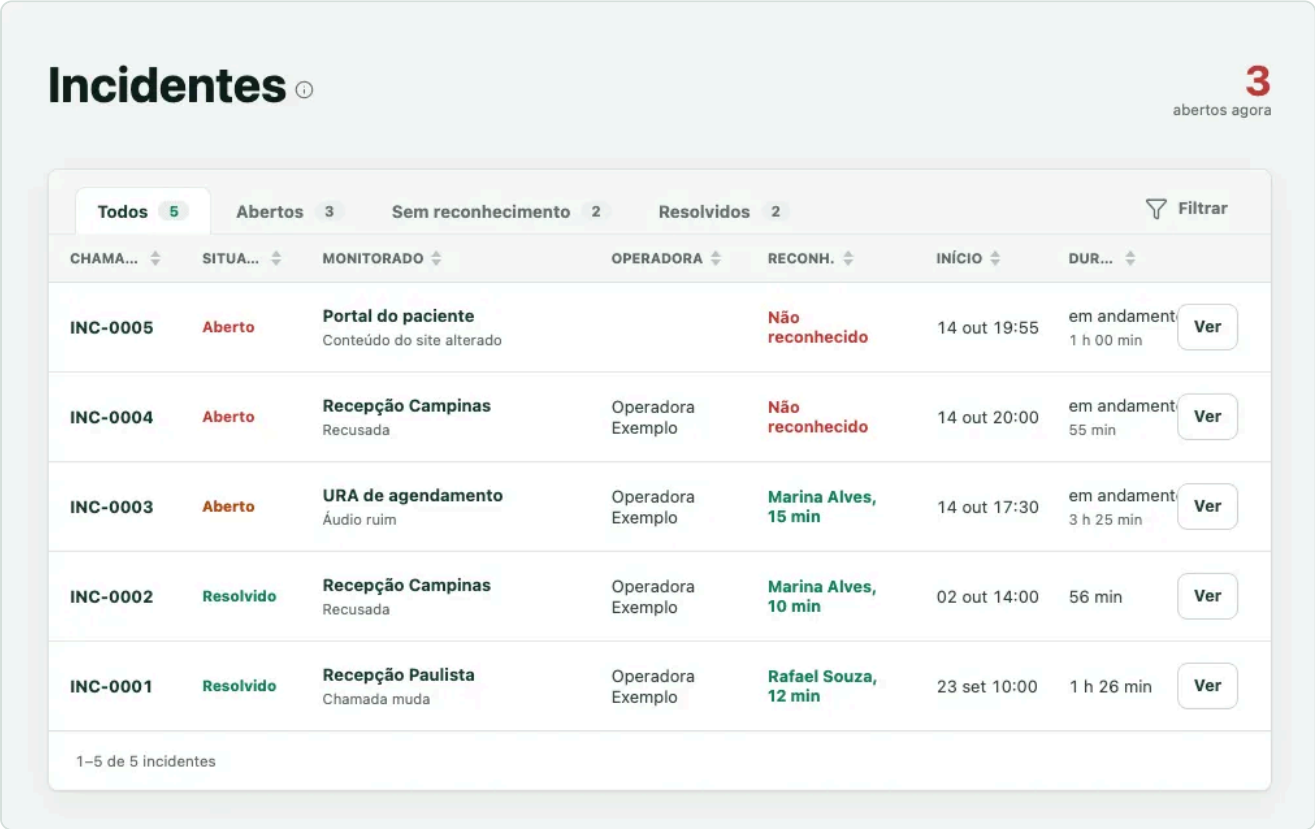
Por Equipe 2N5 Atualizado em 14 de outubro de 2026

Como uma falha vira um incidente

1. Uma chamada de teste falha. O circuito fica **Suspeito** e ninguém é avisado ainda.
2. O Monitor repete o teste, normalmente a cada 2 minutos.
3. Se o primeiro teste e as três novas tentativas falham, ou seja, quatro testes com falha seguidos, a falha é confirmada: o circuito fica **Fora do ar** ou **Degradado** e um incidente abre.
4. O primeiro nível da escada de escalonamento é avisado.
5. Quando o circuito passa em dois testes limpos seguidos, o incidente é encerrado como recuperado e quem foi avisado recebe a mensagem de que ele voltou.

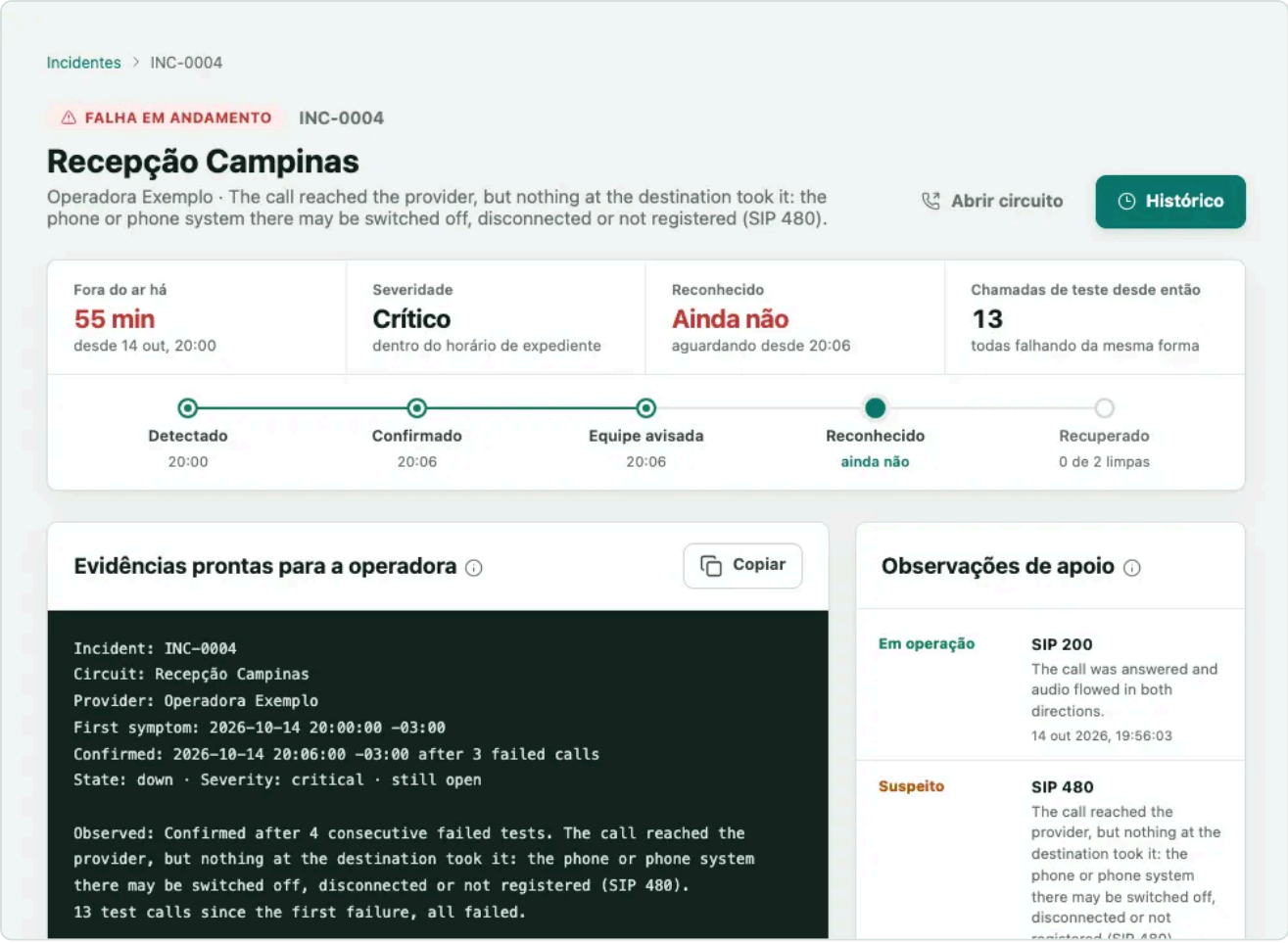
A lista de incidentes

1. No menu lateral, clique em **Incidentes**.
2. Use as abas **Todos**, **Abertos**, **Sem reconhecimento** e **Resolvidos**, ou **Filtrar**.
3. Clique em **Ver** para abrir um incidente.



Cada incidente tem um número, como **INC-0004**. A coluna de reconhecimento mostra quem reconheceu e em quanto tempo, ou **Não reconhecido**.

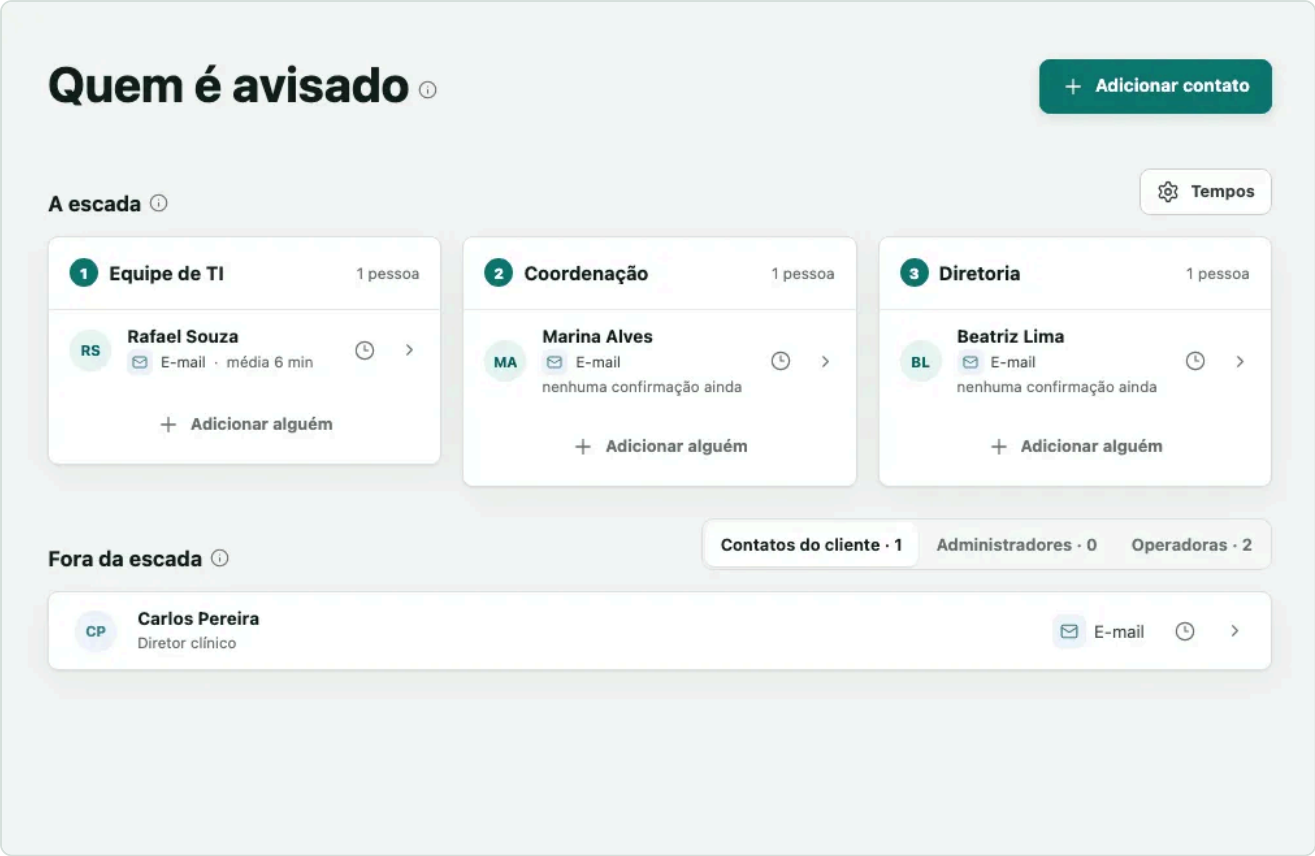
A página de um incidente



- No topo, o circuito, a operadora e o sintoma, com **Abrir circuito** e **Histórico**, que mostra cada mensagem enviada sobre o incidente e para quem.
- **Fora do ar há**, **Severidade**, **Reconhecido** e **Chamadas de teste desde então**. A severidade é **Crítico** quando o incidente abriu dentro do horário de expediente da organização e **Menor** quando abriu fora dele.
- **Onde está** mostra a linha do tempo: **Detectado**, **Confirmado**, **Equipe avisada**, **Reconhecido** e **Recuperado**.
- **Evidências prontas para a operadora** é um bloco de texto com o circuito, a operadora, o primeiro sintoma, a confirmação e as chamadas de teste. Clique em **Copiar** e cole no chamado da operadora, sem reescrever.
- **Observações de apoio** lista as chamadas de teste do período do incidente.

A escada de escalonamento: quem é avisado

1. No menu lateral, clique em **Escalonamento**. A página **Quem é avisado** mostra **A escada**.
2. Cada nível tem um nome e as pessoas dele. A falha confirmada vai primeiro para o nível 1. Se ninguém reconhecer, o aviso é repetido e depois sobe para o nível seguinte.
3. Para ver ou mudar quanto cada nível espera e quantas vezes repete o aviso antes de subir, clique em **Tempos**.
4. Para incluir alguém, use **Adicionar alguém** no nível, ou **Adicionar contato** no topo, e informe o nome, a função, o idioma e os endereços: e-mail e celular.



Em **Fora da escada** ficam os **Contatos do cliente**: pessoas que recebem o aviso de que um circuito caiu e está sendo tratado, e o aviso de que voltou, sem precisar reconhecer nada. Se nenhum nível reconhecer um incidente, a 2N5 é avisada para agir.

Reconhecer pelo link do e-mail

Cada alerta da escada traz um link para reconhecer o incidente. Reconhecer quer dizer: eu assumi, podem parar de avisar.

1. Toque no link da mensagem. A página abre no celular ou no computador, sem precisar entrar no Monitor.
2. Toque em **Reconhecer incidente**.
3. A página confirma: o incidente foi reconhecido e nenhum outro alerta será enviado sobre ele.

Se outra pessoa já tiver reconhecido, a página diz quem foi e que nada mais é necessário. Se o circuito já tiver voltado, a página avisa e registra a sua resposta.

O que cada mensagem quer dizer

Os avisos chegam por e-mail. Os exemplos abaixo usam os circuitos da clínica fictícia deste guia.

A queda foi confirmada

> Alerta para Clínica Aurora: circuito Recepção Campinas FORA DO AR desde 14/10 19:36. Confirme em .../a/... para parar os avisos.

Vai para o primeiro nível da escada. Toque no link e reconheça; depois verifique o circuito ou abra chamado na operadora.

Ninguém reconheceu ainda

> Alerta para Clínica Aurora: Recepção Campinas segue FORA DO AR desde 14/10 19:36, sem

resposta. Confirme em .../a/... para parar.

Vai para o nível seguinte, quando ninguém reconheceu a tempo. Reconheça pelo link, se for assumir.

Aviso ao cliente

Aviso para Clínica Aurora: Recepção Campinas fora do ar desde 14/10 19:36. Estamos cuidando disso e avisaremos quando voltar.

Vai para os contatos do cliente. Não há nada a fazer; é só um aviso.

O circuito voltou

Aviso para Clínica Aurora: Recepção Campinas voltou a funcionar em 14/10 20:42 depois de 1 h 6 min fora do ar. Nada a fazer.

Vai para quem foi avisado da queda. O incidente foi encerrado.

Os e-mails

Por e-mail, o assunto já diz do que se trata numa frase simples, a mesma com que o e-mail começa: *Linha principal está fora do ar* para uma queda, *Linha principal está com qualidade de chamada ruim* quando as chamadas completam mas soam mal, e *Linha principal voltou a funcionar normalmente* quando volta. Cada e-mail termina dizendo por que você o recebe e a quem pedir para não receber mais. O e-mail traz o problema em palavras simples, quando começou, quando foi confirmado e, para quem está na escada, o link **Reconhecer**. Circuitos de dados, sites e caixas de e-mail seguem a mesma lógica, com o nome do circuito ou do serviço no aviso.

Perguntas frequentes

Por que recebi um alerta se o circuito já voltou?

O alerta sai no momento em que a falha é confirmada. Se o circuito volta logo depois, você recebe também o aviso de que ele voltou a funcionar. Abrir o link de um alerta já resolvido mostra que o circuito tinha se recuperado e registra a sua resposta; nenhum alerta novo é enviado sobre aquele incidente.

Preciso reconhecer o incidente se outra pessoa já reconheceu?

Não. Basta uma pessoa reconhecer para os alertas pararem para todos. Se você abrir o link depois, a página mostra quem reconheceu primeiro e diz que nada mais é necessário da sua parte. O nome de quem reconheceu e o tempo até o reconhecimento ficam no incidente e entram nos relatórios.

Por quais canais recebo alertas?

O Monitor avisa por e-mail. Cada contato pode ter mais de um endereço, e a ordem em que eles são usados é definida no cadastro do contato.

GUIA DO USUÁRIO · CAPÍTULO 7

Relatórios

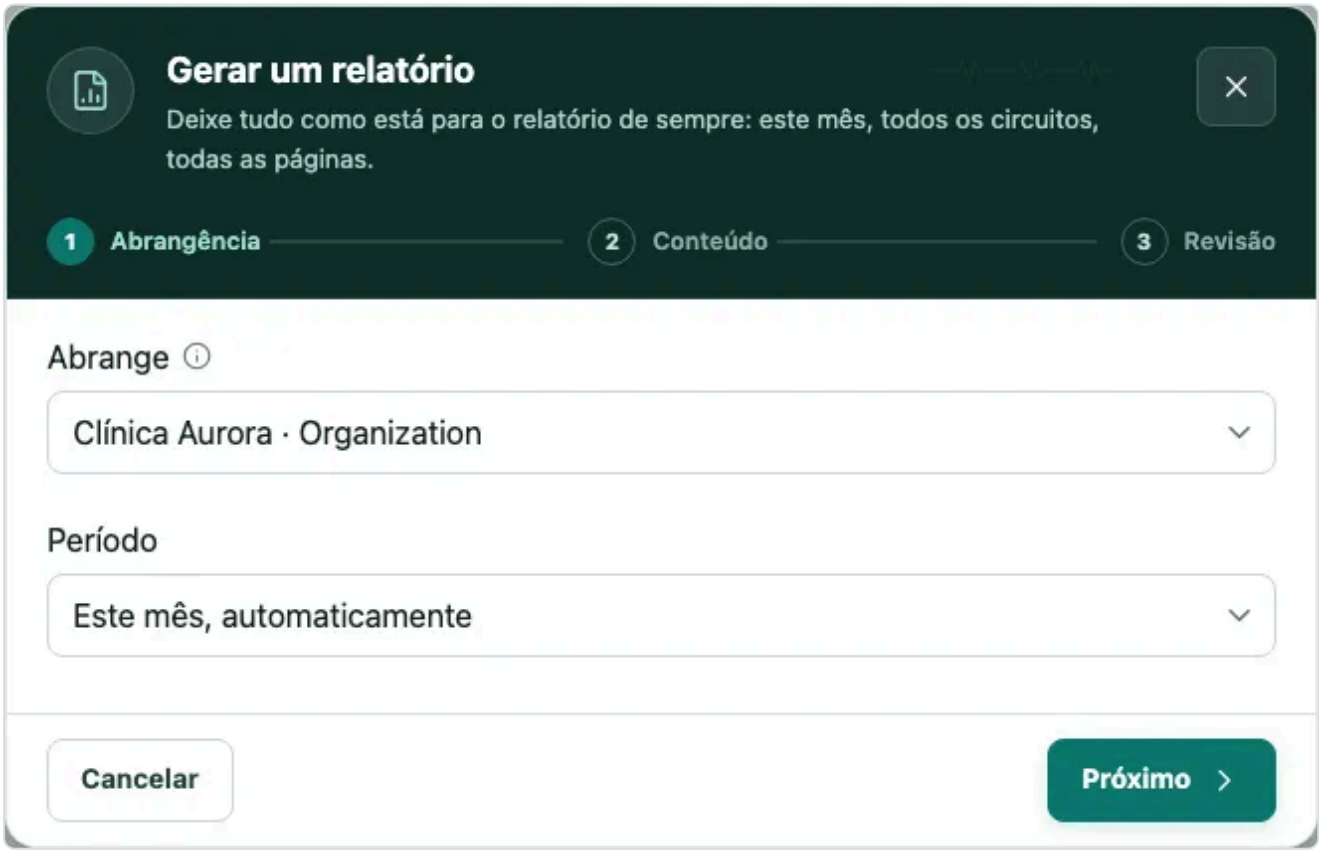
O relatório de serviço é a prova de como os seus circuitos se comportaram em um período: disponibilidade em relação à meta, cada incidente e quanto tempo levou para ser atendido. Você gera quantos quiser, envia por e-mail em PDF e pode programar o envio mensal automático.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

Os relatórios e o SLA são para clientes Enterprise.

Gerar um relatório

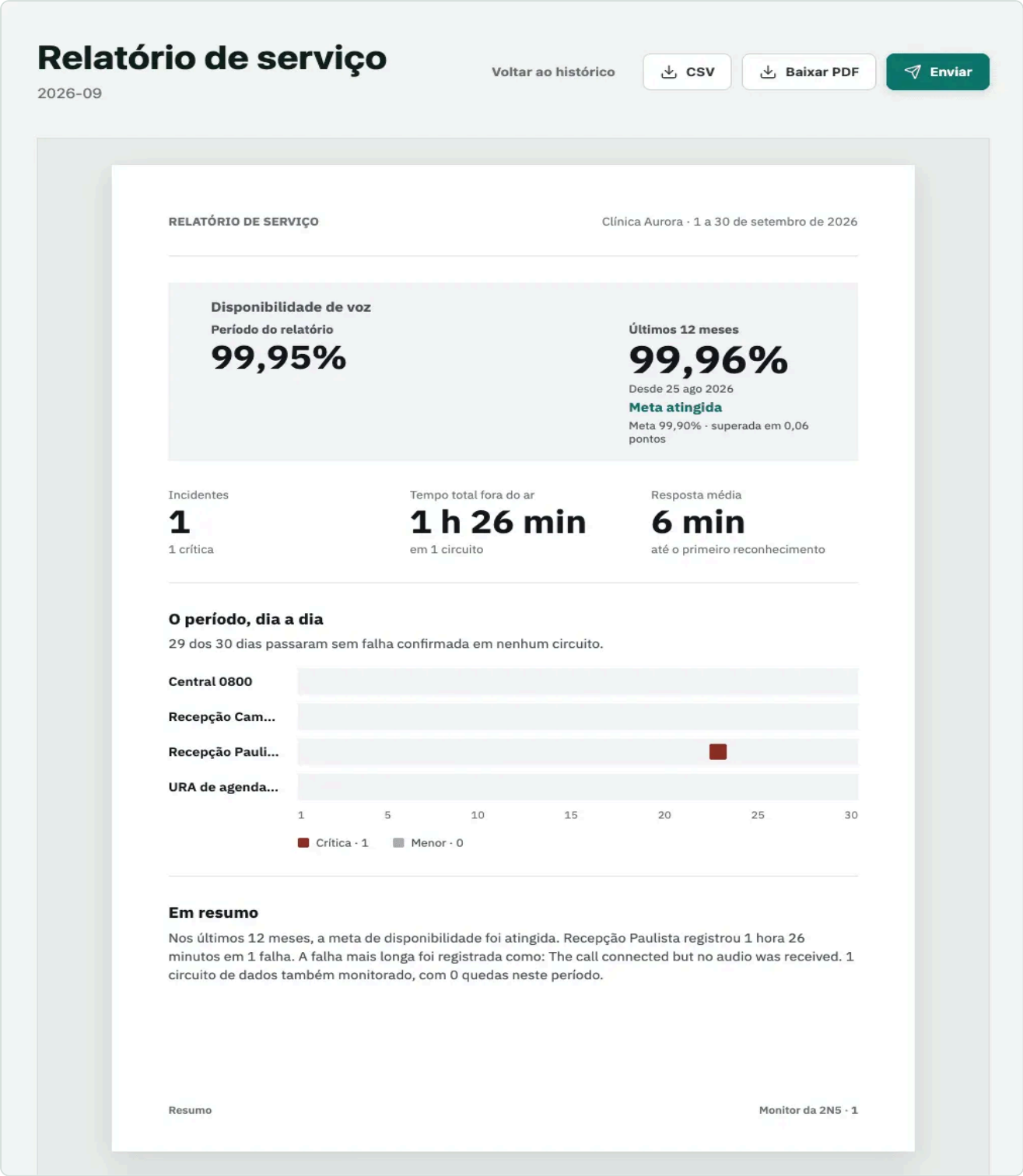
1. No menu lateral, clique em **Relatórios**. A página **Relatórios de serviço** lista os relatórios já gerados em **Histórico**, do mais recente para o mais antigo.
2. Clique em **Gerar relatório**.
3. Em **Abrangência**, escolha em **Abrange** a organização inteira ou uma entidade, e em **Período** uma destas opções:
   - **Este mês, automaticamente**: o relatório de sempre, do mês corrente.
   - **Um mês que eu escolher**: para fechar um mês anterior, como setembro.
   - **Um período personalizado**: informe **Primeiro dia** e **Último dia**, com no máximo um ano no total. É assim que se faz o relatório anual de SLA.
4. Clique em **Próximo**. Em **Conteúdo**, escreva um **Título**, se quiser, e escolha as **Páginas a incluir**, as **Severidades a incluir** e os **Circuitos**. Deixar tudo marcado gera o relatório completo.
5. Clique em **Próximo**, confira a **Revisão** e clique em **Gerar**.



O relatório novo aparece no topo do **Histórico**. Clique em **Ver** para abrir.

Ler o relatório

Na tela, o relatório aparece como as páginas do PDF. No topo ficam **Voltar ao histórico**, **CSV**, **Baixar PDF** e **Enviar**.



- **Resumo**: a **Disponibilidade de voz** do **Período do relatório** e dos **Últimos 12 meses**, com a meta e se ela foi atingida; o número de **Incidentes**, o **Tempo total fora do ar** e a **Resposta média** até o primeiro reconhecimento; **O período, dia a dia**, com uma linha por circuito e uma marca em cada dia com falha confirmada; e **Em resumo**, um parágrafo que conta o mês em palavras.
- **O que aconteceu**: cada incidente, com a data, o circuito, o que o Monitor observou, quanto tempo ficou fora do ar e em quanto tempo foi atendido, e o total no fim.
- **Comparação de circuitos**: cada circuito lado a lado, com a qualidade das chamadas.
- **Desempenho das operadoras**: cada operadora, o que foi prometido em relação ao que foi entregue.

A meta de disponibilidade fica em **Configurações**, na aba **Relatórios e relógio**, e os termos de contrato de cada operadora na aba **Contratos**. **CSV** baixa os números em planilha; **Baixar PDF** baixa o documento.

Enviar um relatório

1. Abra o relatório e clique em **Enviar**.
2. Em **Destinatários**, escolha os contatos do cliente ou digite um endereço. Para cada pessoa, escolha as páginas e o idioma do PDF.
3. Em **Mensagem**, escreva uma **Observação**, se quiser. Ela aparece depois da saudação, acima dos números.
4. Em **Revisar e enviar**, confira **Como o e-mail fica** e envie.

Cada pessoa recebe um PDF só com as páginas escolhidas para ela, com os números do relatório guardado, exatamente como estão. Um mesmo relatório pode ser enviado algumas vezes por hora; depois disso, o Monitor pede para esperar.

Programar o envio mensal

1. Na página **Relatórios de serviço**, clique em **Entrega**.
2. Em **Entrega automática**, ligue **Enviar um relatório todo mês** e escolha **Produzido no** (o dia) e **Às** (o horário).
3. Escolha o idioma do e-mail, ajuste o texto, se quiser, e marque **Incluir os números principais** para trazer a disponibilidade e os incidentes no corpo do e-mail.
4. Salve. **Próximo relatório** mostra quando sai o próximo e que período ele cobre: um mês para trás, até o fim do dia anterior.

Perguntas frequentes

A disponibilidade do relatório inclui as janelas de manutenção?

Não. O tempo dentro de uma janela de manutenção planejada fica fora do cálculo e aparece à parte. O tempo em que o próprio Monitor não conseguiu testar, o Monitoramento sem visibilidade, também fica fora, porque não é queda do seu circuito. A disponibilidade é o tempo no ar dividido pelo tempo medido no período.

Um relatório muda se eu gerar de novo depois?

Cada relatório é guardado exatamente como foi produzido, com os números e os nomes daquele momento, e abre sempre igual no Histórico. Se você gerar de novo o mesmo período, um relatório novo é criado ao lado do anterior. Isso permite enviar a uma operadora ou à diretoria um documento que não muda depois.

Como faço o relatório anual de SLA?

Em Gerar relatório, escolha Um período personalizado e informe o primeiro e o último dia do ano, por exemplo de 1º de janeiro a 31 de dezembro. Um período pode ter no máximo um ano. A primeira página traz a disponibilidade do período e a dos últimos 12 meses, comparadas com a meta de disponibilidade da sua organização.

GUIA DO USUÁRIO · CAPÍTULO 8

Pessoas e organizações

No Monitor há dois tipos de pessoa: gestores, que entram no Monitor e veem as telas, e contatos, que recebem os alertas e os relatórios sem precisar entrar. A estrutura da organização, em entidades, decide o que cada gestor vê.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

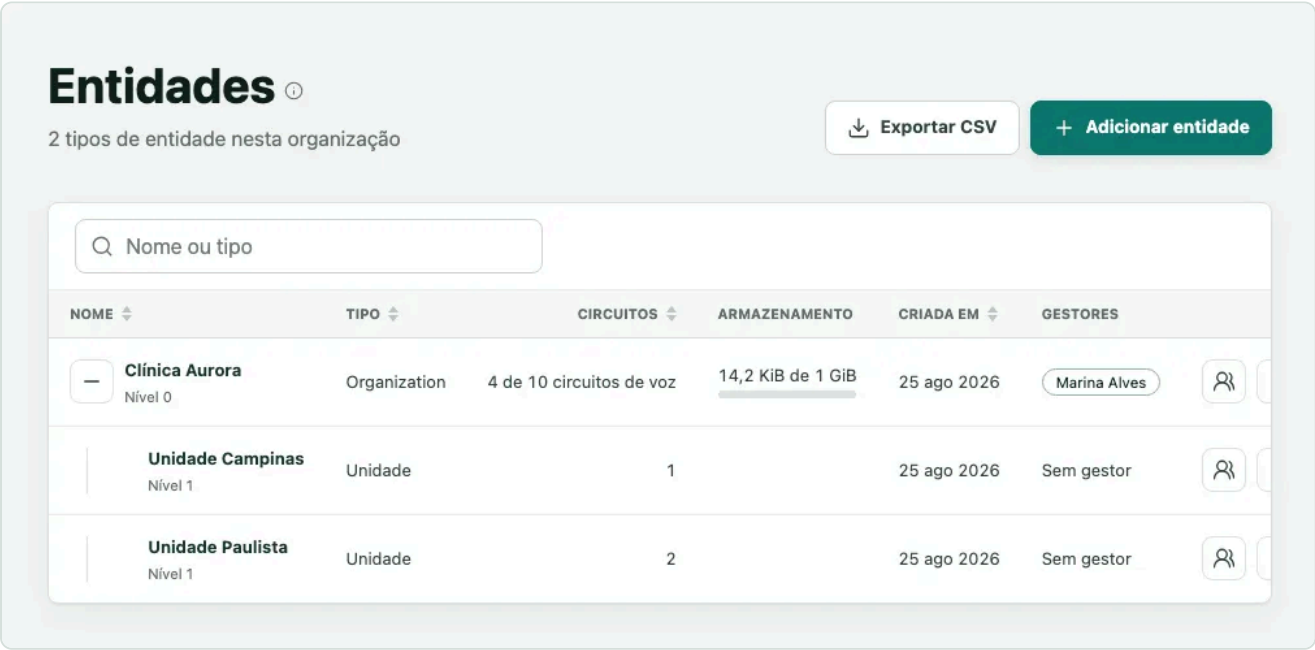
Gestores e contatos

- **Gestores** entram no Monitor com e-mail e senha. Veem o painel, os incidentes e os relatórios da parte da organização que gerenciam, e cuidam da escada de escalonamento, das entidades e dos outros gestores.
- **Contatos** não entram no Monitor. São as pessoas da escada de escalonamento, que recebem os alertas com o link para reconhecer, e os **Contatos do cliente**, que recebem os avisos de queda e de volta e podem receber os relatórios. Os contatos são cadastrados em **Escalonamento**, como explica o capítulo Incidentes e alertas.

Entidades: a estrutura da organização

A organização fica no nível 0, e abaixo dela vêm empresas, unidades, escritórios ou departamentos, em quantos níveis você precisar. Cada circuito, site e caixa de e-mail fica em uma entidade.

1. No menu lateral, em **Comunidade**, clique em **Entidades**.
2. A tabela mostra cada entidade com o **Nível**, o **Tipo**, quantos **Circuitos** tem, o **Armazenamento** usado, quando foi **Criada em** e os **Gestores**. Use **Nome ou tipo** para buscar.
3. Para criar uma entidade, clique em **Adicionar entidade**, dê um nome, escolha um tipo da organização ou digite um novo, e escolha em **Abaixo de** onde ela fica.
4. Para baixar a estrutura em planilha, clique em **Exportar CSV**.



Mover uma entidade leva junto tudo o que está abaixo dela, e cada circuito mantém o seu histórico. Uma entidade só pode ser excluída quando não há nada abaixo dela nem circuito nela.

Convidar um gestor

1. Em **Comunidade**, clique em **Gestores**. A lista mostra cada gestor com **E-mail**, **Entidade**, situação e **Último acesso**, e os convites que ainda esperam resposta.
2. Clique em **Convidar gestor**.
3. Preencha o **Nome** e o e-mail e escolha a entidade que a pessoa vai gerenciar.
4. Clique em **Enviar convite**. A pessoa recebe o e-mail, define a própria senha pelo link e entra.

Enquanto o convite espera, a lista mostra até quando o link vale, com **Enviar novamente** e **Retirar**. Para tirar o acesso de alguém, use **Remover gestor**: a sessão é encerrada na hora. **Exigir duas etapas** torna a verificação em duas etapas obrigatória para os gestores da organização.

Quem vê o quê

Um gestor vê a entidade que gerencia e tudo o que está abaixo dela, e nada ao lado:

Gestor de	Vê
A organização (nível 0)	Todas as entidades, circuitos, incidentes e relatórios.
Uma unidade	Só aquela unidade e o que estiver abaixo dela.

O painel, a lista de incidentes, os relatórios e as entidades se ajustam sozinhos ao que cada gestor pode ver. Um relatório gerado por um gestor de unidade cobre só a unidade dele.

Operadoras

Em **Comunidade**, **Operadoras** lista as operadoras dos seus circuitos, com o contato do suporte técnico de cada uma. É ali que fica o endereço para onde vão as evidências de um incidente quando é preciso abrir chamado.

Perguntas frequentes

Um gestor de uma unidade vê os circuitos das outras unidades?

Não. Um gestor vê a entidade que gerencia e tudo o que está abaixo dela, e nada ao lado. O gestor da Unidade Campinas vê só os circuitos, incidentes e relatórios de Campinas; o gestor da organização vê todas as unidades. Uma entidade pode ter vários gestores, e quem gerencia uma entidade pode convidar gestores para ela e para as entidades abaixo.

Qual é a diferença entre um gestor e um contato?

O gestor tem login: entra no Monitor, vê o painel, gera relatórios e muda o que a conta dele permite. O contato não entra no Monitor; ele recebe os alertas da escada de escalonamento, com o link para reconhecer, ou os avisos e relatórios destinados ao cliente. A mesma pessoa pode ser gestora e contato ao mesmo tempo.

O que acontece com o histórico quando um gestor sai da empresa?

Remova o gestor na tela Gestores: a sessão dele é encerrada na hora e ele deixa de ver a organização. Os circuitos, os incidentes, os relatórios e o histórico continuam na organização. Os reconhecimentos que ele fez seguem nos incidentes, com o nome dele, como registro do que aconteceu.

GUIA DO USUÁRIO · CAPÍTULO 9

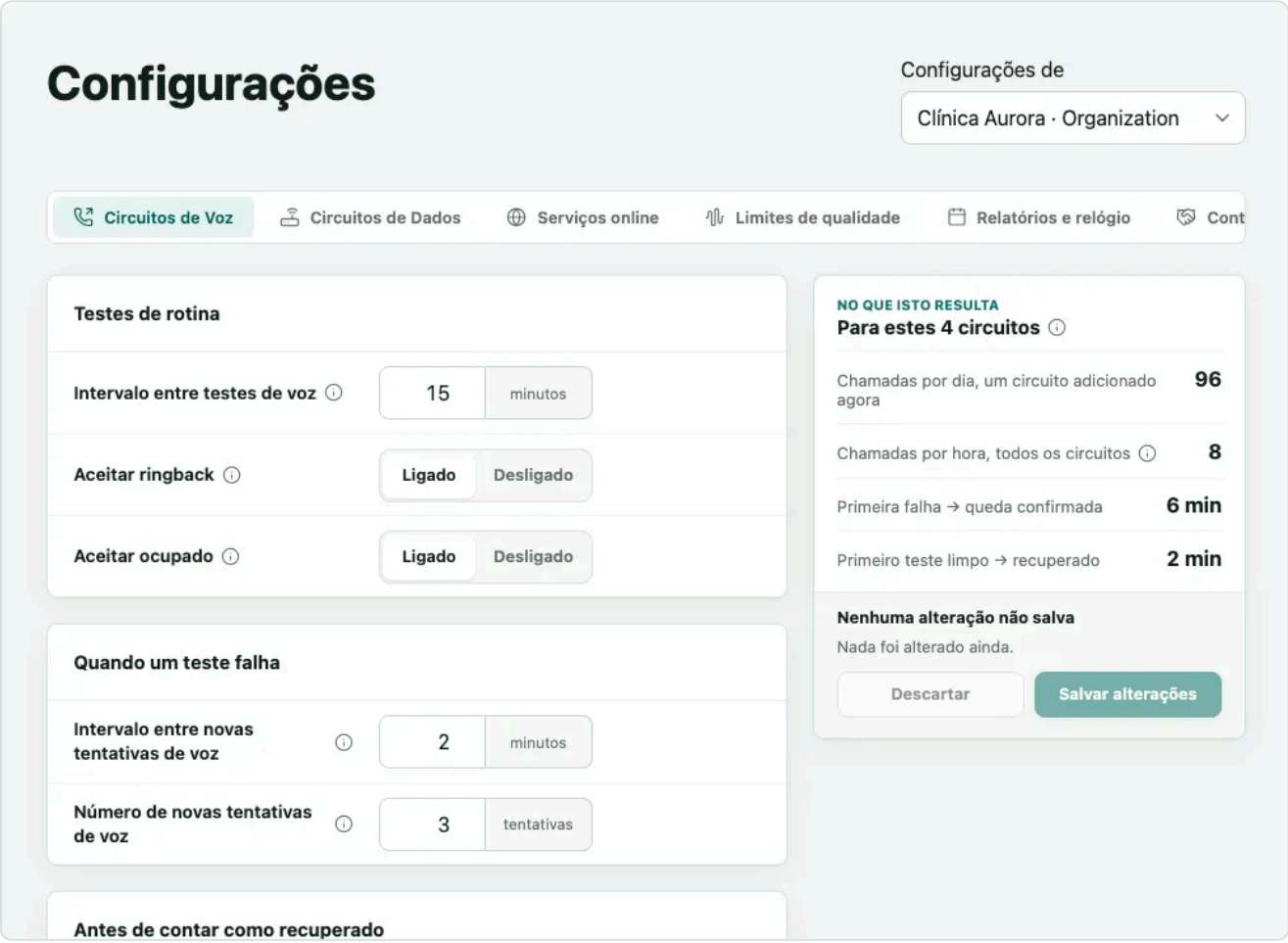
Configurações

O Monitor é um serviço gerenciado: a 2N5 cadastra os seus circuitos, configura os testes e cuida das chamadas de teste. Você ajusta o que é da sua organização, como quem é avisado, os relatórios e os valores padrão da tela Configurações, e pede à 2N5 o resto.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

A tela Configurações

1. No menu lateral, clique em **Configurações**.
2. Em **Configurações de**, escolha a organização inteira ou uma entidade. Uma entidade pode ter valores próprios, diferentes dos da organização.
3. Escolha uma aba: **Circuitos de voz**, **Circuitos de dados**, **Serviços online**, **Limites de qualidade**, **Relatórios e relógio** ou **Contratos**.
4. Mude os valores. O quadro **No que isto resulta** mostra na hora o efeito, como quantas chamadas por dia e quanto tempo da primeira falha até a queda confirmada.
5. Clique em **Salvar alterações**, ou em **Descartar** para desistir.



O que cada aba guarda:

- **Circuitos de voz**: o intervalo entre testes, se um ringback sem atendimento ou um sinal de ocupado contam como circuito funcionando, o intervalo e o número de novas tentativas antes de confirmar a queda, e quantos testes limpos confirmam a recuperação.

- **Circuitos de dados** e **Serviços online**: os padrões dos links, dos sites e das caixas de e-mail.
- **Limites de qualidade**: as notas de MOS-LQO medido abaixo das quais uma chamada conta como degradada e a partir das quais conta como plenamente saudável.
- **Relatórios e relógio**: o fuso horário da organização, usado em todas as telas, alertas e relatórios, e a meta de disponibilidade dos relatórios.
- **Contratos**: os termos de contrato das operadoras, que o relatório compara com o que foi entregue.

Cada circuito guarda os valores com que foi adicionado: uma mudança aqui vale para os circuitos adicionados depois.

O que você muda

Onde	O quê
Configurações da conta	Senha, verificação em duas etapas, sair de todos os dispositivos e excluir a sua conta.
Menu lateral e menu da conta	Idioma e tema.
Escalonamento	Quem é avisado, em que ordem, por quais endereços, e os **Tempos** de cada nível.
Entidades e **Gestores**	A estrutura da organização e quem a gerencia.
Página do circuito	Janelas de manutenção planejada.
Relatórios	Gerar, enviar e programar a entrega mensal.
Página de um incidente de conteúdo	**Esta mudança é esperada**.
Configurações	Os valores padrão que a sua conta pode alterar.

O que só a 2N5 muda

Peça à 2N5 para:

- Incluir no pacote um tipo de item ou aumentar o limite de circuitos, sites ou caixas de e-mail.
- Cadastrar um circuito novo e fazer a chamada de verificação, ou mudar o número, o intervalo de teste ou as novas tentativas de um circuito existente.
- Configurar ou trocar a gravação de referência de um circuito que atende com uma mensagem gravada.
- Mudar a frequência das medições e dos testes de velocidade de um circuito de dados, e os limites que fazem um link contar como degradado ou fora do ar.
- Mudar com que frequência um site ou uma caixa de e-mail é verificado e quando conta como fora do ar, e o que a página de um site deve mostrar.
- Instalar o agente ou configurar a verificação externa de um circuito de dados.
- Enviar um link novo para conectar uma caixa de e-mail.

Quando a tela diz que um valor é definido pela 2N5, ou que o problema é do lado da 2N5, não há nada a fazer do seu lado: a 2N5 já foi avisada. O capítulo Perguntas e ajuda diz como falar com a 2N5.

Perguntas frequentes

Mudei um valor em Configurações. Por que um circuito antigo não mudou?

Cada circuito guarda os valores com que foi adicionado. Os valores da tela Configurações são os padrões da organização ou da entidade e valem para os circuitos adicionados depois da mudança. Para mudar o intervalo de teste, as novas tentativas ou a recuperação de um circuito que já existe, peça à 2N5.

Como aumento o número de circuitos que posso monitorar?

O pacote da sua organização define quantos circuitos de voz, circuitos de dados, sites e caixas de e-mail ela pode ter. A janela Adicionar ativo mostra quanto de cada um já está em uso. Para incluir um tipo que não está no pacote ou aumentar um limite, fale com a 2N5.

Posso adicionar um circuito eu mesmo?

O botão Adicionar ativo, no topo da tela, abre a escolha entre circuito de voz, circuito de dados, site e e-mail, dentro dos limites do seu pacote. Na prática, a 2N5 normalmente cadastra e verifica os circuitos para você, porque cada circuito novo passa por uma chamada de verificação real e depende da conta de chamadas da 2N5.

GUIA DO USUÁRIO · CAPÍTULO 10

Perguntas e ajuda

Este capítulo reúne as perguntas que os clientes mais fazem no dia a dia e diz onde buscar ajuda. Dentro do Monitor, o botão de ajuda abre um tour guiado; fora dele, a equipe da 2N5 atende você pelo canal combinado na contratação.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

O tour guiado

O Monitor tem um tour que para uma vez em cada página e explica o que ela mostra.

1. No topo da tela, clique no botão **?** (**Ajuda e tour guiado**).
2. Clique em **Fazer o tour guiado**. São nove paradas curtas, uma em cada página.

Os textos de ajuda também estão nas próprias telas: o ícone **i** ao lado de um título explica o que o quadro mostra e como o número é calculado.

Como pedir ajuda à 2N5

O Monitor é um serviço gerenciado, e a 2N5 acompanha os seus circuitos junto com você.

1. Antes de escrever, anote o número do incidente, como **INC-0004**, ou o nome do circuito, e o que você viu na tela.
2. Fale com o seu contato na 2N5 pelo canal combinado na contratação.
3. Para um incidente com a operadora, copie o bloco **Evidências prontas para a operadora** da página do incidente e envie junto com o chamado.

Pedidos sobre dados pessoais, como acesso, correção ou exclusão, vão para **privacidade@2n5.com.br**. A Segurança e LGPD explica como os dados são tratados.

Para ler mais

- O glossário explica os termos que aparecem nas telas, como MOS-LQO, jitter e janela de manutenção.
- A Documentação reúne este guia, as páginas do produto e as referências de códigos SIP e causas Q.850, que aparecem no registro de observações.

Perguntas frequentes

O Monitor liga para os meus números o tempo todo? Isso atrapalha o atendimento?

O Monitor faz uma chamada de teste curta em cada circuito, no intervalo combinado, por exemplo a cada 15 ou 30 minutos, e repete só quando um teste falha. Quem atende ouve que é um teste automático e a chamada termina. A cota de chamadas por hora, no painel, mostra quanto da capacidade desta hora já foi usada.

Por que o Monitor não me avisou na primeira falha?

Porque uma falha isolada nunca vira alerta. O Monitor repete o teste e só abre incidente depois de quatro testes com falha seguidos, o primeiro e três novas tentativas, normalmente em poucos minutos. Assim você não recebe alarme falso por uma oscilação de segundos, e quando o alerta chega a falha é real.

De onde vem o horário mostrado nas telas e nos alertas?

Todos os horários das telas, dos alertas e dos relatórios usam o fuso horário da sua organização, mostrado no topo da tela ao lado do relógio, como São Paulo, UTC-3. Ele fica em Configurações, na aba Relatórios e relógio. O horário do seu computador não muda o que o Monitor mostra.

Os dados de chamadas e de contatos ficam guardados por quanto tempo?

Cada tipo de dado tem um prazo de guarda e é apagado quando o prazo termina. O áudio de uma chamada só é guardado quando a chamada é atendida por uma gravação, nunca por uma pessoa. Os prazos e os seus direitos estão na Política de Privacidade; pedidos sobre dados pessoais vão para privacidade@2n5.com.br.

Posso usar o Monitor no celular?

Sim. As telas se ajustam ao celular, com o menu lateral aberto pelo botão no topo. Para o dia a dia no celular, o mais comum é receber o alerta por e-mail e tocar no link para reconhecer o incidente, sem precisar entrar. O painel completo fica mais confortável em uma tela maior.

O produto

COMO FUNCIONA

Como funciona o monitoramento VoIP gerenciado de circuitos de voz

O monitoramento VoIP do Monitor da 2N5 é um serviço gerenciado: você diz à 2N5 quais números monitorar e quem deve saber de um problema, e ela comprova cada circuito com uma chamada real e liga para ele dia e noite, no Brasil. Você recebe o incidente com evidências, depois de um reteste que evita o falso alarme, e o relatório de SLA de cada mês.

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

O que eu preciso fazer para começar?

Preencher um formulário. Você envia à 2N5 os números a monitorar, onde cada um fica (empresa, escritório, departamento) e quem deve ser avisado quando algo falha. Todo o resto é feito pela 2N5: ninguém da sua empresa cria conta de serviço, instala software no PABX ou configura alertas. É assim que o monitoramento VoIP gerenciado funciona na prática.

Quais são as etapas?

1. **Você envia os seus circuitos.** Números, locais e quem deve saber de um problema.
2. **A 2N5 verifica cada um.** Cada circuito é comprovado com uma chamada real antes de entrar no monitoramento, e a saudação esperada é gravada como referência.
3. **A 2N5 liga a noite toda.** No ritmo combinado, cada chamada é avaliada: completou, teve áudio nos dois sentidos, a mensagem certa, a qualidade medida. Falhas são repetidas e alarmes falsos, filtrados.
4. **Você fica sabendo primeiro.** Um incidente com evidências, a escada de escalonamento por e-mail, e, para clientes Enterprise, um relatório de SLA todo mês.

Quem faz o quê?

Você	A 2N5
Envia a lista de circuitos e de contatos	Cadastra cada circuito e comprova com uma chamada real
Diz o que deve atender cada número	Grava a saudação de referência e ajusta os limites de qualidade
Escolhe quem é avisado, e em que ordem	Monta a escada de escalonamento e os relatórios
Recebe os alertas e assume os incidentes	Mantém as chamadas, a plataforma e o próprio monitoramento no ar

O que vigia o próprio monitoramento?

Se a falha estiver do lado da 2N5, por exemplo a nossa plataforma de chamadas sem resposta, o teste fica **sem visibilidade**: não conta contra o seu circuito, não entra no SLA e não acorda a sua equipe. É a 2N5 quem é avisada. Um sinal periódico avisa a 2N5 também se o monitoramento parar de rodar.

Funciona com o meu PABX e a minha operadora?

Sim. O Monitor liga para números, como um cliente liga. Por isso funciona com qualquer PABX ou plataforma de atendimento e com qualquer operadora, sem integração. Ele não depende do que o seu equipamento informa sobre si mesmo. Veja como cada plataforma costuma falhar em silêncio nas páginas de 3CX, Asterisk, Genesys Cloud, Amazon Connect e Microsoft Teams.

Onde ler mais?

O guia de monitoramento de troncos SIP, 0800 e URA explica a técnica, o verbete de monitoramento sintético define o termo, e o guia de ferramentas de monitoramento VoIP no Brasil compara o Monitor com outras ferramentas. Para o Zabbix, veja o comparativo.

Perguntas frequentes

Como funciona um serviço gerenciado de monitoramento de telefonia?

Você entrega à 2N5 a lista de números, o local de cada um e quem deve ser avisado. A 2N5 cadastra e comprova cada circuito com uma chamada real, faz as chamadas de teste, filtra os alarmes falsos, avisa a sua escada de contatos e, para clientes Enterprise, envia o relatório de SLA todo mês. Ninguém da sua empresa instala software nem configura alertas.

Como monitorar o PABX 3CX / Asterisk / Issabel?

Sem instalar nada no PABX: o Monitor da 2N5 liga para os números que entram por ele, como um cliente, e confere se a chamada completa, se há áudio nos dois sentidos e se a voz soa clara. Funciona com 3CX, Asterisk, Issabel e outros, em qualquer versão, local ou hospedado, porque não depende do que o PABX informa sobre si mesmo.

Como monitorar linhas do Genesys / Amazon Connect / Teams Direct Routing?

Do mesmo jeito, pelo lado de fora, ligando para os números que chegam à plataforma. O Monitor da 2N5 não se integra ao Genesys Cloud, ao Amazon Connect nem ao Microsoft Teams: ele liga para os números e confere o resultado como um cliente, com o código SIP quando a chamada falha. Por isso funciona com qualquer plataforma de atendimento.

Preciso instalar alguma coisa?

Não, para os circuitos de voz. A 2N5 faz as chamadas da própria plataforma. Só para acompanhar o link de internet de um local a 2N5 instala um pequeno agente lá, por acesso remoto e com a sua autorização por escrito. No PABX, no SBC e na rede de voz não entra nenhum software.

As chamadas de teste atrapalham as chamadas reais?

Cada teste é uma chamada curta para um número que você escolhe, como um tom de teste, um serviço de eco ou a sua saudação, dentro de um limite de chamadas. Ela ocupa um canal por poucos segundos, como uma chamada de cliente, e as chamadas dos seus clientes nunca são tocadas.

Quanto tempo leva para começar?

O tempo de você enviar a lista e a 2N5 verificar cada circuito com uma chamada real. Um circuito só entra no monitoramento depois de passar nessa verificação, e a saudação esperada é gravada como referência nessa etapa. A 2N5 combina com você o ritmo dos testes e quem recebe cada alerta.

A minha equipe consegue ver o painel?

Sim. Cada gestor entra no Monitor e vê a sua parte da empresa, empresa, escritório ou departamento, com o estado de cada circuito, os incidentes e os relatórios. Quem não é gestor continua recebendo os alertas e os relatórios por e-mail, sem precisar entrar no painel.

E se eu tiver um NOC terceirizado?

O Monitor não substitui quem resolve a falha; ele garante que alguém fique sabendo dela, com as evidências. O NOC pode ser uma das camadas da escada de escalonamento, recebendo o alerta confirmado com o código SIP e a causa Q.850, e assumindo o incidente com um toque.

Qual ferramenta monitora troncos SIP, links de internet e sites juntos?

O Monitor da 2N5 reúne, em um só serviço gerenciado, os circuitos de voz (troncos SIP, 0800, 0300 e 4004), os links de internet, os sites e o e-mail, com a mesma escada de alertas e o mesmo painel. Outras ferramentas cobrem partes disso em separado; os comparativos do site mostram o que cada uma faz, com a fonte de cada afirmação.

MONITORAMENTO DE TRONCOS SIP E VOIP

Monitoramento de troncos SIP e VoIP com chamadas de teste reais

O monitoramento de troncos SIP e VoIP do Monitor da 2N5 liga para cada tronco como um cliente liga, 24 horas por dia, no Brasil. Se a chamada não completa, não leva áudio nos dois sentidos ou soa mal, a sua equipe fica sabendo primeiro, com o código SIP que a operadora devolveu. Cada falha é testada de novo antes do alerta, sem falso alarme.

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

Como saber se um tronco SIP parou de completar chamadas?

A forma direta é ligar para ele. O Monitor faz uma chamada de teste real para cada **circuito de voz** (tronco SIP, ramal de filial ou número da central de atendimento) no ritmo combinado, e confere três coisas: se a chamada completou, se o áudio passou nos dois sentidos e se a voz soou clara. É o monitoramento de chamadas SIP feito do lado de fora, como o cliente vive. Quando qualquer uma das três falha de forma confirmada, a sua equipe recebe o alerta com o código SIP como prova.

O monitoramento comum pergunta ao equipamento se ele está no ar. O PABX responde que sim, o tronco aparece registrado e a rede está verde, enquanto quem liga ouve silêncio. Uma chamada real não depende do que o equipamento diz sobre si mesmo. Essa técnica se chama monitoramento sintético, e o guia de chamadas sintéticas explica quando usá-la junto com o monitoramento passivo, e o guia de monitoramento passivo vs chamadas de teste ativas compara os dois em detalhe.

O que cada chamada de teste verifica?

Verificação	O que conta como falha
A chamada completa	Recusa da operadora (por exemplo SIP 403, 404, 480 ou 503), ou nenhuma resposta
Atende quem deveria atender	A saudação esperada, o tom de teste ou o serviço de eco não atendem
Áudio nos dois sentidos	Áudio em um só sentido ou ausente (ligação muda)
Qualidade de voz	MOS-LQO medido abaixo do limite combinado: a chamada conta como degradada

Cada resultado traz o código SIP e a causa Q.850. Para ler os mais comuns, veja SIP 503, SIP 486, SIP 480, SIP 408 e as causas Q.850 16, 34 e 127. Se a ligação completa e fica muda, o guia de ligação muda e áudio de um lado só mostra as causas. Para o tempo até o primeiro toque, veja o post dial delay, e para a taxa de chamadas atendidas, o ASR e ACD.

Como o Monitor evita alarmes falsos?

Uma chamada que falha é repetida no seu ritmo, o reteste antes de alertar. Só falhas seguidas, quatro por padrão (a primeira e três novas tentativas), abrem um incidente. Uma oscilação de um minuto não acorda ninguém de madrugada, e um alerta às 2h é sempre real.

Se o problema estiver do lado da 2N5, por exemplo a nossa plataforma de chamadas sem resposta, o teste fica **sem visibilidade**: não conta contra o tronco, não entra no SLA e não avisa o cliente. Janelas de manutenção silenciam os alertas enquanto a operadora ou a sua equipe trabalha no circuito.

Que evidências vão para a operadora?

Cada incidente traz um bloco pronto para colar no chamado: o circuito, a operadora, o primeiro sintoma, o código SIP e a causa Q.850 de cada chamada, e a última chamada saudável. É a resposta para o “nenhum defeito encontrado”: horário, número chamado e o que a rota devolveu.

Exemplo de evidência, com dados de demonstração: *SIP 503 Service Unavailable, Q.850 causa 34 (nenhum circuito ou canal disponível), confirmado após 4 chamadas com falha*.

Quem é avisado, e como?

A escada de escalonamento da sua empresa, por e-mail, um nível de cada vez, até alguém reconhecer o incidente com um toque no celular. Veja alertas e escalonamento.

Como o Monitor se compara a ferramentas de rede e de captura?

Ferramentas de rede e de captura respondem a perguntas diferentes: o que o equipamento informa e o que passou pela rede. O Monitor responde se uma chamada real completa. Veja os comparativos com o VoIPmonitor, o Zabbix e o PRTG, e o guia de monitoramento de circuitos de voz.

Perguntas frequentes

Como monitorar um tronco SIP 24 horas?

Com chamadas de teste reais em intervalo fixo, dia e noite, e não apenas com o estado do registro. O Monitor da 2N5 liga para um número atendido por esse tronco, confere se a chamada completou, se havia áudio nos dois sentidos e se a voz soou clara, repete a chamada que falha e só então alerta a equipe, com o código SIP e a causa Q.850.

Qual a diferença entre monitoramento passivo e chamadas de teste ativas?

O monitoramento passivo analisa as chamadas que os clientes já fizeram, por captura de pacotes ou relatórios de chamadas; mostra o que aconteceu, mas não vê nada quando ninguém liga. As chamadas de teste ativas ligam em horários marcados e acham a falha antes do cliente, inclusive de madrugada. Quem precisa saber primeiro precisa do ativo, e os dois se complementam.

O que é monitoramento sintético (chamadas sintéticas)?

Monitoramento sintético, ou de chamadas sintéticas, é o teste em que um sistema faz chamadas reais para o seu número em horários marcados e registra o resultado de cada uma: se completou, o que atendeu, se havia áudio e como estava a qualidade. É o que o Monitor da 2N5 faz em cada circuito de voz, em oposição ao monitoramento passivo.

O que significam os erros SIP 503, 486, 480 e 408 e as causas Q.850 16, 34 e 127?

O SIP 503 diz que o servidor não consegue atender agora, por sobrecarga, manutenção ou falta de canal. O 486 é ocupado, o 480 é destino temporariamente indisponível e o 408 é tempo esgotado sem resposta. Na Q.850, a causa 16 é desligamento normal, a 34 é falta de circuito ou canal e a 127 é falha de interconexão sem detalhe. O Monitor guarda os dois códigos de cada falha.

O Monitor precisa de acesso ao meu PABX ou ao meu SBC?

Não. A 2N5 faz as chamadas de teste da própria plataforma, para os números que você indicar, como qualquer pessoa faria. Nada é instalado no seu PABX, no SBC ou na rede de voz, e o monitoramento não depende do que o equipamento informa sobre si mesmo. Por isso funciona com qualquer PABX ou plataforma de atendimento, sem integração.

Com que frequência cada tronco é testado?

No ritmo combinado com você, por exemplo a cada 15 minutos, ou em horários fixos, inclusive de madrugada e nos fins de semana. Uma chamada que falha é repetida antes de qualquer alerta, e só quatro falhas seguidas, a primeira e três novas tentativas, abrem um incidente. Assim uma oscilação de um minuto não acorda ninguém e um alerta de madrugada é sempre real.

As chamadas de teste ocupam canais do meu tronco?

Cada teste é uma chamada curta para um número que você escolhe, dentro de um limite de chamadas combinado. Ela ocupa um canal do tronco por poucos segundos, como uma chamada de cliente, e nunca toca nas chamadas dos seus clientes. O ritmo dos testes é combinado com você justamente para não disputar canal com o seu atendimento.

Funciona com qualquer operadora?

Sim. O teste disca o número, então funciona com troncos SIP e E1 de qualquer operadora e com qualquer PABX, sem integração. O resultado de cada chamada traz o código SIP e a causa Q.850 que a rota devolveu, que é justamente o que a operadora precisa para abrir ou encerrar um chamado.

O que acontece quando a falha é do lado da 2N5?

O teste é marcado como sem visibilidade, nunca como falha do seu tronco. Ele não conta contra o seu SLA, não abre incidente para você e não acorda ninguém da sua equipe; quem é avisada é a 2N5, se a situação durar mais de 30 minutos. Assim a falha do próprio monitoramento nunca é cobrada do seu circuito.

TESTE E MONITORAMENTO DE 0800 E URA

Teste e monitoramento de 0800 e URA telefônica com chamadas reais

O Monitor da 2N5 faz o teste e o monitoramento de 0800 e URA com chamadas reais, 24 horas por dia, no Brasil. Ele liga para o seu 0800, 0300, 4004 ou número fixo, confere se a URA telefônica atende com a mensagem certa e avisa a equipe antes dos seus clientes, depois de repetir a chamada que falhou.

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

Como saber se o meu 0800 está funcionando 24 horas por dia?

Ligando para ele, a toda hora, como um cliente. O Monitor faz uma chamada de teste real para o seu 0800, 0300, 4004 ou número fixo no ritmo combinado, inclusive de madrugada, e confere se a sua **URA telefônica** atendeu com a mensagem certa. Um painel verde no PABX não prova isso; só uma chamada que chega do lado de fora prova.

Cada número monitorado é um **circuito de voz** no Monitor, com a sua agenda, o seu limite de qualidade e as pessoas que devem saber quando ele falha. O guia de 0800 e URA mostra o passo a passo de quando o número para, e o de 0800 que não completa do celular trata de um problema que só o teste de fora revela. Os termos estão no glossário: 0800, URA e números 4004, 4003 e 3003.

O que pode atender o número, e como cada caso é julgado?

Na implantação, a 2N5 define o que deve atender cada número. Essa escolha decide o que conta como funcionando:

O que deve atender	Passa quando
Uma saudação ou mensagem gravada (a URA)	A chamada é atendida e a saudação escolhida é ouvida. A mensagem de erro de uma operadora não passa
Um tom de teste ou serviço de eco	A chamada é atendida e os tons enviados voltam
Outro: pode tocar ou ser atendido	Tocar até o fim ou ser atendido com áudio, conforme o combinado. Quem atende ouve que é um teste automático

Ocupado, sem atendimento ou tocar até o fim é falha para uma URA: ela atende toda chamada sozinha.

Por que a URA precisa de uma gravação de referência?

Porque “atendeu” não basta. Um número pode completar e tocar a mensagem da operadora avisando que ele não existe, ou uma URA pode ser trocada sem aviso. A 2N5 grava a saudação de referência de cada número na implantação, e cada chamada compara o que ouviu com ela. Essa mesma comparação mede a qualidade de áudio, o MOS-LQO.

O que o Decreto 11.034 (Decreto do SAC) exige do atendimento telefônico?

O Decreto 11.034/2022, em vigor desde 3 de outubro de 2022 e até 1º de novembro de 2026, exige acesso telefônico ao SAC, acesso 24 horas por dia, sete dias por semana, por pelo menos um canal integrado, que não é necessariamente o telefone, e atendimento humano por pelo menos 8 horas por dia. A partir de 2 de novembro de 2026 vale o Decreto 13.135/2026, que o revoga e mantém o telefone

obrigatório, com atendimento humano das 8h às 20h todos os dias (art. 14), e exige ao menos um canal eletrônico 24 horas (art. 12). Nenhum dos dois diz que o 0800 precisa funcionar 24 horas. Para os setores regulados, mostrar que o 0800 e a URA estavam no ar é a parte difícil. Os relatórios de SLA do Monitor mostram a disponibilidade de cada número no ano e no mês, com cada falha e o momento em que alguém assumiu. O guia do decreto do SAC e do RGC traz os artigos.

Quem fica sabendo quando o 0800 cai?

A escada de escalonamento da sua empresa, por e-mail, até alguém reconhecer o incidente. Veja alertas e escalonamento.

Como o Monitor se compara a outras ferramentas de teste de 0800 e URA?

A comparação está nas páginas de alternativas ao Cyara e de Monitor da 2N5 vs Klearcom, com a fonte de cada afirmação sobre os concorrentes e o que não foi verificado.

Perguntas frequentes

Como saber se o meu 0800 está fora do ar?

Ligando para ele de fora, em intervalo fixo, e conferindo o que atendeu. O painel do PABX pode estar verde enquanto a operadora não entrega as chamadas. O Monitor da 2N5 liga para o número como um cliente, compara a mensagem com a gravação de referência e, se a falha se repetir, avisa a sua equipe com o código SIP que a rota devolveu.

Existe empresa que testa 0800 e URA automaticamente no Brasil?

Sim. A 2N5 oferece o Monitor, um serviço gerenciado que liga, a partir do Brasil, para 0800, 0300, 4004 e números fixos, ouve a URA telefônica e compara a mensagem com uma gravação de referência. Também existem serviços internacionais de teste de números gratuitos; os comparativos do site mostram as diferenças, com a fonte de cada afirmação.

Como testar uma URA telefônica sem ligar manualmente?

Com uma chamada de teste automática: um sistema liga para o número em horários marcados, ouve o que atende e compara com a gravação da saudação esperada. Se a mensagem muda, ou a operadora toca um aviso de número inexistente, o teste falha. No Monitor da 2N5 a referência é gravada na implantação, e você não precisa ligar nem programar nada.

Com que frequência testar o 0800 e a URA, inclusive de madrugada?

Quanto menor o intervalo, menos tempo uma queda passa sem ser vista. Cada número tem a sua agenda no Monitor, em intervalos como 15 minutos ou em horários fixos, inclusive de madrugada e nos fins de semana, quando ninguém da equipe está olhando. Uma chamada que falha é repetida antes de qualquer alerta, para não haver falso alarme.

O SAC precisa funcionar 24 horas?

Até 1º de novembro de 2026, o Decreto 11.034/2022 exige acesso ao SAC 24 horas por dia, sete dias por semana, por pelo menos um canal integrado, não necessariamente o telefone, e atendimento humano por telefone por no mínimo 8 horas diárias. A partir de 2 de novembro de 2026, o Decreto 13.135/2026 exige um canal eletrônico 24 horas e atendimento humano por telefone das 8h às 20h. O guia do decreto traz os artigos.

O que o Decreto 11.034 (Decreto do SAC) exige do atendimento telefônico?

Até 1º de novembro de 2026, o Decreto 11.034/2022 torna obrigatório o atendimento por telefone (art. 4º, § 2º), com no mínimo 8 horas diárias de atendimento humano e reclamação e cancelamento no primeiro menu (art. 5º). A partir de 2 de novembro de 2026 vale o Decreto 13.135/2026, que o revoga: atendimento humano por telefone das 8h às 20h, todos os dias (art. 14). Nenhum dos dois cita o 0800.

Como saber se o número de telefone da empresa está funcionando?

Ligue para ele de fora da empresa e de outra rede, porque uma chamada interna não passa pela operadora. Para fazer isso toda hora, use chamadas de teste automáticas: o Monitor da 2N5 liga para o número, 0800, 0300, 4004 ou fixo, confere se completou, se havia áudio e o que atendeu, e avisa quando a falha se confirma.

Qual o melhor serviço de monitoramento de URA?

Depende do que você precisa testar. Procure um serviço que ligue de verdade, a partir do país do número, e não apenas teste a rede; que compare a mensagem com uma gravação de referência, para pegar a URA trocada ou o aviso da operadora; que repita a chamada antes de alertar; e que entregue o código SIP como prova. O Monitor da 2N5 faz essas quatro coisas.

Como testar um 0800 do Brasil de fora do país?

Um 0800 pertence à numeração brasileira, e uma chamada que vem do exterior pode não completar, dependendo da operadora, mesmo com o número funcionando. Por isso o teste fiel é o que parte do Brasil. As chamadas do Monitor da 2N5 partem de operadoras no Brasil, como a de um cliente local, e você não precisa fazer nada para isso.

A chamada de teste chega a falar com um atendente?

Não, quando o número é atendido pela URA ou por uma gravação: a chamada ouve a saudação esperada e desliga. Se o circuito puder ser atendido por uma pessoa, ela ouve antes uma mensagem avisando que é um teste automático, e a chamada termina. A voz de uma pessoa nunca é guardada, para respeitar a privacidade de quem atende.

Vocês guardam o áudio das chamadas?

Só quando quem atende é a gravação ou a URA que você informou, para provar que a linha funciona e medir a qualidade. A voz de uma pessoa nunca é guardada. O áudio guardado é criptografado e fica guardado pelo prazo que a 2N5 definir, e depois é excluído junto com o seu registro.

Como vocês sabem que a mensagem da URA mudou?

Na implantação, a 2N5 grava a saudação de referência de cada número. Cada chamada de teste compara o que ouviu com essa gravação. Uma mensagem diferente, como a de uma operadora dizendo que o número não existe, ou uma URA trocada sem aviso, não passa, e a falha entra na mesma rotina de reteste e alerta.

O teste custa ligação para a minha empresa?

As chamadas de teste partem da plataforma da 2N5 e fazem parte do serviço. Para um 0800, como para qualquer ligação recebida, a tarifa de entrada segue o seu contrato com a operadora. O plano do Monitor não inclui, nem substitui, o que a sua operadora cobra pelo recebimento das chamadas.

QUALIDADE DE VOZ

Qualidade de voz VoIP medida em cada chamada, com MOS-LQO

O Monitor da 2N5 mede a qualidade de voz de cada chamada de teste a partir do áudio que ela recebeu, comparado com a gravação esperada, e não por estimativa de rede. O resultado é o MOS-LQO, uma nota de 1 a 5, e a equipe é avisada quando a qualidade de áudio da chamada cai abaixo do limite combinado e a queda se confirma.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

Como medir a qualidade de voz de um tronco SIP ou de um 0800?

Escutando uma chamada real. O Monitor grava o áudio que a chamada de teste recebeu e o compara com a gravação esperada, a saudação da sua URA ou o tom de teste, usando um modelo perceptual que dá uma nota de 1 a 5, o **MOS-LQO**. É uma medida do que um cliente ouviria, e não uma conta feita com números da rede. É assim que o monitoramento de qualidade de chamada pega uma ligação que completa e soa mal.

Medido ou estimado: qual a diferença?

	MOS estimado (modelo E)	MOS-LQO medido (Monitor)
De onde vem	Perda de pacotes, jitter e atraso informados pela rede	O áudio que a chamada recebeu, comparado com a referência
Padrão	ITU-T G.107 (fator R)	ITU-T P.800.1 (qualidade de escuta objetiva, com referência)
Vê áudio cortado na origem	Não	Sim
Vê uma mensagem errada	Não	Sim: a comparação com a referência não passa

As duas medidas têm o seu lugar. Uma estimativa de rede é útil para olhar a rede; uma chamada escutada diz se a voz chegou. Veja o glossário de MOS, de MOS-LQO e de POLQA e PESQ, e o guia de MOS e MOS-LQO na prática.

Que nota é boa?

A escala MOS vai de 1 (ruim) a 5 (excelente), como na ITU-T P.800. Na prática, perto de 4 a voz soa clara, e abaixo de 3 as pessoas começam a reclamar. Os limites padrão do Monitor são:

Faixa	Leitura
3,8 ou mais	Saudável
De 3,0 a 3,8	Em operação, com a nota marcada abaixo do ideal
Abaixo de 3,0	Degradado: a chamada de teste conta como degradada

Onde a qualidade aparece?

Na página de cada circuito, com a nota de cada chamada de teste e as linhas de limite, no painel ao lado do estado do circuito, e nos relatórios de SLA. Uma queda abaixo do limite passa pelas mesmas novas tentativas de qualquer falha antes de virar alerta.

Por que a gravação de referência é necessária?

Porque um modelo perceptual compara dois sinais: o que deveria ser ouvido e o que foi ouvido. Na implantação, a 2N5 grava a referência de cada número. O áudio guardado é o da gravação ou da URA, nunca a voz de uma pessoa, e é guardado pelo prazo que a 2N5 definir.

E o jitter, a perda de pacotes e o atraso?

A nota medida mostra o efeito na voz; o jitter e a perda de pacotes ajudam a achar a causa na rede. Para ver se a piora veio do link de internet do local, veja o monitoramento do link de internet. Se o problema é uma ligação muda ou com áudio de um lado só, o guia de ligação muda lista as causas mais comuns.

Como o Monitor se compara a ferramentas que estimam o MOS pela rede?

Veja o comparativo com o PRTG, que estima a nota a partir da rede, e com o VoIPmonitor, que analisa chamadas capturadas, cada um com a fonte das afirmações.

Perguntas frequentes

O que é MOS em VoIP e qual é uma nota boa?

MOS (Mean Opinion Score) é a nota de 1 a 5 que resume a qualidade de uma chamada de voz, na escala da ITU-T P.800. Perto de 4 a voz soa clara, e abaixo de 3 as pessoas começam a reclamar. Uma nota boa para o seu circuito é a que se mantém estável e longe do limite de alerta que você combinou.

Qual a diferença entre MOS de rede e MOS-LQO?

O MOS de rede é estimado: um modelo calcula a nota a partir de perda de pacotes, jitter e atraso, sem ouvir nada (ITU-T G.107). O MOS-LQO é medido: um modelo perceptual compara o áudio que chegou com a gravação de referência (ITU-T P.800.1). POLQA e PESQ são modelos desse tipo, e só se comparam notas do mesmo modelo.

Como medir a qualidade de voz de uma ligação VoIP?

Escutando a chamada, e não só olhando a rede. Faça uma chamada de teste, guarde o áudio que chegou e compare com a gravação esperada usando um modelo perceptual, que dá uma nota de 1 a 5. É o que o Monitor da 2N5 faz em toda chamada de teste atendida, a toda hora, e ele alerta quando a nota cai abaixo do limite combinado.

Que modelo de medição vocês usam?

Um modelo perceptual de qualidade de escuta com referência, que devolve MOS-LQO (ITU-T P.800.1). Ele compara o áudio recebido com o áudio de referência e devolve uma nota na escala MOS. Por usar uma referência gravada na implantação, o resultado também revela uma mensagem errada, um áudio cortado e uma ligação muda.

Quais são os limites?

Por padrão, o circuito está saudável com MOS-LQO a partir de 3,8 e degradado abaixo de 3,0; entre os dois, a chamada passa com uma observação. A 2N5 ajusta os limites com você, por circuito, na implantação, porque uma linha de atendimento exige mais da voz do que uma linha de teste interna.

O que acontece quando a qualidade cai?

Uma nota abaixo do limite marca a chamada de teste como degradada, e ela passa pelas mesmas novas tentativas de qualquer falha, o reteste antes de alertar. Se continuar, abre um incidente de qualidade e a escada de escalonamento é avisada, com a nota de cada chamada como prova para a operadora.

ALERTA DE QUEDA DE LINHA E ESCALONAMENTO

Alerta de queda de linha de voz, escalonado até alguém assumir

O alerta de queda de linha do Monitor da 2N5 só dispara para falha confirmada, sem falso alarme: a chamada que falha é repetida antes. Quando um circuito de voz cai de verdade, a primeira camada da sua escada é avisada por e-mail e, se ninguém confirmar a tempo, o alerta sobe até alguém assumir o incidente com um toque no celular.

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

Como garantir que alguém fique sabendo quando a linha cai de madrugada?

Com uma escada de escalonamento que não para até alguém assumir. No Monitor, cada incidente confirmado avisa a **camada 1** por e-mail. Se ninguém confirmar no tempo combinado, avisa a camada 2, depois a 3. Uma única confirmação, um toque no link do e-mail, para a subida e registra quem assumiu. É o alerta de queda de linha que chega antes da reclamação do cliente.

O que acontece entre a falha e o alerta?

Momento	O que o Monitor faz
Uma chamada de teste falha	Repete a chamada no seu ritmo; ninguém é avisado ainda
Falhas seguidas (quatro por padrão)	Abre um incidente com as evidências: códigos SIP, causas Q.850, cada chamada
Incidente aberto	Avisa a camada 1 e os contatos do cliente, por e-mail
Ninguém confirmou a tempo	Avisa a camada seguinte, até a última
Alguém confirma com um toque	Para a subida; o incidente mostra quem e quando
O circuito volta	Fecha o incidente e avisa os contatos do cliente que ele foi resolvido

O tempo até a primeira confirmação entra nos relatórios de SLA como resposta média, para mostrar o quanto a equipe demora para assumir (veja MTTR e MTTA).

Quem fica fora da escada, mas é avisado?

- **Contatos do cliente**: são avisados quando um serviço tem um problema, inclusive qualidade de voz ruim, e quando ele é resolvido. Eles não fazem parte da subida.
- **Administradores**: avisados quando nenhuma camada confirma.

Por que só falhas confirmadas viram alerta?

Porque um alerta às 2h precisa ser real, ou a equipe para de olhar. Uma oscilação de um minuto, uma rota que falhou uma vez ou um problema do lado da própria 2N5 nunca acordam ninguém. Quando a falha é da 2N5, o teste fica sem visibilidade, não conta contra o circuito e é a 2N5 quem recebe o aviso. O guia de alerta de queda de linha sem falso alarme explica o reteste passo a passo.

Dá para silenciar alertas durante uma manutenção?

Sim. Uma janela de manutenção cobre os circuitos que você escolher, num horário marcado. Durante a janela, as falhas desses circuitos não abrem incidente.

Como o Monitor se compara a outros serviços de teste contínuo?

O reteste antes de alertar também existe em outros serviços de teste contínuo de contact center. Veja o comparativo com a alternativa ao Hammer VoiceWatch, com a fonte de cada afirmação.

Perguntas frequentes

Como receber alerta quando a linha telefônica cair?

Cadastre o e-mail da pessoa como contato no Monitor da 2N5. Quando um incidente é confirmado, chega uma mensagem com as evidências e um link, e um toque nele confirma que você assumiu. Cada pessoa pode ter mais de um endereço, e o alerta só é enviado depois de a falha ser confirmada pelo reteste, nunca por uma única chamada que falhou.

Como evitar falso alarme no monitoramento de telefonia?

Confirmando a falha antes de alertar. No Monitor da 2N5, uma chamada que falha é repetida, o reteste antes de alertar, e só quatro falhas seguidas, a primeira e três novas tentativas, abrem um incidente. Uma oscilação de um minuto, uma rota que falhou uma vez e um problema do lado da própria 2N5 nunca acordam ninguém.

Como saber que a linha caiu antes dos clientes?

Ligando para o número de fora, a toda hora, em vez de esperar o cliente reclamar. O Monitor da 2N5 faz uma chamada de teste por circuito no ritmo combinado, inclusive de madrugada, e quando a falha se confirma avisa a primeira camada da sua escada por e-mail, com o código SIP, antes de a primeira reclamação chegar.

Por quais canais os alertas chegam?

Por e-mail, com as evidências e os códigos do incidente e um link: um toque nele confirma que você assumiu o incidente, sem precisar entrar no sistema. O aviso só sai depois de a falha ser confirmada pelo reteste, e a primeira camada da escada o recebe antes das demais.

O que acontece quando alguém confirma?

A subida para. Basta uma confirmação, um toque no link do e-mail: as camadas seguintes não são acordadas, e o incidente mostra quem assumiu e quando. O tempo até essa primeira confirmação também entra no relatório mensal como resposta média da equipe.

E se ninguém confirmar?

O alerta sobe camada por camada, no tempo que você definiu para cada uma. Se nenhuma camada confirmar, os administradores da sua empresa são avisados. Assim um incidente de madrugada não fica parado em uma única pessoa que não viu a mensagem.

Como evitar alertas durante uma manutenção programada?

Com uma janela de manutenção para os circuitos afetados, num horário marcado. Durante a janela, as falhas desses circuitos não abrem incidente e ninguém é acordado. Fora do horário da janela, o monitoramento volta ao normal sozinho e uma falha que continue é tratada como qualquer outra.

RELATÓRIOS DE SLA

Relatório de SLA da operadora de telefonia, com o número de 12 meses

O Monitor da 2N5 entrega todo mês um relatório de SLA da operadora de telefonia, com a disponibilidade de cada circuito de voz no período e nos últimos 12 meses, os incidentes, o tempo fora do ar e o tempo até alguém assumir. É a evidência para cobrar o SLA da operadora, com provas, e para a próxima negociação de contrato.

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

Como gerar um relatório de SLA de telefonia por mês e por ano?

Medindo cada circuito o tempo todo e somando. Como o Monitor liga para cada circuito de voz no ritmo combinado, ele sabe quando cada um esteve fora do ar e por quanto tempo. Todo mês ele monta o relatório de serviço com a disponibilidade do período e dos últimos 12 meses, e o envia por e-mail às pessoas que você escolheu. Os relatórios e o SLA são para clientes Enterprise.

O que o relatório traz?

Bloco	O que mostra
Disponibilidade de voz	O período do relatório e os últimos 12 meses, contra a meta do contrato
Incidentes	Quantos, de que gravidade, e a duração de cada um
Tempo fora do ar	O total no período, por circuito
Resposta média	O tempo até o primeiro reconhecimento de cada incidente
O período, dia a dia	Quais dias tiveram falha confirmada em algum circuito
Por circuito e por operadora	A disponibilidade de cada circuito e de cada operadora

Exemplo com dados de demonstração: disponibilidade de 99,89% no mês e 99,91% nos últimos 12 meses, meta de 99,90% atingida, 4 incidentes, 3 h 55 min fora do ar e 6 minutos, em média, até o primeiro reconhecimento.

Quanto tempo fora do ar cabe em 99,9%?

Em um ano de 365 dias, 99,9% de disponibilidade permite cerca de 8 horas e 46 minutos fora do ar; 99,95%, cerca de 4 horas e 23 minutos; 99,99%, cerca de 53 minutos. Em um mês de 30 dias, 99,9% permite cerca de 43 minutos. A conta é sempre a mesma: o tempo do período multiplicado por (100% menos a meta). A calculadora de SLA faz a conta para qualquer meta e período, e o guia SLA de telefonia: cálculo anual e mensal explica o que conta como queda. O verbete SLA resume os termos.

Como usar o relatório para cobrar o SLA da operadora?

Cada incidente do relatório traz o início, o fim e a duração, e cada chamada de teste traz o código SIP e a causa Q.850 que a rota devolveu. Com isso, o chamado à operadora deixa de ser “a linha caiu” e passa a ser algo como “o circuito falhou das 02h14 às 02h51, com SIP 503 e causa 34” (exemplo com dados de demonstração). O guia como cobrar o SLA da operadora com provas mostra o passo a passo, e o guia do Decreto do SAC explica como provar a disponibilidade em setores regulados.

O que não entra na conta?

Os períodos em que o próprio monitoramento ficou sem visibilidade por um problema do lado da 2N5. Eles saem da conta e aparecem separados, porque a cegueira do monitoramento não é queda do seu circuito, e um número de SLA honesto não pode misturar as duas coisas.

Como o Monitor se compara a ferramentas de SLA?

Veja o comparativo com a Sipfront, que também tem um recurso de SLA, com a fonte de cada afirmação.

Perguntas frequentes

Como calcular o SLA de disponibilidade do meu 0800?

Divida o tempo em que o 0800 completou chamadas pelo tempo total do período e multiplique por 100. Em 30 dias (43.200 minutos), 90 minutos fora do ar dão 99,79%. O difícil é medir o tempo fora do ar: o Monitor da 2N5 mede com chamadas reais, circuito por circuito, e soma a duração de cada incidente confirmado.

Como cobrar o SLA da operadora com provas?

Leve à operadora o relatório e, para cada incidente, o horário de início e de fim, o número chamado, o código SIP e a causa Q.850 de cada chamada de teste e a última chamada saudável. É o registro que costuma faltar quando a operadora diz que não encontrou defeito. Confira no contrato qual medição vale e se a manutenção programada fica fora.

99,9% de disponibilidade por mês é quanto tempo fora do ar?

Em um mês de 30 dias, 99,9% permitem cerca de 43 minutos fora do ar; em um ano de 365 dias, cerca de 8 horas e 46 minutos. A conta é sempre o tempo do período multiplicado por (100% menos a meta). A calculadora de SLA do site faz a conta para qualquer meta e período.

Por que o relatório mostra os últimos 12 meses?

Porque no Brasil o SLA de telefonia costuma ser medido no ano. O número de 12 meses é o que decide se a meta foi cumprida; o mês e os últimos 30 dias aparecem para referência. Num contrato com SLA mensal, vale o número do mês, que também está no relatório.

Quem recebe o relatório?

As pessoas que a sua empresa escolher, por e-mail, cada uma no seu idioma, em português ou em inglês. Um gestor de filial pode receber só o relatório da sua parte da empresa, de modo que cada área veja os próprios circuitos, sem expor os números das outras.

Uma falha do monitoramento entra na conta?

Não. Um período em que a 2N5 não conseguiu testar o circuito por um problema do lado da 2N5 fica fora da conta e aparece separado. A cegueira do monitoramento nunca vira indisponibilidade do seu circuito, e um número de SLA honesto não mistura as duas coisas.

CIRCUITOS DE DADOS

Monitoramento do link de internet de cada filial e local

O Monitor da 2N5 faz o monitoramento do link de internet de cada filial com um pequeno agente que a 2N5 instala no local. Ele responde a primeira pergunta de toda queda, se foi a voz ou a conexão, medindo latência, perda de pacotes, jitter e velocidade, e avisa a equipe quando o link cai.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

Como saber se a queda foi do link de internet ou da linha de voz?

Medindo os dois. No Monitor, o **circuito de dados** de cada local, o link de internet dedicado ou banda larga, é acompanhado por um agente instalado ali mesmo, ao lado das chamadas de teste dos circuitos de voz. É o monitoramento do link de internet de cada filial, ligado ao que a voz sente. O guia de chamadas falhando mostra como separar uma causa da outra.

Cada circuito de voz pode ser ligado ao link do seu local. Com a opção de esperar pelo link, os alertas desse circuito aguardam enquanto o link estiver com uma queda aberta: a sua equipe recebe um alerta sobre o link, e não um por circuito de voz que passa por ele.

O que o agente mede?

Medida	Para que serve
Latência	Mostra atraso na rota até a internet
Perda de pacotes	Explica áudio picotado e chamadas que caem
Jitter	Variação do atraso, que estraga a voz antes de derrubar a chamada
Tempo de DNS	Mostra quando os nomes não resolvem, mesmo com a rede no ar
Velocidade	A velocidade real, para comparar com o contratado

As medições ficam em gráficos das últimas 100 horas na página de cada circuito de dados, e uma queda confirmada do link abre um incidente e sobe a mesma escada de escalonamento dos circuitos de voz. Os termos estão no glossário: jitter e perda de pacotes.

Como o agente é instalado?

A pedido escrito da sua empresa, a 2N5 instala o agente em um computador do local, por acesso remoto. Ele não abre nenhuma porta de entrada: só envia as medições para a 2N5. Quando o local deixa de ser monitorado, o agente é removido pela própria 2N5.

E um local onde não dá para instalar o agente?

A 2N5 testa o link de fora. Ela tenta, a cada intervalo, uma conexão ao endereço público do local, e uma sequência de tentativas sem resposta é tratada como queda do link. É uma verificação mais simples que a do agente: diz se o local responde, sem medir latência, perda ou velocidade.

O que o agente nunca coleta?

Arquivos, navegação, conteúdo do tráfego, nomes de usuários, programas, nomes de redes Wi-Fi e outros aparelhos da rede. Os detalhes estão na Política de Privacidade e em segurança e LGPD.

Como o Monitor se compara a ferramentas de monitoramento de rede?

Veja o comparativo com a Obkio, uma ferramenta de monitoramento sintético de rede por agentes, com a fonte de cada afirmação.

Perguntas frequentes

Como saber se a ligação caiu por causa da operadora ou da minha rede?

Compare os dois lados no mesmo horário: a chamada de teste, feita de fora, e as medições do link do local. Se a chamada de teste falha e o link do local está com perda ou fora do ar, o problema está na conexão do local. Se o link está saudável e a chamada falha, a causa está na rota da operadora de voz. O Monitor da 2N5 mostra os dois lados juntos.

Como monitorar o link de internet de várias filiais?

Instalando um agente em cada local, que mede latência, perda de pacotes, jitter, DNS e velocidade do link e envia as medições para o mesmo painel. No Monitor da 2N5, a 2N5 instala o agente por acesso remoto, com a sua autorização por escrito, e cada gestor vê só a sua parte da empresa. Onde não dá para instalar, a 2N5 testa o link de fora.

O que o agente mede?

Latência, perda de pacotes, jitter, tempo de resposta de DNS e a velocidade real da conexão, além do uso de processador e memória do computador onde ele roda. As medições aparecem em gráficos das últimas 100 horas, e uma queda confirmada do link abre um incidente e sobe a mesma escada de escalonamento dos circuitos de voz.

O agente lê o meu tráfego ou os meus arquivos?

Não. Ele nunca coleta arquivos, navegação, conteúdo do tráfego, nomes de usuários, programas instalados, nomes de redes Wi-Fi ou outros aparelhos da rede. Ele só mede a conexão, não abre nenhuma porta de entrada e envia apenas as medições para a 2N5.

Quem instala o agente?

A 2N5, por acesso remoto, em um computador do local, depois da autorização por escrito da sua empresa. Você não baixa nem configura nada. Quando o local deixa de ser monitorado, a própria 2N5 remove o agente. Se não for possível instalar, a 2N5 usa a verificação de fora, mais simples.

Por quanto tempo as medições ficam guardadas?

Por 13 meses, para que os relatórios anuais fiquem completos, com a comparação entre um mês e outro. Os detalhes do que é guardado, por quanto tempo e como exercer seus direitos estão na página de segurança e LGPD e na Política de Privacidade.

SITES

Monitoramento de sites: fora do ar e alterações no conteúdo

O Monitor da 2N5 acessa o seu site de cinco em cinco minutos e avisa sua equipe quando ele sai do ar. Com uma chave a mais, também compara o conteúdo com uma referência e mostra o site como Conteúdo alterado quando a página muda sem autorização, como num site hackeado, com texto trocado ou um script novo.

Por Equipe 2N5 Atualizado em 21 de outubro de 2026

Como saber se o meu site saiu do ar ou foi alterado?

Verificando duas coisas, a cada intervalo: se o site responde e se a página ainda é a que você aprovou. No Monitor, um **site** é cadastrado só com o endereço. Os servidores da 2N5 o acessam de fora, como um visitante, e uma falha confirmada abre um incidente e sobe a mesma escada de escalonamento dos circuitos de voz.

Como o Monitor sabe que o site saiu do ar?

A cada cinco minutos, por padrão, o Monitor acessa o endereço e espera a página responder. Cada resultado tem um estado.

Resultado	O que o Monitor faz
O site responde normalmente	Registra o tempo de resposta e segue
O site responde devagar, ou o certificado vence em poucos dias	Marca como degradado: um aviso, que não conta como tempo fora do ar
O endereço não existe, a conexão é recusada, a conexão segura falha, o servidor não responde a tempo ou devolve erro	Repete a verificação; falhas seguidas abrem um incidente de queda
O certificado venceu	Conta como queda

O intervalo, o número de repetições e o limite de lentidão são ajustáveis por site. Duas semanas antes de o certificado vencer, os contatos da sua empresa já recebem um aviso.

Se o problema estiver na própria 2N5, por exemplo o verificador sem acesso à internet, o resultado fica como não avaliado: não conta contra o seu site e quem é avisado é a 2N5.

E se o site continuar no ar, mas tiver sido alterado?

É o caso do site hackeado ou alterado sem autorização: a página abre normalmente, mas já não é a sua. Uma verificação de disponibilidade não percebe, porque o servidor responde. Por isso o Monitor oferece, para cada site, a **verificação de conteúdo**: uma só chave, **Verificar também o conteúdo deste site**, ao cadastrar ou editar o site.

Ao ligar a chave, o Monitor lê a página real três vezes e guarda o resultado como **referência**. Não há arquivo para enviar nem regras para escrever: a referência é sempre a página no ar naquele momento, e a verificação segue o mesmo ritmo do teste do site. A cada verificação, ele lê o site de novo e compara:

- **Frases de invasão ou de erro**, de uma lista padrão da 2N5.
- **Texto e estrutura**: quanto do texto mudou e quanto da estrutura da página continua igual, dentro de limites fixos.

- **Scripts inesperados**: um script de um endereço que não estava na referência, um arquivo novo, um código escrito na página que mudou ou um manipulador de eventos novo. O alerta diz “possível injeção de código”.
- **Redirecionamento**: o site passou a terminar em outro endereço.

Uma mudança pequena, dentro do limite, não gera alerta: a referência acompanha a página. Partes que mudam sozinhas, como um relógio ou um contador de visitas, já são ignoradas. Uma página montada inteira por JavaScript não pode ter o conteúdo verificado: ela aparece como ilegível.

O que a sua equipe recebe quando o conteúdo muda?

O site aparece como **Conteúdo alterado**, um estado pior que em operação e melhor que fora do ar, e um incidente próprio, que o Monitor trata como qualquer outro: avisa a primeira camada por e-mail, com um link para confirmar com um toque, sobe de camada se ninguém assumir e avisa os contatos da empresa quando a página volta ao normal. As janelas de manutenção silenciam os alertas durante uma mudança planejada.

Se o site cair ao mesmo tempo, o incidente é um só, o da queda, e a mudança de conteúdo segue como uma linha do registro de observações. Um site lento e uma mudança de conteúdo são dois incidentes. A página do site tem duas seções para o conteúdo, abaixo de Respostas e Certificado: o estado e o que mudou, e as verificações. A página do incidente mostra em que parte do site o texto mudou, o que foi removido e o que foi acrescentado, e quais scripts são novos. A pergunta é uma só: *esta mudança foi feita de propósito?* Se foi, **Esta mudança é esperada** troca a referência e fecha o incidente.

Como o site entra no relatório?

O relatório mensal traz uma página de serviços online com a disponibilidade de cada site, calculada como a dos circuitos de dados: queda é tempo fora do ar, degradado aparece mas não conta, e o tempo em que a 2N5 não pôde verificar sai do cálculo. Mostra também a resposta média.

As alterações de conteúdo têm uma **seção própria**. Elas nunca entram na disponibilidade, porque um site alterado está no ar, e aparecem com o número de incidentes, o tempo em que a página ficou diferente da referência, quantas mudanças foram aceitas e a data da última. O cálculo de disponibilidade segue o conceito de SLA.

Como isso se encaixa com o resto do Monitor?

O site é mais um item da mesma conta, ao lado dos circuitos de voz e dos links de internet: mesmos contatos, mesma escada, mesmas janelas de manutenção, mesmo relatório. Para a caixa de entrada da empresa, veja o monitoramento de e-mail. Como a 2N5 opera o serviço para você, está descrito em Como funciona.

Perguntas frequentes

O que acontece se meu site for alterado?

O site passa a aparecer como Conteúdo alterado e o Monitor abre um incidente de conteúdo, que avisa a primeira camada da sua escada por e-mail. Se ninguém confirmar a tempo, o alerta sobe de camada em camada. O incidente mostra o que mudou na página, em que parte dela e quais scripts apareceram.

Como o Monitor sabe que o site foi hackeado?

Ele não adivinha: compara. A página lida agora é confrontada com a referência guardada, e o Monitor avisa quando o texto ou a estrutura mudam além do limite, aparece uma frase de invasão ou de erro, o site passa a terminar em outro endereço ou surge um script que não estava na referência. Os limites são fixos: não há nada para configurar.

Posso aceitar uma mudança esperada?

Sim. No incidente, o botão “Esta mudança é esperada” faz da página de hoje a nova referência e encerra o incidente, com o seu nome registrado. Não existe fila de aprovação: quem tem acesso decide na hora, e pequenas mudanças dentro do limite são acompanhadas sozinhas.

Uma alteração de conteúdo conta como site fora do ar?

Não. Um site alterado continua no ar, então o incidente de conteúdo nunca entra no cálculo de indisponibilidade. Ele aparece numa seção própria do relatório mensal. Se o site cair enquanto o conteúdo está alterado, há um só incidente, o da queda, e a mudança continua anotada no registro de observações. Assim, uma alteração indevida não piora a disponibilidade apresentada no relatório.

Uma lentidão ou um erro passageiro dispara alerta?

Não. Uma verificação que falha é repetida, e só falhas seguidas abrem um incidente. Um site lento ou com certificado perto de vencer aparece como degradado, um aviso que não conta como tempo fora do ar. Se a falha for da própria 2N5, o resultado fica como não avaliado e não conta contra o seu site.

Como saber se o meu site foi hackeado ou alterado?

Comparando o site com uma referência guardada a cada verificação. O Monitor da 2N5 avisa quando o texto ou a estrutura mudam além do limite, aparece uma frase de invasão ou de erro, o site passa a terminar em outro endereço ou surge um script novo, e abre um incidente de conteúdo. Esse tipo de alteração indevida, a desfiguração do site, é vista mesmo com o site no ar.

Como monitorar se o meu site saiu do ar e receber alerta?

Com verificações automáticas, feitas de fora da empresa em intervalo fixo. O Monitor da 2N5 acessa o site, repete a verificação que falha e só abre um incidente depois de falhas seguidas, para evitar falso alarme. O alerta chega por e-mail à primeira camada da sua escada de contatos e sobe de camada se ninguém confirmar a tempo.

E-MAIL

Monitoramento de e-mail: as mensagens estão chegando?

O Monitor da 2N5 envia um e-mail de teste por hora para uma caixa da sua empresa, confere onde ele caiu e o apaga em seguida. Se a mensagem não chega, cai no spam ou a caixa está enchendo, sua equipe é avisada antes de o cliente reclamar.

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

Como saber se os e-mails da empresa estão chegando?

Enviando um e-mail de verdade e conferindo se ele chegou. No Monitor, uma **verificação de e-mail** usa um endereço de teste da sua empresa, uma caixa que ninguém lê. Por padrão, a cada hora, o remetente da 2N5 envia uma mensagem para ele, o Monitor procura essa mensagem na caixa e registra em quanto tempo ela chegou e em que pasta caiu. Isso responde à pergunta de quem depende de e-mail: *quem escreve para nós consegue nos alcançar?*

Como funciona o teste de ida e volta?

1. **Envio.** O Monitor envia ao endereço de teste uma mensagem simples, sem links, imagens ou rastreadores. O remetente se chama “Monitor da 2N5”, e o assunto fica em português quando o endereço termina em `.br` e em inglês nos demais. A mensagem leva uma identificação própria da rodada em um cabeçalho e na última linha do texto.
2. **Busca.** Cerca de uma vez por minuto, o Monitor procura essa identificação na caixa, inclusive na pasta de spam.
3. **Veredito.** Chegou à caixa de entrada: aprovado. Caiu no spam ou chegou depois do prazo da verificação: degradado. Não apareceu em quinze minutos: o Monitor envia outro teste e, se este também não chegar, abre um incidente.
4. **Limpeza.** A mensagem encontrada vai para a lixeira na hora, junto com qualquer teste anterior que tenha chegado atrasado. Ninguém da empresa vê um teste.

Cada rodada guarda o tempo de entrega e o resultado das verificações de remetente feitas pelo servidor que recebeu (SPF, DKIM e DMARC), para que um resultado de spam possa dizer o porquê.

Que tipos de caixa o Monitor consegue acompanhar?

Tipo de conta	O que o Monitor faz
Conta Google ou Google Workspace	Quem administra a caixa entra uma vez com o Google, por um link de conexão válido por 7 dias, e o Monitor passa a procurar nela a mensagem de teste. Não se pede servidor, porta nem senha
Só envio (SMTP)	Não lê caixa nenhuma: a cada rodada, o próprio servidor de saída da empresa envia um teste desse endereço para uma caixa da 2N5, onde o Monitor o procura, na caixa de entrada ou no spam, e o apaga. Fica fora do ar quando o servidor não responde, não criptografa, recusa o login, se recusa a enviar ou o teste não chega, e degradado quando cai no spam
Caixa de outro provedor, por IMAP	Lê a caixa com login e senha, inclusive a pasta de spam, e também pode conferir se a empresa consegue enviar, como acima, com o mesmo login

Na prática, a 2N5 faz a configuração com você, como no resto do serviço gerenciado. O provedor de e-mail é sempre o que a sua empresa já usa.

O que acontece quando a caixa de e-mail enche?

Quando a caixa informa o espaço usado e o limite, ou você informa o tamanho dela, o Monitor mostra a porcentagem usada e a compara com duas marcas de cada verificação:

- **Marca de aviso**: as pessoas responsáveis são avisadas uma vez a cada vez que a marca é cruzada, e a verificação continua aprovada.
- **Marca de alerta**: a verificação passa a falhar e sobe a escada de escalonamento. O mesmo vale para um teste que volta devolvido por caixa cheia.

Sem um limite conhecido, o Monitor mostra só o tamanho, nunca uma porcentagem inventada. Com a caixa em 100%, quem escreve para o endereço recebe uma devolução, e a tela de aviso lembra que é preciso liberar espaço ou aumentar a cota com o provedor.

Que alertas a sua equipe recebe?

Um e-mail que não chega abre um incidente e dispara os alertas escalonados: e-mail para a primeira camada, com confirmação em um toque, e a subida de camada em camada se ninguém assumir. Quando as mensagens voltam a chegar, os contatos da empresa são avisados de que foi resolvido.

Spam, atraso e caixa quase cheia são avisos. Eles informam os contatos, sem acordar a escada. Uma janela de manutenção silencia a verificação durante um trabalho planejado.

Como o e-mail entra no relatório?

O relatório mensal inclui a verificação de e-mail na página de serviços online: a disponibilidade, calculada como a dos circuitos de dados, a parcela dos testes que chegou à caixa de entrada e o tempo de entrega. Vale o mesmo critério do SLA: queda é tempo fora do ar, aviso aparece mas não conta, e o tempo em que a 2N5 não pôde verificar fica fora do cálculo.

O que o monitoramento de e-mail não faz?

O teste confirma que o e-mail enviado **para** a empresa chega. Ele não mede se as mensagens que a empresa envia caem na caixa de entrada de outras pessoas. Para o site da empresa, veja o monitoramento de sites.

Perguntas frequentes

O e-mail de teste cai na caixa de entrada?

É o que se espera, e o Monitor confere. Se o teste cair no spam ou chegar mais tarde do que o limite da verificação, o resultado fica como degradado, um aviso que não sobe a escada. O teste é escrito como um e-mail comum, sem links nem imagens, e é apagado assim que é encontrado.

O que acontece quando a caixa de e-mail enche?

A verificação lê o espaço usado e compara com duas marcas, de aviso e de alerta. Na marca de aviso, as pessoas são avisadas uma vez e a verificação continua aprovada. Na de alerta, ela passa a falhar e sobe a escada, porque com a caixa cheia quem escreve para a empresa recebe uma devolução.

Alguém da empresa precisa ler os e-mails de teste?

Não. O endereço de teste é uma caixa que ninguém lê, e cada mensagem é movida para a lixeira assim que é encontrada, junto com qualquer teste anterior que tenha chegado atrasado. O texto do teste diz que ele é automático e que não precisa ser respondido.

O Monitor verifica os e-mails que a minha empresa envia?

O teste de ida e volta confirma que o e-mail enviado para a empresa chega. Opcionalmente, o Monitor também confere o envio: ele entra no servidor de saída da empresa e pede que aceite uma mensagem desse endereço, mas para antes de enviar qualquer coisa.

Uma falha da 2N5 conta como e-mail fora do ar?

Não. Se o remetente da 2N5 não consegue enviar o teste, ou a caixa deixa de poder ser lida, o resultado fica como não avaliado: não conta contra a sua empresa e quem é avisado é a 2N5. Assim, a sua equipe só é acordada por problemas que de fato afetam o e-mail da empresa.

Como saber se os e-mails da empresa estão chegando?

Com um teste de ida e volta. O Monitor da 2N5 envia um e-mail de teste por hora para uma caixa da empresa, confere se ele caiu na caixa de entrada ou no spam e o apaga em seguida. Se a mensagem não chega, atrasa ou a caixa está enchendo, a sua equipe é avisada antes de o cliente reclamar.

SEGURANÇA E LGPD

Segurança e LGPD no monitoramento VoIP da 2N5

O monitoramento VoIP do Monitor da 2N5 trata o mínimo de dados pessoais para vigiar circuitos de voz e de dados no Brasil. Esta página resume o que é guardado, por quanto tempo e como é protegido, e a regra principal: a voz de uma pessoa nunca é guardada. O texto completo, que vale como compromisso, está na Política de Privacidade.

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

Quem é responsável pelos dados?

Depende do dado. A 2N5 é a **controladora** dos dados que ela mesma decide tratar: pedidos de demonstração, contas de acesso e registros de acesso e de segurança. Para os dados de monitoramento que um cliente fornece ou que o serviço gera para ele, como contatos de alerta, números chamados, gravações e relatórios, a empresa cliente é a controladora e a 2N5 é a **operadora**, que trata os dados só conforme as instruções do cliente.

O que é guardado, e por quanto tempo?

Dado	Por quanto tempo
Pedido de demonstração	12 meses após o último contato
Registro técnico de cada chamada de teste	O prazo que a 2N5 definir
Áudio guardado (só gravação ou URA)	O prazo que a 2N5 definir, criptografado
Mensagens de alerta enviadas e medições do circuito de dados	13 meses
Registros de acesso (Marco Civil, art. 15)	6 meses
Vereditos, índices de qualidade e incidentes	Durante o contrato

Qual é a regra do áudio das chamadas?

A voz de uma pessoa nunca é guardada. O áudio de uma chamada de teste só fica guardado quando quem atende é a gravação ou a URA que o cliente informou, e apenas para provar que a linha funciona e medir a qualidade. Se qualquer outra coisa atender, inclusive uma pessoa, o áudio é destruído ao fim da chamada e só o resultado fica. Uma chamada que pode ser atendida por uma pessoa toca antes uma mensagem dizendo que é um teste automático.

Como os dados são protegidos?

- Todo o tráfego com o serviço é criptografado.
- O áudio, as gravações, as senhas de serviços conectados e as chaves de assinatura são criptografados um a um, em repouso, com as chaves guardadas separadas dos dados.
- Os dados de cada empresa ficam separados, e cada gestor vê só a parte da empresa que lhe foi atribuída.
- Os administradores da 2N5 entram com verificação em duas etapas; qualquer gestor pode ativá-la, e uma empresa pode exigi-la de todos.
- Tentativas de acesso com erro repetido pausam o acesso, e a troca de senha encerra as outras sessões.

- O acesso administrativo aos servidores é restrito e auditado, e as cópias de segurança diárias são guardadas por 14 dias.

E o agente instalado nos locais?

Ele só é instalado com a autorização por escrito do cliente, não abre nenhuma porta de entrada e mede só a conexão: latência, perda, jitter, DNS e velocidade. Ele nunca coleta arquivos, navegação, conteúdo do tráfego, nomes de usuários ou outros aparelhos da rede.

Como exercer seus direitos?

Escreva ao encarregado da 2N5 em **privacidade@2n5.com.br** ou ligue para **+55 (11) 2050-1096**. A página LGPD explica cada direito e o prazo de resposta, e a Política de Privacidade traz o texto completo.

Onde ler mais?

O guia de monitoramento de troncos SIP, 0800 e URA mostra como as chamadas de teste funcionam, o verbete de monitoramento sintético define o termo, e os comparativos mostram como o Monitor se compara a outras ferramentas.

Perguntas frequentes

O Monitor grava as conversas da minha central?

Não. Ele só faz as próprias chamadas de teste e não escuta as chamadas dos seus clientes nem as conversas da sua central. O áudio de uma chamada de teste só é guardado quando quem atende é a gravação ou a URA informada, e a voz de uma pessoa nunca é guardada.

O monitoramento VoIP precisa de acesso à rede de voz da minha empresa?

Não. O Monitor da 2N5 não entra no PABX, no SBC nem na rede de voz: ele só liga para os números que você indica, de fora, como um cliente. O único software instalado, e só com a sua autorização por escrito, é o pequeno agente de link de internet, que não abre porta de entrada e mede só a conexão.

Onde ficam os dados?

Em prestadores de infraestrutura em nuvem contratados pela 2N5, alguns fora do Brasil, inclusive nos Estados Unidos. As transferências seguem o art. 33 da LGPD, com as cláusulas-padrão contratuais aprovadas pela ANPD. Os dados de cada empresa ficam separados dos de outras, e cada gestor vê só a parte que lhe foi atribuída.

O site do Monitor usa cookies de rastreamento?

Não. Este site não grava cookies e não carrega ferramentas de análise ou publicidade. Ele guarda só o tema que você escolher (claro, escuro ou o do computador), neste navegador, para que o site e o produto abram no mesmo tema; essa escolha nunca é enviada à 2N5. O produto guarda só o necessário para funcionar, como manter você conectado.

Como peço os meus dados ou a exclusão deles?

Escrevendo ao encarregado da 2N5 em privacidade@2n5.com.br ou ligando para +55 (11) 2050-1096. A página LGPD explica cada direito, como acesso, correção e exclusão, e em quanto tempo respondemos, e a Política de Privacidade traz o texto completo, com os prazos de guarda de cada dado.

PLANOS

Planos do Monitor da 2N5 para monitorar 0800, URA e troncos SIP, e como contratar

O Monitor da 2N5 tem planos mensais publicados para monitorar 0800, URA e troncos SIP, em reais e com impostos inclusos. Cada plano inclui um número de canais monitorados e de testes diários por canal, e a 2N5 faz a implantação como serviço gerenciado. Escolha um plano abaixo e agende uma demonstração nos seus próprios números.

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

Planos

No site, os cartões de planos desta página mostram o preço mensal de cada plano e o que ele inclui, em reais e com impostos inclusos. Cada plano inclui um número de **canais monitorados** e de **testes diários por canal**. Um canal é um circuito de voz, um circuito de dados, um site ou uma verificação de e-mail.

Se o plano não bastar, há dois adicionais, cobrados por mês:

- **Canal extra:** mais um canal monitorado.
- **Teste diário extra:** mais um teste por dia, cobrado por canal.

O preço mensal é: preço do plano + canais extras × preço do canal extra + testes diários extras × preço do teste diário extra × número de canais (os incluídos mais os extras).

Por exemplo, um plano com 1 canal, mais 2 canais extras e 1 teste diário extra: preço do plano + 2 × canal extra + 1 × teste diário extra × 3 canais.

O plano **Enterprise** é sob consulta, com preço por organização.

O que cada plano inclui, como os canais de alerta, a lista de escalonamento e os relatórios com SLA, está no cartão dele, que vem do próprio cadastro de planos da 2N5. Se o cartão não lista uma coisa, o plano não a inclui.

O que está incluído?

Incluído	Como
Implantação	A 2N5 cadastra cada circuito, comprova com uma chamada real e grava a referência
Chamadas de teste	Da plataforma da 2N5, no ritmo de testes diários do seu plano
Qualidade de voz medida	MOS-LQO de cada chamada, contra a gravação esperada
Alertas	Pelos canais que o cartão do plano lista, com reteste antes de alertar
Evidências	Código SIP e causa Q.850 de cada falha, prontos para a operadora
Relatórios e SLA	Nos planos cujo cartão os lista, todo mês, em português ou inglês
Acesso ao painel	Para os gestores da sua empresa, cada um na sua parte

Como contratar?

1. Escolha um plano e clique no botão do cartão dele.

2. Agende a demonstração: o pedido já chega à 2N5 com o plano escolhido. São três perguntas, cerca de um minuto.
3. A 2N5 mostra o Monitor com os números que você escolheu.
4. Você envia o formulário com os circuitos e os contatos, e a 2N5 faz a implantação.

Quer comparar antes de escolher um plano?

O guia de ferramentas de monitoramento VoIP no Brasil e os comparativos mostram, com a fonte de cada afirmação, em que o Monitor difere de outras ferramentas. O guia de monitoramento de troncos SIP, 0800 e URA explica o que é monitorado, e o verbete SLA define o termo usado nos relatórios.

Perguntas frequentes

Quanto custa monitorar 0800 e troncos SIP?

Depende do plano: os planos mensais estão publicados nesta página, em reais e com impostos inclusos. Cada plano inclui um número de canais monitorados e de testes diários por canal; um canal é um circuito de voz, um circuito de dados, um site ou uma verificação de e-mail. Se precisar de mais, você soma canais extras e testes diários extras. O plano Enterprise é sob consulta, com preço por organização.

Existe teste grátis?

Existe a demonstração: a 2N5 prepara o Monitor com os números que você escolher e mostra como ele trataria uma falha neles, com o código SIP e o alerta que a sua equipe receberia. Como é um serviço gerenciado, não há cadastro para testar sozinho.

A implantação é cobrada à parte?

A implantação é feita pela 2N5, como parte do serviço gerenciado. Você envia o formulário com os circuitos e os contatos; a 2N5 cadastra, verifica cada circuito com uma chamada real, grava a saudação de referência e configura a escada de alertas e os relatórios.

Quem assina o contrato?

A sua empresa, com a 2N5 Tecnologia da Informação e Telecomunicações Ltda., CNPJ 26.593.241/0001-85. As regras de uso estão nos Termos de Uso, e o tratamento de dados, na Política de Privacidade e na página de segurança e LGPD, que explica o que é guardado e por quanto tempo.

Referência

REFERÊNCIA

Códigos SIP: o que cada resposta significa

Um código de resposta SIP é o número de três dígitos que um servidor devolve a uma chamada: 1xx enquanto ela está em andamento, 2xx quando completa, e de 3xx a 6xx quando não completa. Esta é a lista completa do registro da IANA, com a leitura que o Monitor faz de cada um numa chamada de teste.

Como ler um código SIP?

> O primeiro dígito diz a classe: 4xx é uma recusa da requisição (número inexistente, ocupado, credenciais), 5xx é uma falha do servidor que tentou completar a chamada (sobrecarga, rota, manutenção) e 6xx é uma recusa definitiva em qualquer destino. A causa Q.850 que costuma vir junto, no cabeçalho Reason, diz o motivo do lado da rede de telefonia.

Na coluna "Leitura numa chamada de teste", Fora do ar quer dizer que a chamada conta como falha do circuito; o o Monitor a repete a cada 2 minutos antes de abrir um incidente. "Depende" quer dizer que a leitura muda com o que deve atender o número, e a página do código explica cada caso. Os códigos 1xx e 2xx não são falhas.

1xx: provisória (a chamada está em andamento)

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 100	Trying	RFC 3261	Não é falha
SIP 180	Ringing	RFC 3261	Não é falha
SIP 181	Call Is Being Forwarded	RFC 3261	Não é falha
SIP 182	Queued	RFC 3261	Não é falha
SIP 183	Session Progress	RFC 3261	Não é falha
SIP 199	Early Dialog Terminated	RFC 6228	Não é falha

2xx: sucesso

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 200	OK	RFC 3261	Não é falha
SIP 202	Accepted (Deprecated)	RFC 6665	Não é falha
SIP 204	No Notification	RFC 5839	Não é falha

3xx: redirecionamento

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 300	Multiple Choices	RFC 3261	Fora do ar
SIP 301	Moved Permanently	RFC 3261	Fora do ar

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 302	Moved Temporarily	RFC 3261	Fora do ar
SIP 305	Use Proxy	RFC 3261	Fora do ar
SIP 380	Alternative Service	RFC 3261	Fora do ar

4xx: falha da requisição

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 400	Bad Request	RFC 3261	Fora do ar
SIP 401	Unauthorized	RFC 3261	Sem visibilidade
SIP 402	Payment Required	RFC 3261	Fora do ar
SIP 403	Forbidden	RFC 3261	Fora do ar
SIP 404	Not Found	RFC 3261	Fora do ar
SIP 405	Method Not Allowed	RFC 3261	Fora do ar
SIP 406	Not Acceptable	RFC 3261	Fora do ar
SIP 407	Proxy Authentication Required	RFC 3261	Sem visibilidade
SIP 408	Request Timeout	RFC 3261	Fora do ar
SIP 410	Gone	RFC 3261	Fora do ar
SIP 412	Conditional Request Failed	RFC 3903	Fora do ar
SIP 413	Request Entity Too Large	RFC 3261	Fora do ar
SIP 414	Request-URI Too Long	RFC 3261	Fora do ar
SIP 415	Unsupported Media Type	RFC 3261	Fora do ar
SIP 416	Unsupported URI Scheme	RFC 3261	Fora do ar
SIP 417	Unknown Resource-Priority	RFC 4412	Fora do ar
SIP 420	Bad Extension	RFC 3261	Fora do ar
SIP 421	Extension Required	RFC 3261	Fora do ar
SIP 422	Session Interval Too Small	RFC 4028	Fora do ar
SIP 423	Interval Too Brief	RFC 3261	Fora do ar
SIP 424	Bad Location Information	RFC 6442	Fora do ar
SIP 425	Bad Alert Message	RFC 8876	Fora do ar
SIP 428	Use Identity Header	RFC 8224	Fora do ar
SIP 429	Provide Referrer Identity	RFC 3892	Fora do ar
SIP 430	Flow Failed	RFC 5626	Fora do ar
SIP 433	Anonymity Disallowed	RFC 5079	Fora do ar
SIP 436	Bad Identity Info	RFC 8224	Fora do ar
SIP 437	Unsupported Credential	RFC 8224	Fora do ar
SIP 438	Invalid Identity Header	RFC 8224	Fora do ar
SIP 439	First Hop Lacks Outbound Support	RFC 5626	Fora do ar
SIP 440	Max-Breadth Exceeded	RFC 5393	Fora do ar

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 469	Bad Info Package	RFC 6086	Fora do ar
SIP 470	Consent Needed	RFC 5360	Fora do ar
SIP 480	Temporarily Unavailable	RFC 3261	Depende do circuito
SIP 481	Call/Transaction Does Not Exist	RFC 3261	Fora do ar
SIP 482	Loop Detected	RFC 3261	Fora do ar
SIP 483	Too Many Hops	RFC 3261	Fora do ar
SIP 484	Address Incomplete	RFC 3261	Fora do ar
SIP 485	Ambiguous	RFC 3261	Fora do ar
SIP 486	Busy Here	RFC 3261	Depende do circuito
SIP 487	Request Terminated	RFC 3261	Depende do circuito
SIP 488	Not Acceptable Here	RFC 3261	Fora do ar
SIP 489	Bad Event	RFC 6665	Fora do ar
SIP 491	Request Pending	RFC 3261	Fora do ar
SIP 493	Undecipherable	RFC 3261	Fora do ar
SIP 494	Security Agreement Required	RFC 3329	Fora do ar

5xx: falha do servidor

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 500	Server Internal Error	RFC 3261	Fora do ar
SIP 501	Not Implemented	RFC 3261	Fora do ar
SIP 502	Bad Gateway	RFC 3261	Fora do ar
SIP 503	Service Unavailable	RFC 3261	Fora do ar
SIP 504	Server Time-out	RFC 3261	Fora do ar
SIP 505	Version Not Supported	RFC 3261	Fora do ar
SIP 513	Message Too Large	RFC 3261	Fora do ar
SIP 555	Push Notification Service Not Supported	RFC 8599	Fora do ar
SIP 580	Precondition Failure	RFC 3312	Fora do ar

6xx: falha global

Código	Nome oficial	Definido em	Leitura numa chamada de teste
SIP 600	Busy Everywhere	RFC 3261	Depende do circuito
SIP 603	Decline	RFC 3261	Depende do circuito
SIP 604	Does Not Exist Anywhere	RFC 3261	Fora do ar
SIP 606	Not Acceptable	RFC 3261	Fora do ar
SIP 607	Unwanted	RFC 8197	Fora do ar
SIP 608	Rejected	RFC 8688	Fora do ar

Fontes: registro de códigos de resposta SIP da IANA e RFC 3261, consultados em 7 de outubro de 2026. Veja também a lista de causas Q.850 e a consulta de código SIP.

CÓDIGOS SIP

SIP 180 Ringing: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 180 Ringing é uma resposta provisória: o destino recebeu o INVITE e está alertando o usuário, ou seja, o telefone está tocando. Não é falha. O problema aparece quando o 180 se repete e nada vem depois. Nesse caso, verifique se a chamada termina em 200 OK, 480 ou 487.

SIP 180 na referência

Código	180
Nome oficial	Ringing
Classe	1xx: provisória (a chamada está em andamento)
Definido em	RFC 3261

Como o Monitor trata o SIP 180

O SIP 180 sozinho não é falha: a chamada ainda está em andamento. O que conta é como ela termina. A tabela mostra a leitura de uma chamada de teste que toca até o teste parar de esperar, para cada tipo de circuito, conforme o que deve atender o número.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Em operação

Para "Outro": Com "Contar ringback como alcançável" desmarcado: Fora do ar.

O que o Monitor registra para uma URA: “O número tocou e nada atendeu, mas este circuito deveria atender todas as chamadas sozinho.”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

O que significa o SIP 180 na prática?

O SIP 180 Ringing é a resposta provisória que diz “o destino está tocando”. Pela RFC 3261, o agente que recebeu o INVITE está tentando alertar o usuário, e o lado que ligou pode usar esse aviso para gerar o tom de chamada localmente. O 180 cria um diálogo provisório (early dialog), mas não encerra nada: a chamada ainda espera uma resposta final, que pode ser 200 OK (atendeu), um erro 4xx, 5xx ou 6xx, ou um CANCEL de quem ligou.

Por isso o 180, sozinho, não é um diagnóstico. Ele diz que a sinalização chegou até alguém capaz de tocar. O que importa para quem monitora um tronco ou um 0800 é o que acontece depois do 180: se o destino atende, em quanto tempo, e se a chamada não fica tocando indefinidamente sem que ninguém, nem a URA, atenda.

Causas comuns no Brasil

- Ramal ou telefone IP tocando normalmente num PABX Asterisk, Issabel, FreePBX, 3CX ou Intelbras: comportamento esperado.
- 0800 ou URA que deveria atender na hora, mas fica tocando porque o servidor da URA travou e o PABX segue alertando um destino que não responde.
- Fila de atendimento sem agentes logados, configurada para tocar até alguém entrar, em vez de rejeitar ou mandar para uma mensagem.
- Regra de horário errada no PABX, que manda as chamadas de fora do expediente para um grupo de ramais que ninguém atende.
- Interconexão com a rede de telefonia em que a operadora repassa o alerta do destino (celular ou fixo) como 180.
- Tom de chamada ausente para quem liga, porque o 180 chegou sem SDP e o equipamento de origem não gera o tom localmente.

Como diagnosticar

1. Capture a sinalização com `sngrep` (por exemplo, `sngrep port 5060`) e confira a sequência: INVITE, 100 Trying, 180 Ringing e qual resposta final chega depois.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e repita a chamada. Veja se o 180 traz corpo SDP ou não.
3. Use `core show channels` durante a chamada para ver em que ramal, fila ou aplicação o canal está parado enquanto toca.
4. No 3CX, ative o “Verbose logging” e leia o log de atividade da chamada para ver para qual ramal ou fila ela foi entregue.
5. Meça o tempo entre o 180 e a resposta final. Se a chamada termina em 487 Request Terminated, foi o lado que ligou que desistiu. Se termina em 480, foi o destino que encerrou.
6. Se o 180 se repete muitas vezes, verifique se o destino usa respostas provisórias confiáveis (`Require: 100rel` e PRACK, RFC 3262) e se os PRACK estão chegando.

O que mandar para a operadora

- Data e hora de cada tentativa, com fuso horário (por exemplo, horário de Brasília, UTC-3).
- Número de origem (A) e número chamado (B), no formato exato enviado no INVITE.
- Call-ID de pelo menos uma chamada afetada.
- A sequência completa de respostas: quantos 180, se veio 183, e a linha da resposta final (por exemplo, `SIP/2.0 480 Temporarily Unavailable`).
- Header Reason, se houver, com a causa Q.850 (`Reason: Q.850;cause=19`).
- O trace em pcap gerado pelo `sngrep` ou `tcpdump`, quando disponível.

Perguntas frequentes

Por que recebo 180 Ringing mas não ouço o tom de chamada?

Quando o 180 chega sem SDP, quem gera o tom de chamada é o seu lado, localmente. Se o PABX ou o telefone não geram esse tom, a chamada fica em silêncio até ser atendida. Se o destino envia áudio próprio, o normal é usar 183 Session Progress com SDP. Confira a configuração de ringback do tronco e do ramal.

Uma chamada que toca e ninguém atende é um problema?

Depende do destino. Um ramal pessoal pode simplesmente não atender. Já um 0800 ou uma URA deveriam atender sempre. Se o 180 se repete e a chamada termina em 480 Temporarily Unavailable ou é cancelada pelo lado que ligou (487), o atendimento automático parou de funcionar, ou a fila está sem posições livres.

Uma chamada de teste real percebe quando o 0800 só toca?

Sim. A chamada de teste é uma chamada real, então ela vê a sequência de respostas SIP até a resposta final, e não só o primeiro 180. Um 180 sozinho não define o resultado. Quando o teste falha, ele é repetido antes de qualquer alerta, para separar um problema real de uma oscilação passageira.

CÓDIGOS SIP

SIP 183 Session Progress: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 183 Session Progress é uma resposta provisória que informa o andamento da chamada antes do atendimento. Na prática, quase sempre traz SDP e abre áudio antecipado (early media): tom de chamada, música ou um aviso gravado. Não é falha. Ouça o que esse áudio diz e confira qual resposta final chega depois.

SIP 183 na referência

Código	183
Nome oficial	Session Progress
Classe	1xx: provisória (a chamada está em andamento)
Definido em	RFC 3261

Como o Monitor trata o SIP 183

O SIP 183 sozinho não é falha: a chamada ainda está em andamento. O que conta é como ela termina. A tabela mostra a leitura de uma chamada de teste que ouve uma mensagem antes de ser atendida, para cada tipo de circuito, conforme o que deve atender o número.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “O número nunca tocou e nada atendeu, mas este circuito deveria atender todas as chamadas sozinho.”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

O que significa o SIP 183 na prática?

Pela RFC 3261, o SIP 183 Session Progress serve para informar o andamento da chamada quando nenhuma outra resposta provisória se aplica. Na prática, ele quase sempre carrega um SDP e abre o caminho de áudio antes do atendimento, o chamado early media (RFC 3960). Assim, quem liga ouve o que o destino quer mostrar antes do 200 OK: o tom de chamada gerado pela rede, uma música, um aviso de gravação ou uma mensagem da operadora.

É aqui que mora o risco para quem monitora. Um 0800 que toca mensagem antes de atender é normal, mas a mesma técnica é usada pela rede para anunciar que o número não existe, que o assinante está fora de área ou que a rota está congestionada. A chamada “fala” sem ter sido atendida, e só a resposta final e o conteúdo do áudio dizem se deu certo.

Causas comuns no Brasil

- 0800 ou URA que toca um aviso antes do atendimento, como “esta ligação pode ser gravada”, enviado como early media.
- Rede da operadora (Vivo, Claro, Algar, Embratel ou outras) gerando o tom de chamada como áudio, em vez de deixar o seu lado gerar localmente.
- Mensagem gravada da rede informando número inexistente, telefone desligado ou fora da área de cobertura, tocada antes de uma resposta final de erro.
- Gateway de interconexão com a telefonia convencional que traduz o andamento da chamada em 183 com áudio.
- PABX Asterisk, Issabel ou FreePBX usando `Progress()` ou `Playback(...,noanswer)` no plano de discagem para tocar áudio sem atender.
- 3CX ou Intelbras repassando o early media da operadora para o ramal que originou a chamada.

Como diagnosticar

1. Capture a chamada com `sngrep port 5060` e abra o 183: veja se ele traz corpo `application/sdp` e para qual IP e porta o áudio vai.
2. No Asterisk, Issabel ou FreePBX, use `pjsip set logger on` (ou `sip set debug on` no chan_sip) para ver o 183 completo e a resposta final que vem depois.
3. Grave ou escute o áudio antecipado. No `sngrep`, a tela de fluxo de RTP ajuda a confirmar se há pacotes de áudio chegando antes do 200 OK.
4. Confira se o 183 exige confirmação (`Require: 100rel`). Nesse caso, o seu lado precisa responder com PRACK (RFC 3262), senão o destino pode reenviar o 183 e encerrar a tentativa.
5. Se o áudio é de erro, procure na resposta final o header `Reason: Q.850;cause=...` (RFC 6432) para ver a causa exata.
6. Se não há áudio, verifique NAT e firewall: o SDP do 183 pode apontar para um IP privado ou para portas RTP bloqueadas.

O que mandar para a operadora

- Data e hora das chamadas, com fuso horário.
- Número de origem (A) e número chamado (B), como aparecem no INVITE.
- Call-ID de uma chamada afetada e o SDP recebido no 183.
- O que se ouviu no áudio antecipado (texto do aviso ou trecho gravado).
- A linha da resposta final e o header Reason com a causa Q.850, se houver.
- O pcap da chamada, incluindo o RTP, quando disponível.

Perguntas frequentes

Por que o 0800 toca uma mensagem antes de atender?

Porque o destino ou a operadora enviou 183 Session Progress com SDP e começou a mandar áudio antes do 200 OK. É assim que funcionam avisos como "sua ligação pode ser gravada" ou músicas de espera antes do atendimento. Enquanto não chega o 200 OK, a chamada não foi atendida do ponto de vista do SIP, mesmo que você já esteja ouvindo algo.

Ouvir áudio no 183 significa que a chamada completou?

Não. O áudio antecipado pode ser exatamente o aviso de que a chamada não vai completar, como "o número chamado não existe" ou "este telefone está desligado". Uma verificação que só escuta se há som pode marcar como funcionando um 0800 que, na verdade, está tocando uma mensagem de erro da rede. É preciso olhar a resposta final e o conteúdo do áudio.

Uma chamada de teste real enxerga o que acontece depois do 183?

Sim. Por ser uma chamada real, ela acompanha a chamada até a resposta SIP final, em vez de parar no 183. O 183 sozinho não define o resultado. A chamada também avalia o áudio nos dois sentidos e a qualidade de voz medida (MOS-LQO), e uma falha é repetida antes de qualquer alerta.

CÓDIGOS SIP

SIP 400 Bad Request: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 400 Bad Request significa que o servidor recebeu a mensagem SIP mas não conseguiu interpretá-la, por erro de sintaxe. A causa mais comum é um header malformado, muitas vezes alterado por um SIP ALG no roteador. Leia a frase de motivo da resposta, que deveria indicar o problema, e compare o INVITE com o que a operadora espera.

SIP 400 na referência

Código	400
Nome oficial	Bad Request
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	41 (Temporary failure)

Como o Monitor trata o SIP 400

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora recusou a chamada (SIP 400).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 400 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 400 na prática?

Pela RFC 3261, o SIP 400 Bad Request indica que a requisição não pôde ser entendida por causa de sintaxe malformada. A própria RFC recomenda que a frase de motivo detalhe o problema, por exemplo “Missing Call-ID header field”. Na prática, muitos servidores respondem só “Bad Request”, e o diagnóstico depende de comparar a mensagem enviada com o que o servidor espera.

É uma falha final: a chamada não acontece, e repetir a mesma mensagem dá o mesmo resultado. Num tronco que funcionava, um 400 que surge de repente costuma vir de uma mudança no caminho, como um roteador novo, uma atualização do PABX ou uma regra nova no SBC da operadora. Ver o erro 400 SIP em todas as chamadas aponta para configuração; em só algumas, para números ou headers específicos.

Causas comuns no Brasil

- SIP ALG ativo em roteador de provedor de internet, reescrevendo headers e o SDP de forma inválida.
- Request-URI com caracteres que a operadora não aceita, como espaços, hífens ou um `+` onde ela espera só dígitos.
- Nome de exibição (Caller ID) com acentos ou aspas mal codificados, gerado pelo cadastro do ramal no Asterisk, Issabel ou FreePBX.
- Header obrigatório ausente ou duplicado depois de uma customização no PABX ou de uma regra de manipulação no SBC.
- SDP inconsistente, por exemplo com IP vazio ou linhas fora da ordem esperada, depois de uma mudança de NAT.
- Atualização de versão do 3CX, Intelbras ou Asterisk que mudou o formato de algum header enviado ao tronco.

Como diagnosticar

1. Capture com `sngrep port 5060` e leia a resposta inteira: a frase de motivo e o header `Warning`, se houver, costumam dizer o que está errado.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e compare, linha a linha, o INVITE recusado com um INVITE que funciona.
3. Faça a mesma captura no PABX e na borda da rede. Se a mensagem muda entre os dois pontos, há um equipamento alterando o SIP. Desative o SIP ALG do roteador.
4. Teste com um número de destino simples, só com dígitos, e com o nome de exibição sem acentos, para isolar o campo problemático.
5. No 3CX, ative o “Verbose logging” e procure a resposta 400 no log de atividade, junto com o INVITE que a provocou.
6. Se o 400 aparece no REGISTER, antes de qualquer chamada, revise usuário, domínio e porta configurados no tronco.

O que mandar para a operadora

- Data e hora com fuso horário de algumas tentativas recusadas.
- Número de origem (A) e número chamado (B), no formato enviado.
- Call-ID e a mensagem completa que recebeu o 400 (INVITE ou REGISTER).
- A linha completa da resposta, com frase de motivo e header Warning.
- Quantas tentativas falharam e se todas as chamadas são afetadas ou só algumas.
- O pcap da captura, quando disponível.

Perguntas frequentes

O SIP 400 é problema meu ou da operadora?

Quase sempre a mensagem que saiu do seu lado chegou fora do padrão, seja por configuração do PABX, seja por um equipamento no caminho que a alterou. Mas há casos em que o servidor da operadora é mais rígido que a RFC 3261 e recusa algo válido. Compare a mensagem capturada na saída do PABX com a que chega ao servidor.

Que causa Q.850 aparece quando o 400 passa para a rede de telefonia?

Pela RFC 3398, um gateway que converte SIP para ISUP traduz o 400 Bad Request na Q.850 cause 41 (Temporary failure). Por isso, do lado da telefonia convencional, um 400 pode aparecer como falha temporária, embora a origem seja uma mensagem SIP malformada. Nenhuma causa Q.850 é convertida em 400 no sentido inverso.

CÓDIGOS SIP

SIP 401 Unauthorized: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 401 Unauthorized é o desafio de autenticação do registrar ou do servidor: ele pede que a requisição seja reenviada com credenciais digest. Uma vez é normal no REGISTER e no INVITE. Se o 401 volta depois do reenvio, o usuário, a senha ou o realm estão errados. Confira as credenciais do tronco com a operadora.

SIP 401 na referência

Código	401
Nome oficial	Unauthorized
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	21 (Call rejected)

Como o Monitor trata o SIP 401

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	**Sem visibilidade**
Um tom de teste ou serviço de eco	**Sem visibilidade**
Outro: pode tocar ou ser atendido	**Sem visibilidade**

Sem visibilidade quer dizer que a falha está do lado da 2N5, não no seu circuito: o teste não conta contra o circuito, não entra no SLA e não avisa o cliente. A 2N5 é avisada se durar.

O que o Monitor registra para uma URA: “A operadora não aceitou a conta de chamadas da 2N5, geralmente por usuário ou senha errados, então nenhuma chamada de teste chegou ao circuito. É um problema de configuração do lado da 2N5, não uma queda deste circuito (SIP 401).”

Se a operadora devolve o SIP 401 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 401 na prática?

Pela RFC 3261, o SIP 401 Unauthorized indica que a requisição exige autenticação do usuário. Ele é enviado por registrars e por agentes que recebem a chamada, e traz o header `WWW-Authenticate` com o desafio digest: realm, nonce e o algoritmo. O cliente calcula a resposta com usuário e senha e reenvia a requisição com o header `Authorization`.

Por isso, ver um 401 isolado é rotina: muitos troncos desafiam todo REGISTER e todo INVITE. O sinal de problema é o ciclo REGISTER, 401, REGISTER com credenciais e outro 401. Se o desafio repetido traz `stale=true`, o nonce apenas expirou e o cliente deve tentar de novo com o novo nonce. Sem `stale`, as credenciais foram recusadas, e é esse erro 401 SIP repetido que impede o registro do tronco. Para proxies, o equivalente é o SIP 407.

Causas comuns no Brasil

- Senha do tronco trocada no portal da operadora e não atualizada no Asterisk, Issabel, FreePBX ou 3CX.
- Usuário de autenticação diferente do número do tronco: muitas operadoras usam um login de autenticação separado do usuário que vai no From.
- Realm ou domínio configurado errado, fazendo o PABX responder ao desafio com dados de outro servidor.
- Tronco contratado para autenticação por IP, mas o PABX passou a sair por outro IP público, e a operadora volta a pedir credenciais.
- Dois PABX registrando com as mesmas credenciais, um derrubando o registro do outro.
- Caracteres especiais na senha que o painel do PABX salva ou escapa de forma diferente.

Como diagnosticar

1. No Asterisk ou FreePBX com PJSIP, rode `pjsip show registrations` e veja se o tronco está `Registered` ou `Rejected`. No chan_sip (comum no Issabel), use `sip show registry`.
2. Ative `pjsip set logger on` (ou `sip set debug on`) e confirme se há um segundo 401 depois do envio com `Authorization`.
3. Compare o realm do header `WWW-Authenticate` com o configurado no tronco e confira o usuário enviado no campo `username` do `Authorization`.
4. No FreePBX, revise os campos de autenticação do tronco PJSIP (usuário, senha e servidor). No 3CX, confira “Authentication ID” e senha, e ative o “Verbose logging”.
5. Use `sngrep port 5060` para ver a escada completa e garantir que o reenvio sai pelo mesmo IP e porta da primeira tentativa.
6. Se o tronco é por IP, confirme com `curl ifconfig.me` qual IP público o servidor está usando.

O que mandar para a operadora

- Data e hora com fuso horário das tentativas de registro ou de chamada.
- Número ou identificador do tronco e o usuário de autenticação usado.
- Call-ID de um REGISTER ou INVITE recusado.
- As duas respostas 401, com o header `WWW-Authenticate` completo, mostrando o realm.
- O IP público de origem e quantas tentativas falharam.
- O pcap da captura, quando disponível, sem expor a senha em texto.

Perguntas frequentes

Ver 401 no log do Asterisk significa que o tronco está com problema?

Não necessariamente. O fluxo normal de autenticação é: REGISTER ou INVITE sem credenciais, 401 com o header WWW-Authenticate, reenvio com o header Authorization e, então, 200 OK. O problema é quando o segundo envio, já com credenciais, também recebe 401. Isso indica credenciais recusadas, e não apenas o desafio.

Qual a diferença entre 401 e 403 num tronco SIP?

O 401 diz "preciso saber quem você é" e oferece um desafio para autenticar. O 403 Forbidden diz "sei o que você pediu e não vou atender", e autenticar de novo não resolve. Se você vê 401 seguido de 403, a autenticação passou, mas a operadora recusou a chamada por outro motivo, como o número de

origem.

CÓDIGOS SIP

SIP 403 Forbidden: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 403 Forbidden significa que o servidor entendeu a requisição e se recusou a atendê-la, e autenticar de novo não resolve. Em troncos no Brasil, a causa mais comum é a operadora não reconhecer o número de origem enviado. Confira o número no From e no P-Asserted-Identity e confirme com a operadora quais números o tronco pode usar.

SIP 403 na referência

Código	403
Nome oficial	Forbidden
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	21 (Call rejected), 55 (Incoming calls barred within CUG), 57 (Bearer capability not authorized), 87 (User not member of CUG)

Como o Monitor trata o SIP 403

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora recusou esta chamada. A causa mais comum é a operadora não reconhecer o número de onde a chamada vem; também pode significar que este número está bloqueado ou suspenso, ou que a conta está sem crédito (SIP 403).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 403 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 403 na prática?

Pela RFC 3261, o SIP 403 Forbidden indica que o servidor entendeu a requisição, mas se recusa a atendê-la. A autorização não vai ajudar e a requisição não deveria ser repetida. É diferente do SIP 401: no 401 o servidor ainda não sabe quem você é; no 403 ele sabe e decidiu negar.

Em troncos SIP no Brasil, o 403 é um dos códigos mais frequentes quando “o tronco registra, mas não liga”. A operadora aceitou o registro ou o IP, mas uma regra de negócio barrou aquela chamada: o número de origem, o destino, o estado da conta ou o endereço de onde a chamada veio. A frase de motivo e o header `Warning` às vezes dizem qual regra foi aplicada, e vale ler os dois antes de abrir chamado sobre o erro 403 SIP.

Causas comuns no Brasil

- Número de origem (identificação do chamador) que não pertence ao tronco, enviado no From ou no P-Asserted-Identity por um ramal ou uma regra do PABX.
- Número de origem em formato diferente do esperado pela operadora, por exemplo com ou sem DDD, com `0` à frente ou em E.164 (`+55...`).
- Linha ou tronco bloqueado ou suspenso, por exemplo por falta de pagamento ou por um bloqueio administrativo.
- Plano pré-pago ou com franquia sem crédito disponível para aquele tipo de chamada.
- Destino bloqueado no contrato: celular, longa distância, internacional ou números de tarifação especial.
- IP de origem não autorizado num tronco por IP, depois de uma troca de link de internet ou de uma migração do Asterisk, Issabel, FreePBX ou 3CX.

Como diagnosticar

1. Capture com `sngrep port 5060` e anote a frase de motivo do 403, o header `Warning` e o `Reason: Q.850;cause=21`, se houver (Q.850 cause 21, chamada rejeitada).
2. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e confira os headers From, P-Asserted-Identity e Remote-Party-ID do INVITE.
3. Ligue para o mesmo destino usando o número principal do tronco como origem. Se funciona, o problema é o número de origem do ramal ou da rota.
4. Ligue para destinos de tipos diferentes (fixo local, celular, longa distância) para ver se o bloqueio é por tipo de destino.
5. No 3CX, ative o “Verbose logging” e revise o campo de identificação de saída configurado no tronco e na regra de saída.
6. Confirme no portal ou com o financeiro da operadora se a conta está ativa e com crédito.

O que mandar para a operadora

- Data e hora com fuso horário de algumas tentativas recusadas.
- Número de origem (A) e número chamado (B), exatamente como saíram no INVITE.
- Call-ID de pelo menos uma chamada recusada.
- A linha completa da resposta, com frase de motivo, header Warning e Reason com a causa Q.850.
- O IP público de onde as chamadas saem e quantas tentativas falharam.
- O pcap da captura, quando disponível.

Perguntas frequentes

Por que recebo 403 só em algumas chamadas?

Quando o 403 aparece só para certos destinos, a operadora costuma estar bloqueando aquele tipo de chamada no seu contrato, como celular, longa distância, internacional ou números de tarifação especial. Quando aparece só para certos ramais, o problema geralmente é o número de origem que esses ramais enviam, que não pertence ao tronco.

Qual causa Q.850 acompanha o 403?

Pela RFC 3398, a Q.850 cause 21 (Call rejected) é a mais comum, e o 403 é traduzido de volta como cause 21. Também são convertidas em 403 as causas 55 e 87, ligadas a grupos fechados de usuários, e a 57, capacidade de portadora não autorizada. Na prática, a cause 21 é a que você mais vai ver.

CÓDIGOS SIP

SIP 404 Not Found: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 404 Not Found significa que o servidor tem informação definitiva de que o usuário ou número não existe no domínio chamado. A causa mais comum em troncos é o formato do número: falta de DDD, prefixo errado ou E.164 onde a operadora espera outro formato. Compare o número enviado no INVITE com o formato aceito pela operadora.

SIP 404 na referência

Código	404
Nome oficial	Not Found
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	1 (Unallocated (unassigned) number), 2 (No route to specified transit network (national use)), 3 (No route to destination), 26 (Non-selected user clearing)

Como o Monitor trata o SIP 404

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “O número não existe ou foi discado errado, então a operadora não completou a chamada (SIP 404).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 404 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 404 na prática?

Pela RFC 3261, o SIP 404 Not Found indica que o servidor tem informação definitiva de que o usuário não existe no domínio informado na Request-URI. O mesmo código é usado quando o domínio da Request-URI não corresponde a nenhum domínio atendido por quem recebeu a requisição.

Num tronco, o erro 404 SIP quase sempre se resume a “esse número não existe aqui”. Às vezes o número realmente não está alocado, e a rede costuma responder com a Q.850 cause 1. Com frequência, porém, o número existe e foi enviado no formato errado, ou chegou ao PABX de destino, que não tem rota para ele. Quando a chamada entra no seu próprio PABX e recebe 404, o DID não está configurado nas rotas de entrada. Se o número existia e foi desativado, o código mais preciso seria o SIP 410; se faltam dígitos, o SIP 484.

Causas comuns no Brasil

- Número enviado num formato que a operadora não aceita: sem DDD, com `0` a mais, com código de prestadora (CSP) onde não deveria, ou E.164 (`+55`) onde ela espera só dígitos.
- Celular discado sem o nono dígito, ou fixo discado com um dígito a mais.
- 0800 enviado incompleto ou com DDD na frente.
- Número de destino que não está alocado ou foi desativado.
- Número portado roteado para a operadora antiga (a RFC 3398 mapeia a cause 26 para 404 nesse caso).
- DID de entrada sem rota no Asterisk, Issabel, FreePBX ou 3CX: o PABX responde 404 porque não encontra o ramal no contexto.

Como diagnosticar

1. Capture com `sngrep port 5060` e veja a Request-URI do INVITE: é ali que está o número exatamente como saiu.
2. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip). Em chamadas de entrada, o log mostra a extensão não encontrada no contexto. Confira com `dialplan show <número>@<contexto>`.
3. Revise as regras de saída (dial patterns) do FreePBX ou do 3CX: um prefixo removido ou adicionado a mais muda o número enviado.
4. Teste o mesmo destino em formatos diferentes, por exemplo `11987654321` e `5511987654321`, para descobrir o que a operadora aceita.
5. Procure o header `Reason: Q.850;cause=1` (RFC 6432) ou outra causa na resposta: ele diferencia número não alocado de falta de rota (cause 3).
6. Ligue para o mesmo número a partir de outra linha. Se também não completa, o número de fato não existe.

O que mandar para a operadora

- Data e hora com fuso horário das tentativas.
- Número de origem (A) e número chamado (B), exatamente como estavam na Request-URI.
- Call-ID de pelo menos uma chamada.
- A linha completa da resposta e o header Reason com a causa Q.850, se houver.
- O formato de discagem que você está usando e quantas tentativas falharam.
- O pcap da captura, quando disponível.

Perguntas frequentes

Em que formato devo enviar o número para a operadora?

Depende da operadora e do contrato. Algumas aceitam DDD mais o número (10 ou 11 dígitos), outras pedem E.164 com ou sem o +55, e outras aceitam a discagem tradicional, com `0`, código da prestadora e DDD. O 0800 tem 11 dígitos, como 0800 123 4567. Peça o formato oficial por escrito e ajuste a regra de saída do PABX.

Qual a diferença entre 404, 410 e 484?

O 404 diz que o número não existe naquele destino. O 410 Gone diz que ele existia e não está mais em serviço, de forma permanente. O 484 Address Incomplete diz que faltam dígitos. Na prática, muitas operadoras usam 404 para os três casos, então vale conferir também a causa Q.850 que vem junto.

CÓDIGOS SIP

SIP 407 Proxy Authentication Required: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 407 Proxy Authentication Required é o desafio de autenticação de um proxy, normalmente o da operadora, que pede o reenvio do INVITE com credenciais digest. Receber um 407 na primeira tentativa é normal. Se o 407 se repete depois do reenvio, as credenciais ou o realm estão errados. Revise a autenticação do tronco no PABX.

SIP 407 na referência

Código	407
Nome oficial	Proxy Authentication Required
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	21 (Call rejected)

Como o Monitor trata o SIP 407

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Sem visibilidade
Um tom de teste ou serviço de eco	Sem visibilidade
Outro: pode tocar ou ser atendido	Sem visibilidade

Sem visibilidade quer dizer que a falha está do lado da 2N5, não no seu circuito: o teste não conta contra o circuito, não entra no SLA e não avisa o cliente. A 2N5 é avisada se durar.

O que o Monitor registra para uma URA: "A operadora não aceitou a conta de chamadas da 2N5, geralmente por usuário ou senha errados, então nenhuma chamada de teste chegou ao circuito. É um problema de configuração do lado da 2N5, não uma queda deste circuito (SIP 407)."

Se a operadora devolve o SIP 407 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 407 na prática?

Pela RFC 3261, o SIP 407 Proxy Authentication Required é semelhante ao SIP 401, mas indica que o cliente precisa primeiro se autenticar com o proxy. O proxy envia o header `Proxy-Authenticate` com o desafio digest (realm e nonce), e o cliente reenvia a requisição com o header `Proxy-Authorization`.

Em troncos SIP, o fluxo normal de uma chamada é INVITE, 407, ACK, novo INVITE com credenciais e, então, 100 Trying e 180 ou 183. Por isso o 407 aparece em quase todo log de chamada de saída e não indica problema sozinho. O sinal de falha, o verdadeiro erro 407 SIP, é o segundo 407, logo depois do INVITE que já trazia credenciais, ou um PABX que nunca reenvia o INVITE. Se o novo desafio traz `stale=true`, o nonce só expirou e basta tentar de novo.

Causas comuns no Brasil

- Senha ou usuário de autenticação do tronco desatualizados no Asterisk, Issabel, FreePBX ou 3CX.
- Tronco no PABX sem autenticação de saída configurada, de modo que o INVITE nunca é reenviado com credenciais.
- Realm diferente entre o REGISTER e o INVITE, com o PABX usando a credencial errada para o desafio do proxy.
- Usuário no From do INVITE diferente do login de autenticação que a operadora associou ao tronco.
- Tronco por IP que passou a sair por outro IP público, levando o proxy da operadora a exigir credenciais.
- SBC no meio do caminho que remove ou reescreve o header `Proxy-Authorization`.

Como diagnosticar

1. Capture com `sngrep port 5060` e confira se o INVITE é reenviado depois do 407 e se o segundo envio também recebe 407.
2. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e compare o realm do `Proxy-Authenticate` com o do `Proxy-Authorization`.
3. Rode `pjsip show endpoint <tronco>` e confira se o endpoint tem `outbound_auth` apontando para a autenticação certa. No chan_sip, revise `secret`, `defaultuser` e `fromuser`.

4. No 3CX, ative o “Verbose logging” e revise “Authentication ID” e senha do tronco.
5. Teste uma chamada logo depois de reiniciar o registro com `pjsip send register <tronco>`, para descartar nonce vencido.
6. Se houver SBC ou firewall com inspeção SIP, capture antes e depois dele para ver se o header de autenticação chega intacto.

O que mandar para a operadora

- Data e hora com fuso horário das chamadas recusadas.
- Número de origem (A), número chamado (B) e o usuário de autenticação do tronco.
- Call-ID de uma chamada afetada.
- Os dois 407 recebidos, com o header `Proxy-Authenticate` completo (realm e nonce).
- O IP público de onde as chamadas saem e quantas tentativas falharam.
- O pcap da captura, quando disponível, sem expor a senha.

Perguntas frequentes

Qual a diferença entre 401 e 407?

Os dois são desafios de autenticação digest e funcionam do mesmo jeito. O 401 vem de um registrar ou do destino final e usa os headers WWW-Authenticate e Authorization. O 407 vem de um proxy no caminho e usa Proxy-Authenticate e Proxy-Authorization. Em troncos, é comum o REGISTER receber 401 e o INVITE receber 407.

O registro do tronco está OK, mas as chamadas recebem 407. Por quê?

O registro e a chamada podem usar credenciais ou realms diferentes, e alguns PABX só respondem ao desafio do INVITE se o tronco tiver autenticação de saída configurada. Também acontece quando o INVITE sai com um usuário no From diferente do esperado pela operadora. Compare o Proxy-Authorization do INVITE com o Authorization do REGISTER.

CÓDIGOS SIP

SIP 408 Request Timeout: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 408 Request Timeout significa que a requisição não teve resposta a tempo. Ou o servidor não conseguiu localizar o destino a tempo, ou o próprio equipamento de origem desistiu depois de esperar. A causa mais comum é rede: firewall, NAT ou rota até o servidor. Capture o tráfego e veja se o INVITE sai e se alguma resposta volta.

SIP 408 na referência

Código	408
Nome oficial	Request Timeout
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	18 (No user responding), 102 (Recovery on timer expiry)

Como o Monitor trata o SIP 408

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora não respondeu à chamada a tempo (SIP 408).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 408 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 408 na prática?

Pela RFC 3261, o SIP 408 Request Timeout indica que o servidor não conseguiu produzir uma resposta num tempo adequado, por exemplo porque não localizou o usuário a tempo. O cliente pode repetir a requisição mais tarde, sem alterações.

Na prática, o erro 408 SIP tem duas origens. Pode vir de um servidor no caminho, como o proxy da operadora ou o PABX de destino, que repassou a chamada e não recebeu resposta. Ou pode ser gerado localmente pelo seu PABX, quando o INVITE não teve resposta nenhuma até o temporizador B expirar. Em chamadas que vêm da telefonia convencional, ele costuma corresponder à Q.850 cause 18; no sentido contrário, à Q.850 cause 102. Em todos os casos, alguém parou de responder.

Causas comuns no Brasil

- Firewall ou regra de NAT bloqueando as respostas SIP que voltam da operadora, depois de uma troca de roteador ou de link.
- Ramal de destino que aparece como registrado no Asterisk, Issabel, FreePBX ou 3CX, mas cujo mapeamento de NAT expirou e já não recebe o INVITE.
- INVITE grande demais sobre UDP, com muitos codecs ou headers, fragmentado no caminho e descartado por algum equipamento.
- Servidor da operadora indisponível ou rota de internet instável até ele.
- DNS do tronco apontando para um servidor desativado.
- Telefone IP desligado ou sem rede, com o registro ainda válido no PABX.

Como diagnosticar

1. Capture com `sngrep port 5060` e confirme se o INVITE sai, quantas retransmissões acontecem e se volta algum 100 Trying.
2. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip). Se o 408 não aparece na rede, foi gerado localmente.

3. Para ramais, rode `pjsip show contacts` (ou `sip show peers`) e veja se o contato está `Avail` ou `Unavail`, com o tempo de resposta do qualify.
4. Verifique o tamanho do INVITE na captura. Se passa de cerca de 1.300 bytes, reduza a lista de codecs ou teste o tronco em TCP.
5. Rode `tcpdump -i any -w trace.pcap port 5060` também no roteador ou firewall, se possível, para ver onde a mensagem se perde.
6. No 3CX, ative o “Verbose logging” e confira no log de atividade se o tronco ou o ramal ficou sem resposta.

O que mandar para a operadora

- Data e hora com fuso horário das chamadas sem resposta.
- Número de origem (A) e número chamado (B).
- Call-ID de uma chamada afetada e o horário de cada retransmissão do INVITE.
- A linha completa do 408, se ele veio da rede, e o header Reason com a causa Q.850, se houver.
- O IP e a porta de destino usados e quantas tentativas falharam.
- O pcap capturado na borda da sua rede.

Perguntas frequentes

O 408 sempre vem da operadora?

Não. Pela RFC 3261, quando um INVITE fica sem nenhuma resposta até o temporizador B expirar (32 segundos com os valores padrão), o próprio equipamento de origem trata a falha como 408. Muitas vezes nenhum 408 passou pela rede. Se a captura mostra o INVITE saindo e nada voltando, o problema está no caminho ou no servidor de destino.

Que causa Q.850 acompanha o 408?

Pela RFC 3398, a Q.850 cause 18 (No user responding) é convertida em 408 quando a chamada sai da rede de telefonia para o SIP. No sentido inverso, um 408 que entra na rede de telefonia vira a Q.850 cause 102 (Recovery on timer expiry). As duas falam de tempo esgotado sem resposta do destino.

CÓDIGOS SIP

SIP 410 Gone: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 410 Gone significa que o destino não está mais disponível naquele servidor e não há endereço de encaminhamento conhecido, numa condição considerada permanente. Na telefonia, quase sempre é um número desativado, cancelado ou trocado. Confirme com o dono do número se ele ainda está ativo e atualize o cadastro ou a rota para o número novo.

SIP 410 na referência

Código	410
Nome oficial	Gone
Classe	4xx: falha da requisição

Definido em	RFC 3261
Causas Q.850 que costumam vir junto	22 (Number changed), 23 (Redirection to new destination)

Como o Monitor trata o SIP 410

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora recusou a chamada: o número não está mais em serviço (SIP 410).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 410 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 410 na prática?

Pela RFC 3261, o SIP 410 Gone indica que o recurso pedido não está mais disponível no servidor e que não se conhece endereço de encaminhamento. A condição deve ser considerada permanente. Se o servidor não sabe se a condição é permanente, a RFC manda usar o SIP 404 no lugar.

Num tronco telefônico, o erro 410 SIP normalmente quer dizer “este número existia e deixou de existir”. É mais específico que o 404 e por isso menos comum: muitas redes respondem 404 ou tocam um aviso gravado mesmo quando o número foi desativado. Quando o 410 aparece, vale tratar como um sinal forte de mudança cadastral, e não como falha passageira de rede. Repetir a chamada não muda o resultado.

Causas comuns no Brasil

- Linha fixa ou celular cancelado pelo assinante e ainda não realocado a outro cliente.
- 0800 ou número de serviço desativado em migração de contrato ou de operadora.
- Número trocado pela empresa, com o antigo ainda cadastrado em agendas, URAs ou regras do PABX.
- DID de entrada removido do tronco, mas ainda divulgado ou ainda presente em encaminhamentos de outros sistemas.
- Ramal excluído num PABX Asterisk, Issabel, FreePBX, 3CX ou Intelbras configurado para responder 410 a usuários removidos.

Como diagnosticar

1. Capture com `sngrep port 5060` e confira se a resposta é mesmo `410 Gone` e se há header `Reason: Q.850;cause=22` (RFC 6432).
2. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e veja de qual servidor veio o 410: da operadora ou de um PABX mais adiante.
3. Ligue para o mesmo número a partir de outra linha, de preferência de outra operadora, para confirmar que o resultado se repete.
4. Verifique se o número não está escrito errado no PABX ou na regra de saída: um dígito trocado pode levar a um número antigo desativado.
5. No 3CX, ative o “Verbose logging” e confira o número exato enviado ao tronco.
6. Se o número é seu, consulte a operadora que o detém sobre o status da linha e a data de alteração.

O que mandar para a operadora

- Data e hora com fuso horário das tentativas.
- Número de origem (A) e número chamado (B), como enviados no INVITE.
- Call-ID de pelo menos uma chamada.
- A linha completa da resposta 410 e o header Reason com a causa Q.850, se houver.
- Desde quando o número deixou de completar e quantas tentativas falharam.
- O pcap da captura, quando disponível.

Perguntas frequentes

Um número que recebe 410 pode voltar a funcionar?

Pode, mas não sozinho. O 410 indica uma condição que o servidor considera permanente, como o cancelamento da linha. Ele só volta a completar se o número for reativado ou realocado. Se o 0800 ou o número da sua empresa recebe 410, fale com a operadora que detém o número: ele pode ter sido cancelado por engano ou numa migração.

Que causa Q.850 acompanha o 410?

Pela RFC 3398, a Q.850 cause 22 (Number changed) sem número novo informado é convertida em 410, assim como a cause 23 (Redirection to new destination). Quando a rede informa o número novo, a cause 22 vira 301 Moved Permanently, com o número novo no header Contact. No sentido inverso, um 410 vira cause 22.

CÓDIGOS SIP

SIP 415 Unsupported Media Type: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 415 Unsupported Media Type significa que o servidor recusou a requisição porque o corpo da mensagem está num formato que ele não aceita para aquele método. Não é incompatibilidade de codec, que gera 488. A causa mais comum é um Content-Type inesperado. Leia o header Accept da resposta, que lista os formatos aceitos.

SIP 415 na referência

Código	415
Nome oficial	Unsupported Media Type
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	79 (Service or option not implemented, unspecified)

Como o Monitor trata o SIP 415

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora recusou a chamada (SIP 415).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 415 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 415 na prática?

Pela RFC 3261, o SIP 415 Unsupported Media Type indica que o servidor se recusa a atender a requisição porque o corpo da mensagem está num formato que ele não suporta para o método pedido. O servidor deve devolver a lista de formatos aceitos nos headers `Accept`, `Accept-Encoding` ou `Accept-Language`, conforme o problema.

Em troncos, o erro 415 SIP é raro numa chamada comum, porque quase todo INVITE leva só `application/sdp`. Ele aparece quando algum equipamento acrescenta outro conteúdo, como um corpo multipart com informações de sinalização da rede de telefonia, um corpo compactado, ou quando mensagens dentro da chamada, como INFO para DTMF, usam um tipo que o outro lado não aceita. Para incompatibilidade de codecs, o código correto é o SIP 488.

Causas comuns no Brasil

- PABX ou SBC enviando INVITE com corpo `multipart/mixed` (SDP mais dados de sinalização da telefonia) para uma operadora que só aceita SDP.
- DTMF enviado por SIP INFO com `application/dtmf-relay` ou `application/dtmf`, recusado pelo outro lado ao navegar numa URA.
- Corpo compactado (`Content-Encoding: gzip`) que o servidor de destino não sabe abrir.
- Header `Content-Type` ausente ou escrito errado depois de uma customização no Asterisk, Issabel, FreePBX ou 3CX.

- Gateway de interconexão configurado para SIP-I ou SIP-T falando com um tronco SIP comum.

Como diagnosticar

1. Capture com `sngrep port 5060` e confira o método que recebeu o 415 (INVITE, INFO, MESSAGE) e o `Content-Type` enviado.
2. Leia os headers `Accept`, `Accept-Encoding` e `Accept-Language` da resposta para saber o que o servidor aceita.
3. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e confira o modo de DTMF do tronco. Em PJSIP, prefira `dtmf_mode=rfc4733`.
4. Se o INVITE leva corpo multipart, revise o SBC ou gateway que o acrescenta e desative a inclusão de dados de sinalização da telefonia para esse tronco.
5. No 3CX, ative o “Verbose logging” e confira o modo de DTMF e os parâmetros avançados do tronco.
6. Faça uma chamada de teste a uma URA e digite opções para confirmar que os dígitos chegam sem 415.

O que mandar para a operadora

- Data e hora com fuso horário das ocorrências.
- Número de origem (A) e número chamado (B).
- Call-ID da chamada e o método que recebeu o 415.
- A linha completa da resposta e os headers `Accept` recebidos.
- O `Content-Type` enviado e quantas tentativas falharam.
- O pcap da captura, quando disponível.

Perguntas frequentes

O 415 é a mesma coisa que codec incompatível?

Não. Codec incompatível é tratado dentro do SDP e costuma gerar o SIP 488 Not Acceptable Here. O 415 fala do tipo do corpo inteiro, indicado no header Content-Type, como application/sdp, multipart/mixed ou application/dtmf-relay. Se o servidor não aceita esse tipo para o método usado, responde 415, sem chegar à negociação de codecs.

Por que recebo 415 no meio da chamada, ao digitar na URA?

Quando o PABX envia os dígitos DTMF por mensagens SIP INFO, o corpo vai com um tipo como application/dtmf-relay. Se o outro lado não aceita esse tipo, responde 415 ao INFO e o dígito se perde, embora a chamada continue. Troque o envio de DTMF para RFC 4733 (eventos no RTP), que é o padrão mais aceito pelas operadoras.

CÓDIGOS SIP

SIP 480 Temporarily Unavailable: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

Resposta curta: SIP 480 Temporarily Unavailable significa que o destino foi localizado, mas não está disponível para atender agora: não está registrado, está em Não Perturbe ou não atendeu. A causa mais comum num PABX é o ramal ou o telefone IP sem registro. Verifique o registro do destino e procure o header Retry-After, que pode sugerir quando tentar de novo.

SIP 480 na referência

Código	480
Nome oficial	Temporarily Unavailable
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	19 (No answer from user (user alerted)), 20 (Subscriber absent), 31 (Normal, unspecified), 18 (No user responding)

Como o Monitor trata o SIP 480

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Depois de tocar	Sem ter tocado
Uma saudação ou mensagem gravada (a URA)	Fora do ar	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar	Fora do ar
Outro: pode tocar ou ser atendido	Em operação	Fora do ar

Para "Outro": Com "Contar ringback como alcançável" desmarcado: Fora do ar.

O que o Monitor registra para uma URA: “O número tocou e ninguém atendeu, mas este circuito deveria atender todas as chamadas sozinho (SIP 480).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 480 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 480 na prática?

Pela RFC 3261, o SIP 480 Temporarily Unavailable indica que o sistema do destino foi contatado, mas o usuário não está disponível no momento: não está logado, está num estado que impede a comunicação ou ativou o Não Perturbe. A resposta pode trazer o header `Retry-After` com um horário melhor para ligar. Proxies e servidores de redirecionamento também usam o 480 quando reconhecem o usuário, mas não têm um endereço válido para entregar a chamada.

Na telefonia, o 480 também carrega situações da rede: a Q.850 cause 20, como celular desligado ou fora de área, a cause 19, quando o destino tocou e não atendeu, e a Q.850 cause 31. É um código “temporário”: o mesmo número pode completar minutos depois. O erro 480 SIP repetido no mesmo destino, porém, merece investigação.

Causas comuns no Brasil

- Ramal ou telefone IP sem registro no Asterisk, Issabel, FreePBX, 3CX ou Intelbras, por queda de rede, reinício ou senha trocada.
- Ramal com Não Perturbe ativado, configurado para rejeitar a chamada em vez de mandar para a caixa postal.
- Celular de destino desligado, sem sinal ou fora da área de cobertura.
- Chamada que tocou até o tempo limite do PABX ou da rede, sem atendimento.
- Servidor de URA ou de atendimento automático que perdeu o registro com o PABX, deixando o 0800 sem destino.
- Fila sem agentes disponíveis, configurada para encerrar a chamada em vez de mantê-la em espera.

Como diagnosticar

1. Capture com `sngrep port 5060` e veja quem gerou o 480: a operadora ou o seu PABX. Confira os headers `Reason: Q.850;cause=...` e `Retry-After`.
2. No Asterisk ou FreePBX, rode `pjsip show contacts` (ou `sip show peers` no chan_sip) e confirme se o ramal de destino está registrado e respondendo.
3. Ative `pjsip set logger on` (ou `sip set debug on`) e repita a chamada para ver se ela chegou a tocar (180 ou 183) antes do 480.
4. Rode `core show channels` durante a chamada para ver em que fila, grupo ou ramal ela parou.
5. Revise no PABX as regras de Não Perturbe, de horário e de fila para o destino afetado.
6. No 3CX, ative o “Verbose logging” e confira o status do ramal ou da fila no momento da chamada.

O que mandar para a operadora

- Data e hora com fuso horário das chamadas.
- Número de origem (A) e número chamado (B).
- Call-ID de pelo menos uma chamada.
- A linha completa do 480, com os headers Reason (causa Q.850) e Retry-After, se houver.
- Se a chamada chegou a tocar e quantas tentativas falharam.
- O pcap da captura, quando disponível.

Perguntas frequentes

Qual causa Q.850 vem junto com o 480?

Pela RFC 3398, três causas são convertidas em 480: a 19 (No answer from user, o destino tocou e não atendeu), a 20 (Subscriber absent, como celular desligado ou fora de área) e a 31 (Normal, unspecified). No sentido inverso, um 480 que entra na rede de telefonia vira a Q.850 cause 18 (No user responding).

O 480 indica que meu 0800 está fora do ar?

Para um 0800 ou uma URA, que deveriam atender sempre, um 480 é sinal de problema: o destino final não está disponível, seja porque o servidor da URA saiu do registro, seja porque a fila não tinha ninguém para atender. Para um ramal pessoal, pode ser só alguém em Não Perturbe ou fora da mesa.

CÓDIGOS SIP

SIP 481 Call/Transaction Does Not Exist: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 481 Call/Transaction Does Not Exist significa que o servidor recebeu uma requisição que não corresponde a nenhum diálogo ou transação que ele conheça. A causa mais comum é um lado já ter encerrado a chamada enquanto o outro continua enviando mensagens. Se as chamadas caem sempre no mesmo minuto, revise os timers de sessão e o NAT.

SIP 481 na referência

Código	481
Nome oficial	Call/Transaction Does Not Exist
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	41 (Temporary failure)

Como o Monitor trata o SIP 481

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora recusou a chamada (SIP 481).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 481 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 481 na prática?

Pela RFC 3261, o SIP 481 Call/Transaction Does Not Exist indica que o servidor recebeu uma requisição que não corresponde a nenhum diálogo ou transação existente. O diálogo é identificado pelo Call-ID e pelas tags do From e do To. Se qualquer um desses valores muda no caminho, ou se um lado já esqueceu a chamada, a próxima mensagem recebe 481.

A RFC também diz que, quando uma requisição dentro do diálogo recebe 481, o cliente deve encerrar o diálogo. Por isso o erro 481 SIP raramente impede a chamada de começar. O efeito típico é a chamada que completa, fala normalmente e cai sozinha depois de alguns minutos, ou o CANCEL que chega tarde

demais. Um gateway que leva o 481 para a rede de telefonia o traduz como Q.850 cause 41, falha temporária.

Causas comuns no Brasil

- Renovação do timer de sessão (re-INVITE ou UPDATE) que chega a um SBC ou PABX que já descartou a chamada, derrubando a ligação sempre no mesmo minuto.
- Mapeamento de NAT expirado no roteador durante a chamada, fazendo as mensagens seguintes chegarem a outro destino.
- SIP ALG do roteador reescrevendo tags ou o Call-ID.
- Reinício ou troca de nó do SBC da operadora ou do PABX (Asterisk, Issabel, FreePBX, 3CX) no meio de chamadas ativas.
- CANCEL enviado depois que a chamada já foi atendida ou encerrada do outro lado.
- BYE enviado pelos dois lados quase ao mesmo tempo.

Como diagnosticar

1. Capture com `sngrep port 5060` e encontre a mensagem que recebeu 481: BYE, CANCEL, re-INVITE, UPDATE ou INFO.
2. Compare o Call-ID e as tags From e To dessa mensagem com as do INVITE original. Se mudaram, algum equipamento no caminho está reescrevendo o SIP.
3. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e confira os headers `Session-Expires` e `Min-SE` negociados.
4. Meça a duração das chamadas que caem. Se é sempre próxima da metade do Session-Expires, o problema está na renovação da sessão.
5. Revise o tempo de expiração de UDP no firewall e desative o SIP ALG do roteador.
6. No 3CX, ative o “Verbose logging” e confira se o tronco recebeu o 481 da operadora ou se foi o 3CX que o enviou.

O que mandar para a operadora

- Data e hora com fuso horário do início e da queda das chamadas.
- Número de origem (A) e número chamado (B).
- Call-ID da chamada e a mensagem que recebeu o 481.
- A linha completa da resposta e o valor de Session-Expires negociado.
- Quantas chamadas caíram e se a duração se repete.
- O pcap da chamada inteira, do INVITE à queda.

Perguntas frequentes

Por que minhas chamadas caem sempre depois do mesmo tempo?

Um padrão comum é o timer de sessão (RFC 4028). Cada lado renova a sessão com um re-INVITE ou UPDATE no intervalo combinado. Se essa renovação recebe 481 ou não tem resposta, a RFC 3261 diz que o diálogo deve ser encerrado, e a chamada cai. Quando isso acontece sempre no mesmo minuto, confira o Session-Expires negociado.

Receber 481 num BYE é grave?

Normalmente não. Se o outro lado já havia encerrado a chamada e o seu BYE chega depois, o 481 só confirma que não há mais nada para encerrar. O problema é o 481 em mensagens dentro de uma chamada que ainda deveria estar ativa, como re-INVITE, UPDATE ou INFO, porque isso derruba a ligação no meio.

CÓDIGOS SIP

SIP 484 Address Incomplete: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 484 Address Incomplete significa que o número enviado na Request-URI está incompleto e o destino não consegue completar a chamada sem mais dígitos. A causa mais comum é uma regra de discagem do PABX que corta dígitos, como DDD, o nono dígito do celular ou parte do 0800. Compare o número enviado com o formato completo esperado.

SIP 484 na referência

Código	484
Nome oficial	Address Incomplete
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	28 (Invalid number format (address incomplete))

Como o Monitor trata o SIP 484

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora recusou a chamada: o número discado está incompleto (SIP 484).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 484 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 484 na prática?

Pela RFC 3261, o SIP 484 Address Incomplete indica que o servidor recebeu uma requisição com uma Request-URI incompleta. A RFC recomenda que a frase de motivo traga mais informação. O código também é usado na discagem por partes (overlap dialing, RFC 3578), em que o número é enviado aos poucos e o 484 pede mais dígitos.

Em troncos SIP no Brasil, a discagem por partes é rara, e o 484 quase sempre significa que o PABX enviou menos dígitos do que deveria. Os formatos variam: chamada local com 8 dígitos (fixo) ou 9 (celular), longa distância com `0` + código da prestadora (CSP) + DDD + número, 0800 com 11 dígitos, ou E.164 com `+55`. Uma regra que corta o prefixo errado gera o erro 484 SIP. Se o número estiver completo mas não existir, o código esperado é o SIP 404.

Causas comuns no Brasil

- Regra de saída no FreePBX, Issabel ou 3CX que remove dígitos demais, por exemplo cortando o DDD junto com o `0`.
- Celular discado sem o nono dígito, ainda presente em agendas e cadastros antigos.
- 0800 cadastrado com um dígito a menos na URA, no CRM ou no PABX.
- Telefone IP com plano de discagem que envia o número cedo demais, antes de o usuário terminar de digitar.
- Número de longa distância enviado sem DDD a uma operadora que exige DDD em toda chamada.
- Número de serviço curto que a operadora não reconhece naquela forma.

Como diagnosticar

1. Capture com `sngrep port 5060` e conte os dígitos da Request-URI do INVITE que recebeu o 484.
2. No Asterisk ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e compare o número discado no ramal com o número que saiu para o tronco.
3. Revise as rotas de saída (dial patterns, prefixos a remover e a adicionar) no FreePBX ou no Issabel. No 3CX, revise as regras de saída e ative o “Verbose logging”.
4. No Asterisk, use `dialplan show <número>@<contexto>` para ver qual regra combinou com o número.
5. Teste o mesmo destino no formato completo, por exemplo DDD mais número, e em E.164, para descobrir o que a operadora aceita.
6. Confira o header `Reason: Q.850;cause=28` (RFC 6432) na resposta, se a operadora o envia.

O que mandar para a operadora

- Data e hora com fuso horário das tentativas.
- Número de origem (A) e número chamado (B), exatamente como estavam na Request-URI.
- Call-ID de pelo menos uma chamada.
- A linha completa do 484 e o header Reason com a causa Q.850, se houver.
- O formato de discagem que você está usando e quantas tentativas falharam.
- O pcap da captura, quando disponível.

Perguntas frequentes

Por que o PABX manda o número antes de eu terminar de discar?

Alguns telefones e PABX enviam o número assim que ele combina com uma regra de discagem curta. Se a regra aceita, por exemplo, oito dígitos, um celular com nove dígitos é enviado incompleto e volta como 484. Ajuste o plano de discagem do telefone e as regras de saída do PABX para os formatos atuais.

Que causa Q.850 vem junto com o 484?

Pela RFC 3398, a Q.850 cause 28 (Invalid number format, address incomplete) é convertida em 484, e o 484 é traduzido de volta como cause 28 quando a chamada passa para a rede de telefonia. Por isso, num log de interconexão, o mesmo problema pode aparecer como 484 de um lado e cause 28 do outro.

CÓDIGOS SIP

SIP 486 Busy Here: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 486 Busy Here significa que o destino foi alcançado, mas não pode aceitar outra chamada naquele ponto. Em ramal ou celular, é a pessoa já em ligação. Em tronco SIP, o mais comum é o limite de canais simultâneos esgotado. Confira quantas chamadas estavam ativas no momento e compare com o limite contratado.

SIP 486 na referência

Código	486
Nome oficial	Busy Here
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	17 (User busy)

Como o Monitor trata o SIP 486

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Em operação

Para "Outro": Com "Contar ocupado como alcançável" desmarcado: Fora do ar.

O que o Monitor registra para uma URA: “O número estava ocupado: o telefone está em outra chamada, mas este circuito deveria atender todas as chamadas sozinho (SIP 486).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 486 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 486 na prática?

O SIP 486 Busy Here é uma resposta final da classe 4xx: o sistema do destino foi contatado, mas não quer ou não consegue aceitar mais uma chamada naquele ponto. A RFC 3261 permite que a resposta traga o cabeçalho Retry-After, sugerindo quando tentar de novo. Na conversão para a rede telefônica, a RFC 3398 associa o 486 à Q.850 cause 17 (User busy), e o caminho inverso também leva a 486.

Em uma linha comum, “ocupado” quer dizer que alguém já está falando. Em tronco SIP, o sentido costuma ser outro: todos os canais simultâneos contratados ou configurados estão em uso, e a próxima chamada é recusada como ocupada. Por isso, um erro 486 SIP em horário de pico merece atenção mesmo quando ninguém está no telefone. Diferente do SIP 600, o 486 vale só para aquele destino; outro ponto ainda pode atender.

Causas comuns no Brasil

- Canais simultâneos esgotados no tronco SIP contratado com a operadora (Vivo, Claro, Algar, Embratel ou outra), em geral em horário de pico ou durante uma campanha de ligações.
- Limite de canais configurado no próprio PABX (Asterisk, Issabel, FreePBX, 3CX) menor que o contratado, recusando chamadas antes de o tronco encher.
- Ramal ou celular de destino já em ligação, sem chamada em espera habilitada.
- Fila ou grupo de atendimento de uma URA sem agentes livres, configurado para devolver ocupado em vez de manter a chamada na fila.
- Função “não perturbe” ativada em ramal Intelbras, aparelho IP ou softphone, que muitos equipamentos sinalizam como 486.
- Chamadas presas: canais que não foram liberados depois de uma falha no BYE continuam contando como em uso.

Como diagnosticar

1. Capture a sinalização com `sngrep` no servidor e veja quem gerou o 486: o PABX, o SBC ou a operadora. Os cabeçalhos Via, Server e User-Agent da resposta ajudam a identificar.
2. No Asterisk, Issabel ou FreePBX, rode `core show channels` no momento da falha para contar as chamadas ativas e comparar com o limite do tronco.
3. Ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e procure `Reason: Q.850;cause=17` e um eventual `Retry-After` na resposta.
4. Procure canais presos: chamadas com duração muito longa em `core show channels` costumam ser sessões que nunca receberam BYE.
5. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log se a recusa partiu do tronco ou de uma regra interna.
6. Ligue para o mesmo número por outro tronco ou por um celular. Se completar, o problema está na capacidade da rota, não no destino.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A) e número de destino (B), no formato enviado no INVITE.
- Call-ID da chamada e a linha completa da resposta, como `SIP/2.0 486 Busy Here`.
- O cabeçalho Reason com a causa Q.850, se veio, e o valor do Retry-After.
- Quantas tentativas falharam, em que intervalo, e quantas chamadas estavam ativas no tronco naquele momento.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

Qual a diferença entre SIP 486 e SIP 600?

O 486 Busy Here diz que o destino está ocupado naquele ponto, e outro aparelho ou outra rota ainda pode atender. O 600 Busy Everywhere é uma falha global: o destino sabe que nenhum outro ponto vai aceitar a chamada, e o proxy não deve tentar outras rotas. Em troncos e PABX no Brasil, o 486 aparece com muito mais frequência.

Por que o tronco dá ocupado se ninguém está no telefone?

Porque em tronco SIP 'ocupado' costuma significar que não há canal livre. Se o contrato prevê, por exemplo, 30 chamadas simultâneas e todas estão em uso, a próxima pode receber 486. Alguns SBCs e operadoras usam o SIP 503 com a Q.850 cause 34 nessa mesma situação. Compare o pico de chamadas com o limite contratado.

Uma chamada de teste real recebe esse ocupado?

Sim. Uma chamada de teste real passa pelo tronco como qualquer outra ligação, então recebe a resposta SIP final que a rede devolve, inclusive o 486. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 487 Request Terminated: o que significa e como resolver

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP 487 Request Terminated significa que o INVITE foi encerrado por um CANCEL antes de a chamada ser atendida. O mais comum é quem ligou desligar enquanto tocava, ou o PABX desistir por tempo esgotado. Não é falha do destino. Investigue só quando aparece em excesso: veja quem enviou o CANCEL e depois de quantos segundos.

SIP 487 na referência

Código	487
Nome oficial	Request Terminated
Classe	4xx: falha da requisição
Definido em	RFC 3261

Como o Monitor trata o SIP 487

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Depois de tocar	Sem ter tocado
Uma saudação ou mensagem gravada (a URA)	Fora do ar	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar	Fora do ar
Outro: pode tocar ou ser atendido	Em operação	Fora do ar

Para "Outro": Com "Contar ringback como alcançável" desmarcado: Fora do ar.

O que o Monitor registra para uma URA: “O número tocou e ninguém atendeu, mas este circuito deveria atender todas as chamadas sozinho (SIP 487).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 487 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 487 na prática?

O SIP 487 Request Terminated é a resposta que um pedido recebe quando é encerrado por um BYE ou por um CANCEL, segundo a RFC 3261. No caso típico, o fluxo é este: o INVITE sai, o destino responde 180 ou 183 e começa a tocar, quem ligou desiste e o seu lado envia CANCEL. O destino confirma o CANCEL com 200 OK e responde ao INVITE original com 487.

Por isso, o 487 vem do destino, mas a decisão de encerrar partiu de quem ligou. Ele aparece o tempo todo em logs de PABX e quase sempre é normal. O erro 487 SIP só merece investigação quando o volume foge do padrão, quando o CANCEL sai sempre no mesmo número de segundos (sinal de um tempo limite configurado) ou quando o CANCEL chega de um equipamento que você não controla.

Causas comuns no Brasil

- Cliente desistiu enquanto tocava ou enquanto ouvia uma mensagem antes do atendimento.
- Tempo de toque esgotado no PABX: o `Dial()` do Asterisk, ou o tempo de toque de grupo ou fila no FreePBX e no Issabel, terminou e o PABX enviou CANCEL.
- Grupo de toque simultâneo: um ramal atendeu e os demais receberam CANCEL.
- Fila de URA que transborda para outro destino depois de um tempo, cancelando a tentativa anterior.
- Discador de campanha com tempo de toque curto, que desiste antes de a pessoa conseguir atender.
- SBC entre o PABX e o tronco da operadora com temporizador próprio, que cancela o INVITE antes do tempo do PABX.

Como diagnosticar

1. Abra a chamada no `sngrep` e localize o CANCEL: veja quem o enviou e quantos segundos se passaram desde o INVITE e desde o 180 ou 183.
2. Se o CANCEL sai do seu PABX sempre no mesmo intervalo, como 20, 30 ou 60 segundos, revise o tempo do `Dial()` no plano de discagem ou o tempo de toque do grupo e da fila.
3. Ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e leia o cabeçalho Reason do CANCEL, como `Reason: SIP;cause=200` ou `Reason: Q.850;cause=16`.
4. No Asterisk, confira a variável `DIALSTATUS`: `CANCEL` indica que quem ligou desligou antes do atendimento, e `NOANSWER` indica que o tempo de toque acabou.
5. No 3CX, ative o log detalhado (Verbose) e veja no Activity Log quem encerrou a chamada antes do atendimento.
6. Compare a proporção de chamadas com 487 com o total do dia. Uma alta repentina costuma vir de mudança de configuração ou de fila sobrecarregada.

O que mandar para a operadora

- Só abra chamado se o CANCEL chegou do lado da operadora sem que ninguém do seu lado tenha desligado.
- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A sequência completa: INVITE, respostas provisórias, CANCEL e `SIP/2.0 487 Request Terminated`, com os horários de cada mensagem.
- O cabeçalho Reason do CANCEL e quantas chamadas foram afetadas.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

O SIP 487 é um erro?

Na maioria das vezes, não. Ele é a resposta padrão ao INVITE depois que o lado que ligou envia CANCEL, e aparece em qualquer log de PABX com chamadas não atendidas. Passa a ser problema quando surge em volume fora do normal, com tempo de toque curto demais ou com um CANCEL que ninguém do seu lado pediu.

Que causa Q.850 corresponde ao SIP 487?

A RFC 3398 não define causa Q.850 para o 487. No caminho da rede telefônica para o SIP, a Q.850 cause 16 (Normal call clearing) normalmente vira um BYE ou um CANCEL, e não um código de resposta. Por isso, quando a chamada vem de uma central telefônica e o chamador desiste, você vê o CANCEL seguido do 487.

Por que vejo 487 em ramais que não atenderam um grupo de toque?

Num grupo de toque simultâneo, o PABX chama vários ramais ao mesmo tempo. Quando um atende, ele envia CANCEL aos outros, e cada um responde 487. O CANCEL pode trazer o cabeçalho Reason indicando que a chamada foi completada em outro ponto. É o comportamento esperado.

SIP 488 Not Acceptable Here: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 488 Not Acceptable Here significa que o destino recebeu o INVITE, mas não aceitou a proposta de mídia do SDP. A causa mais comum é não haver codec em comum, como oferecer só G.729 a quem aceita G.711 lei A (PCMA). Compare os codecs da oferta com os aceitos pelo tronco e leia o cabeçalho Warning.

SIP 488 na referência

Código	488
Nome oficial	Not Acceptable Here
Classe	4xx: falha da requisição
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	65 (Bearer capability not implemented), 70 (Only restricted digital information bearer capability is available (national use))

Como o Monitor trata o SIP 488

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “O telefone do outro lado não consegue usar nenhum dos formatos de áudio (codecs) que a chamada ofereceu, então a chamada não pôde ser completada (SIP 488).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 488 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 488 na prática?

O SIP 488 Not Acceptable Here tem o mesmo sentido do SIP 606, mas vale só para o recurso endereçado no Request-URI, então o pedido pode funcionar em outro ponto. Em termos simples: o destino recebeu o INVITE, leu a oferta de mídia no SDP e não aceitou o codec, o perfil de transporte ou outro detalhe da sessão. A resposta pode trazer um SDP com as capacidades do destino e um cabeçalho Warning, como `305 Incompatible media format` ou `304 Media type not available`.

Ele também aparece no meio da chamada, como resposta a um re-INVITE, por exemplo numa troca para fax T.38. Pela RFC 3398, um gateway converte o erro 488 SIP em Q.850 conforme o Warning: cause 31 por padrão, ou cause 65 (Bearer capability not implemented) quando o Warning fala de capacidade de portadora. No sentido contrário, as causes 65 e 70 viram 488.

Causas comuns no Brasil

- PABX oferece só G.729 ou Opus, e o tronco da operadora (Vivo, Claro, Algar, Embratel ou outra) aceita G.711 lei A (PCMA).
- Aparelho ou softphone importado com G.711 lei µ (PCMU) como único codec, padrão nos Estados Unidos, falando com tronco que só aceita PCMA.
- Chamada recebida em que a operadora oferece só G.729 e o Asterisk não tem o módulo do codec, então o próprio PABX responde 488.
- Mídia criptografada: oferta com `RTP/SAVP` (SRTP) para um tronco que só aceita `RTP/AVP`, ou o contrário.
- Re-INVITE para fax T.38 enviado a um destino que não suporta T.38.
- Mudança de codec numa transferência ou na retirada de espera, recusada pelo SBC no meio da chamada.

Como diagnosticar

1. Abra a chamada no `sngrep`, entre no INVITE e leia a linha `m=audio` e as linhas `a=rtpmap`. Payload 8 é PCMA, 0 é PCMU e 18 é G.729.
2. Leia o Warning da resposta, por exemplo `Warning: 305 sbc.operadora "Incompatible media format"`, e o SDP que veio junto, se houver.
3. No Asterisk, Issabel ou FreePBX, rode `pjsip show endpoint <tronco>` e confira a linha `allow` (no chan_sip, `sip show peer <tronco>`). `core show translation` mostra quais conversões de codec estão disponíveis.
4. Compare o perfil da linha `m=audio`: `RTP/AVP` é áudio sem criptografia, `RTP/SAVP` é SRTP. Confira a opção `media_encryption` do endpoint.
5. Faça um teste com o tronco aceitando só `alaw`. Se a chamada completar, ajuste a ordem dos codecs.
6. Se o 488 vier num re-INVITE, veja o que o disparou (T.38, espera, transferência) com `pjsip set logger on` ou, no 3CX, com o log detalhado (Verbose).

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 488 Not Acceptable Here` e o cabeçalho Warning.
- O SDP do INVITE enviado, com as linhas `m=audio` e `a=rtpmap`.
- Se foi no INVITE inicial ou num re-INVITE, e quantas chamadas falharam.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

Qual codec usar em tronco SIP no Brasil?

O G.711 lei A (PCMA, payload 8) é o codec da rede telefônica brasileira e o mais aceito pelas operadoras. Muitos troncos também aceitam G.729 para economizar banda. Deixar PCMA na lista de codecs do tronco evita a maioria dos 488. Confirme com a operadora a lista exata, porque cada contrato pode ser diferente.

Qual a diferença entre SIP 488 e SIP 606?

Os dois dizem que a proposta de mídia não foi aceita. O 488 vale só para aquele destino, e o pedido pode funcionar em outro ponto. O 606 é uma falha global: nenhum outro ponto deve aceitar, e o proxy para de tentar. Na prática, o 488 aparece muito mais em troncos e PABX.

Uma chamada de teste real pega esse erro?

Sim. Uma chamada de teste real negocia a mídia com o destino como qualquer ligação, então recebe o 488 quando a proposta é recusada. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 500 Server Internal Error: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 500 Server Internal Error significa que um servidor na rota encontrou uma condição inesperada e não conseguiu processar o pedido. As causas comuns são falha de software no PABX, no SBC ou na operadora, ou um 503 de um servidor seguinte convertido em 500 por um proxy. Identifique quem gerou a resposta antes de abrir chamado.

SIP 500 na referência

Código	500
Nome oficial	Server Internal Error
Classe	5xx: falha do servidor
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	111 (Protocol error, unspecified), 127 (Interworking, unspecified), 41 (Temporary failure)

Como o Monitor trata o SIP 500

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora não conseguiu completar a chamada por uma falha do lado dela: uma falha interna na operadora (SIP 500).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 500 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 500 na prática?

O SIP 500 Server Internal Error é a resposta genérica da classe 5xx: o servidor encontrou uma condição inesperada que o impediu de atender o pedido. A RFC 3261 permite que ele traga Retry-After, e o cliente pode tentar de novo depois de alguns segundos. O código não diz qual foi a falha, só que ela aconteceu do lado do servidor que respondeu.

Um detalhe importa no diagnóstico: pela RFC 3261, um proxy que recebe apenas um SIP 503 de um servidor seguinte não deve repassá-lo, e sim gerar um 500. Então um erro 500 SIP pode esconder uma indisponibilidade mais adiante. Na interligação com a rede telefônica, a RFC 3398 converte a Q.850 cause 127 (Interworking, unspecified), a cause 111 e qualquer causa sem mapeamento em 500.

Causas comuns no Brasil

- Falha de software no PABX (Asterisk, Issabel, FreePBX, 3CX) depois de uma atualização de versão ou de módulo.
- Dependência interna fora do ar em PABX ou plataforma da operadora, como banco de dados ou serviço de roteamento.
- Proxy ou SBC que recebeu um 503 do servidor seguinte e o converteu em 500.
- Gateway SIP para E1 que recebeu da central uma causa Q.850 sem mapeamento, como 111 ou 127, e devolveu 500.
- SBC da operadora (Vivo, Claro, Algar, Embratel ou outra) com falha intermitente durante manutenção ou reinício.

Como diagnosticar

1. Capture a chamada com `sngrep` e identifique quem gerou o 500 pelos cabeçalhos Via, Server e User-Agent.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e procure o cabeçalho Reason, como `Reason: Q.850;cause=127`, e um eventual Retry-After.
3. Se o 500 saiu do seu PABX, leia o log completo do Asterisk no mesmo horário em busca de erros de módulo ou de banco de dados.
4. Rode `pjsip show registrations` e `core show channels` para descartar tronco caído ou PABX sobrecarregado.
5. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log qual etapa falhou.
6. Repita a chamada algumas vezes. Um 500 em toda chamada aponta para configuração ou software; um 500 intermitente aponta para sobrecarga ou falha mais adiante.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 500 Server Internal Error` e os cabeçalhos Server, Reason e Retry-After, se vieram.
- Quantas tentativas falharam e se a falha é constante ou intermitente.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

O SIP 500 vem sempre da operadora?

Não. Qualquer servidor na rota pode gerar o 500: o seu PABX, um SBC na sua rede, o SBC da operadora ou um equipamento mais adiante. Antes de abrir chamado, capture a resposta e confira os cabeçalhos Via, Server e User-Agent. Se o 500 nasceu no seu PABX, o problema é local.

Que causa Q.850 acompanha o SIP 500?

Pela RFC 3398, um gateway converte o SIP 500 em Q.850 cause 41 (Temporary failure). No sentido contrário, a cause 111 (Protocol error, unspecified), a cause 127 (Interworking, unspecified) e qualquer causa sem mapeamento próprio viram 500. Um cabeçalho `Reason: Q.850;cause=127` indica falha de conversão entre redes.

Uma chamada de teste real pega esse erro?

Sim. Uma chamada de teste real recebe a resposta SIP final que a rede devolve, inclusive o 500. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 501 Not Implemented: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 501 Not Implemented significa que o servidor não suporta a funcionalidade necessária para atender o pedido, tipicamente um método SIP que ele não reconhece. Aparece mais em REFER, UPDATE, INFO ou MESSAGE do que no INVITE. Veja no trace qual método recebeu o 501 e ajuste o PABX para não enviá-lo àquele tronco.

SIP 501 na referência

Código	501
Nome oficial	Not Implemented
Classe	5xx: falha do servidor
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	29 (Facility rejected), 79 (Service or option not implemented, unspecified)

Como o Monitor trata o SIP 501

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora não conseguiu completar a chamada por uma falha do lado dela (SIP 501).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 501 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 501 na prática?

O SIP 501 Not Implemented diz que o servidor não suporta a funcionalidade necessária para atender o pedido. Pela RFC 3261, é a resposta adequada quando quem recebe não reconhece o método do pedido e não consegue suportá-lo para nenhum usuário. Proxies encaminham pedidos de qualquer método, então o 501 costuma vir do equipamento final, como o SBC da operadora ou o PABX do destino.

Na prática, o erro 501 SIP raramente bloqueia a chamada inteira. Ele costuma atingir uma função: a transferência que usa REFER, a atualização de sessão com UPDATE, o DTMF via INFO ou uma mensagem MESSAGE. O cabeçalho CSeq da resposta mostra o método recusado, como `CSeq: 102 REFER`. Na interligação com a rede telefônica, a RFC 3398 converte o 501 em Q.850 cause 79 e faz o caminho inverso a partir das causes 29 e 79.

Causas comuns no Brasil

- Transferência de chamada pelo aparelho ou pelo PABX gerando REFER para um tronco de operadora (Vivo, Claro, Algar, Embratel ou outra) que não implementa esse método.
- UPDATE enviado para renovar a sessão ou atualizar dados da chamada a um equipamento que não o suporta.
- INFO para DTMF ou MESSAGE para texto enviados por aparelhos IP ou softphones a um tronco que não trata esses métodos.
- SUBSCRIBE ou PUBLISH de presença e de luzes de ocupação (BLF) indo por engano para o tronco, em vez de ficar entre ramais.
- Gateway SIP para E1 que recebeu da central a Q.850 cause 79 ou 29 e devolveu 501.

Como diagnosticar

1. Abra o trace no `sngrep` e filtre a resposta 501. O cabeçalho CSeq mostra qual método foi recusado.

2. Envie ou capture um OPTIONS para o tronco e leia o cabeçalho Allow da resposta: ele lista os métodos que o equipamento aceita.
3. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e repita a ação que falhou, como a transferência, para ver qual pedido saiu.
4. Rode `pjsip show endpoint <tronco>` e revise as opções que geram métodos extras, como modo de DTMF e temporizadores de sessão.
5. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log qual pedido recebeu o 501.
6. Se o 501 vier em resposta ao INVITE, procure no SDP ou nos cabeçalhos Require e Supported alguma extensão que o destino não implementa.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 501 Not Implemented` e o cabeçalho CSeq com o método recusado.
- Qual função falhou para o usuário (transferência, DTMF, chamada inteira).
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

Qual a diferença entre SIP 501 e SIP 405?

O 501 Not Implemented diz que o servidor não reconhece o método e não o suporta para nenhum usuário. O 405 Method Not Allowed diz que o servidor reconhece o método, mas ele não é permitido para aquele recurso. Nos dois casos, o cabeçalho Allow da resposta ou de um OPTIONS mostra quais métodos o equipamento aceita.

Um 501 na resposta ao OPTIONS derruba o tronco?

Em geral, não. O OPTIONS é usado como teste de vida do tronco, e qualquer resposta mostra que o equipamento do outro lado está no ar. O que importa para as chamadas é a resposta ao INVITE. Confira, porém, se o seu PABX ou SBC trata um 501 ao OPTIONS como falha, porque isso varia conforme a configuração.

Uma chamada de teste real pega esse erro?

Sim, quando ele vem em resposta ao INVITE. Uma chamada de teste real recebe a resposta SIP final que a rede devolve. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 502 Bad Gateway: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 502 Bad Gateway significa que um servidor agindo como gateway ou proxy recebeu uma resposta inválida do servidor seguinte na rota. Em troncos, costuma indicar falha na interconexão da operadora com a rede de destino, ou destino fora de serviço. Identifique pelos cabeçalhos quem gerou o 502 e informe a operadora com o Call-ID.

SIP 502 na referência

Código	502
Nome oficial	Bad Gateway
Classe	5xx: falha do servidor
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	27 (Destination out of order), 38 (Network out of order)

Como o Monitor trata o SIP 502

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	**Fora do ar**
Um tom de teste ou serviço de eco	**Fora do ar**
Outro: pode tocar ou ser atendido	**Fora do ar**

O que o Monitor registra para uma URA: “A operadora não conseguiu completar a chamada por uma falha do lado dela: um servidor na rota recebeu uma resposta inválida do seguinte (SIP 502).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 502 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 502 na prática?

O SIP 502 Bad Gateway é uma resposta da classe 5xx. Pela RFC 3261, o servidor que responde estava agindo como gateway ou proxy e recebeu uma resposta inválida do servidor seguinte, aquele que ele consultou para atender o pedido. Ou seja, quem envia o 502 não é o culpado direto: ele está avisando que o próximo salto falhou.

Na interligação com a rede telefônica, a RFC 3398 converte a Q.850 cause 27 (Destination out of order) em 502, e o 502 em cause 38 (Network out of order). Por isso, um erro 502 SIP numa chamada para fixo, celular ou 0800 costuma significar que a central do destino não conseguiu entregar a chamada. Em monitoramento de troncos SIP, o importante é separar um 502 isolado de um 502 que se repete para o mesmo destino.

Causas comuns no Brasil

- Destino fora de serviço na rede de outra operadora, sinalizado pela central com a Q.850 cause 27 e convertido em 502 pelo gateway.
- Falha na interconexão entre a operadora do seu tronco (Vivo, Claro, Algar, Embratel ou outra) e a rede onde o número está.
- PABX do destino com URA própria ou link E1 fora do ar, fazendo o gateway da operadora receber falha.

- SBC na sua rede, na frente do Asterisk, Issabel, FreePBX ou 3CX, recebendo do PABX uma resposta que ele não aceita.
- Equipamento atualizado na rota que passou a enviar mensagens fora do padrão para o salto anterior.

Como diagnosticar

1. Capture a chamada com `sngrep` e veja quem gerou o 502 pelos cabeçalhos Via, Server e User-Agent.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e procure `Reason: Q.850;cause=27` ou outra causa na resposta.
3. Ligue para o mesmo número por outro tronco ou por um celular. Se também falhar, o problema está no destino.
4. Teste outros números da mesma operadora de destino. Se todos falharem, a suspeita é a interconexão.
5. Se o 502 vier de um SBC seu, capture também do lado do PABX e compare a resposta que o PABX mandou com a que o SBC repassou.
6. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log qual tronco devolveu o 502.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 502 Bad Gateway` e os cabeçalhos Server e Reason.
- Se outros números da mesma rede de destino também falham, e quantas tentativas foram feitas.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

O SIP 502 é problema do meu PABX?

Raramente. O 502 é gerado por um equipamento que fica no meio da rota, como um proxy, um SBC ou um gateway para a rede telefônica, quando o salto seguinte devolve algo inválido. Se o 502 vem da operadora, a falha costuma estar além dela. Se vem de um SBC seu, confira a resposta que o PABX mandou para ele.

Que causa Q.850 acompanha o SIP 502?

Pela RFC 3398, um gateway converte o SIP 502 em Q.850 cause 38 (Network out of order). No sentido contrário, a Q.850 cause 27 (Destination out of order) vira 502. Um cabeçalho `Reason: Q.850;cause=27` indica que a central do destino considerou o destino fora de serviço.

Uma chamada de teste real pega esse erro?

Sim. Uma chamada de teste real recebe a resposta SIP final que a rede devolve, inclusive o 502. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

SIP 503 Service Unavailable: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 503 Service Unavailable significa que o servidor está temporariamente incapaz de processar a chamada, por sobrecarga ou manutenção. Em troncos, o mais comum é falta de canal ou de rota na operadora, ou um SBC fora do ar. Leia o Retry-After e a causa Q.850 no cabeçalho Reason e, se persistir, abra chamado com o Call-ID.

SIP 503 na referência

Código	503
Nome oficial	Service Unavailable
Classe	5xx: falha do servidor
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	34 (No circuit/channel available), 38 (Network out of order), 41 (Temporary failure), 42 (Switching equipment congestion), 47 (Resource unavailable, unspecified), 58 (Bearer capability not presently available), 88 (Incompatible destination)

Como o Monitor trata o SIP 503

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora não conseguiu completar a chamada por uma falha do lado dela: o serviço da operadora está indisponível (SIP 503).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 503 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 503 na prática?

O SIP 503 Service Unavailable diz que o servidor está temporariamente impossibilitado de processar o pedido, por sobrecarga ou manutenção. Pela RFC 3261, ele pode trazer Retry-After indicando quando tentar de novo, e quem recebe deve procurar um servidor alternativo. Sem Retry-After, o cliente trata a resposta como um 500.

Em troncos, o erro 503 SIP é o jeito mais comum de dizer “não há como completar agora”. A causa Q.850 no cabeçalho Reason ajuda a entender o motivo. Pela RFC 3398, viram 503 a cause 34 (No circuit/channel available), a cause 38 (Network out of order), a cause 41 (Temporary failure), a cause 42

(Switching equipment congestion), a cause 47 (Resource unavailable, unspecified), além das causes 58 e 88. No sentido contrário, o 503 vira cause 41.

Causas comuns no Brasil

- Canais simultâneos esgotados no tronco da operadora (Vivo, Claro, Algar, Embratel ou outra), com `Reason: Q.850;cause=34`.
- Limite de chamadas por segundo atingido em discadores e campanhas que disparam muitas ligações ao mesmo tempo.
- Manutenção programada ou reinício do SBC da operadora, às vezes com Retry-After.
- Congestionamento ou falha temporária na rota até a rede do destino, com causa 41 ou 42.
- PABX (Asterisk, Issabel, FreePBX, 3CX) sem nenhum tronco de saída disponível, gerando o 503 para o ramal.
- Licença ou capacidade do SBC esgotada na sua própria rede.

Como diagnosticar

1. Capture a chamada com `sngrep` e identifique quem gerou o 503 pelos cabeçalhos Via, Server e User-Agent.
2. Ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e leia o Reason, como `Reason: Q.850;cause=34`, e o Retry-After.
3. Rode `pjsip show registrations` para confirmar que o tronco está registrado e `core show channels` para contar as chamadas ativas.
4. Compare o número de chamadas ativas com o limite de canais contratado. Se bater no teto, o 503 é capacidade.
5. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log qual tronco respondeu e se havia rota alternativa.
6. Repita a chamada depois do tempo do Retry-After e por outro tronco. Se o 503 continuar só num tronco, o problema está nele.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 503 Service Unavailable` e os cabeçalhos Reason e Retry-After.
- Quantas tentativas falharam, em que intervalo, e quantas chamadas estavam ativas no tronco.
- Se a falha atinge todos os destinos ou só alguns.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

O que fazer com o cabeçalho Retry-After num SIP 503?

Ele diz quantos segundos esperar antes de mandar novos pedidos àquele servidor. Pela RFC 3261, quem recebe o 503 deve tentar um servidor alternativo e não mandar outros pedidos ao mesmo servidor durante esse tempo. Sem Retry-After, o 503 deve ser tratado como um 500. Se o seu PABX tem um segundo tronco, configure-o como rota alternativa.

O 503 sempre vem da operadora?

Não. O próprio PABX ou um SBC na sua rede também gera 503, por exemplo quando nenhum tronco de saída está disponível. Antes de abrir chamado, capture a resposta e confira os cabeçalhos Via, Server e User-Agent. Se o 503 nasceu dentro da sua rede, a operadora não vai encontrar nada.

Uma chamada de teste real pega esse erro?

Sim. Uma chamada de teste real passa pelo tronco como qualquer ligação e recebe a resposta SIP final que a rede devolve, inclusive o 503. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 504 Server Time-out: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 504 Server Time-out significa que um servidor na rota não recebeu a tempo a resposta de outro servidor que consultou para processar a chamada. Em troncos, costuma indicar um salto seguinte lento ou fora do ar, como a interconexão da operadora ou uma consulta de roteamento. Veja quem gerou o 504 e quanto tempo levou.

SIP 504 na referência

Código	504
Nome oficial	Server Time-out
Classe	5xx: falha do servidor
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	102 (Recovery on timer expiry)

Como o Monitor trata o SIP 504

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A operadora não conseguiu completar a chamada por uma falha do lado dela: um servidor na rota não recebeu resposta do seguinte a tempo (SIP 504).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 504 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 504 na prática?

O SIP 504 Server Time-out é uma resposta da classe 5xx. Pela RFC 3261, o servidor que responde não recebeu a tempo a resposta de um servidor externo que ele consultou para processar o pedido. Esse servidor externo pode ser o próximo proxy da rota, um gateway para a rede telefônica ou um serviço de consulta, como um servidor DNS ou uma base de roteamento.

Na interligação com a rede telefônica, a RFC 3398 associa o 504 à Q.850 cause 102 (Recovery on timer expiry), nos dois sentidos. Um erro 504 SIP mostra que o primeiro salto está no ar, mas que algo depois dele demorou demais. Se o seu PABX não recebe resposta nenhuma, o código que aparece costuma ser o SIP 408, gerado localmente.

Causas comuns no Brasil

- Interconexão lenta ou fora do ar entre a operadora do seu tronco (Vivo, Claro, Algar, Embratel ou outra) e a rede do destino.
- Consulta externa lenta no roteamento da chamada, como DNS ou uma base de roteamento consultada pelo SBC.
- Gateway SIP para E1 sem resposta da central dentro do temporizador, sinalizado com a Q.850 cause 102.
- SBC na sua rede, na frente do Asterisk, Issabel, FreePBX ou 3CX, aguardando um PABX sobrecarregado ou travado.
- Perda de pacotes ou bloqueio de firewall entre dois servidores da rota, fazendo as respostas não chegarem.

Como diagnosticar

1. Capture a chamada com `sngrep` e veja quem gerou o 504 pelos cabeçalhos Via, Server e User-Agent, e quanto tempo passou entre o INVITE e a resposta.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e procure `Reason: Q.850;cause=102`.
3. Se o 504 vier de um SBC seu, capture também do lado do PABX e confira se o PABX respondeu e com que atraso.
4. Rode `core show channels` e verifique a carga do servidor no horário da falha.
5. Ligue para o mesmo número por outro tronco e para outros números da mesma rede de destino, para separar rota e destino.
6. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log quanto tempo o tronco levou para responder.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 504 Server Time-out`, os cabeçalhos Server e Reason e o tempo entre o INVITE e a resposta.

- Se outros destinos também falham e quantas tentativas foram feitas.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

Qual a diferença entre SIP 504 e SIP 408?

O 408 Request Timeout diz que o pedido não teve resposta dentro do tempo esperado, e muitas vezes é gerado pelo próprio PABX quando ninguém respondeu. O 504 vem de um servidor no meio da rota, que recebeu o seu pedido mas não obteve resposta a tempo do servidor que precisou consultar. Com o 504, você sabe que pelo menos o primeiro salto está no ar.

Que causa Q.850 acompanha o SIP 504?

Pela RFC 3398, o SIP 504 vira Q.850 cause 102 (Recovery on timer expiry), e a cause 102 vira 504 no sentido contrário. Um cabeçalho `Reason: Q.850;cause=102` indica que um temporizador do protocolo expirou na rede telefônica antes de a chamada ser completada.

Uma chamada de teste real pega esse erro?

Sim. Uma chamada de teste real recebe a resposta SIP final que a rede devolve, inclusive o 504. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 600 Busy Everywhere: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 600 Busy Everywhere significa que o destino foi contatado, está ocupado e sabe que nenhum outro ponto aceitaria a chamada agora. É uma falha global da classe 6xx, então o proxy para de tentar outras rotas. Em tronco, pode indicar canais simultâneos esgotados. Verifique quem gerou a resposta e o limite de canais da rota.

SIP 600 na referência

Código	600
Nome oficial	Busy Everywhere
Classe	6xx: falha global
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	17 (User busy)

Como o Monitor trata o SIP 600

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar

O que deve atender o número	Leitura
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Em operação

Para "Outro": Com "Contar ocupado como alcançável" desmarcado: Fora do ar.

O que o Monitor registra para uma URA: “O número estava ocupado: o telefone está em outra chamada, mas este circuito deveria atender todas as chamadas sozinho (SIP 600).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 600 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 600 na prática?

O SIP 600 Busy Everywhere é uma resposta da classe 6xx, a das falhas globais. Segundo a RFC 3261, o sistema do destino foi contatado com sucesso, mas o destino está ocupado e não quer receber a chamada agora. O destino só deve usar essa resposta quando sabe que nenhum outro ponto conseguiria aceitar a chamada; ela pode trazer Retry-After com um horário melhor para tentar.

A consequência prática é que um proxy que recebe um 600 encerra as tentativas pendentes e não procura outras rotas. É aí que ele se separa do SIP 486, que diz “ocupado aqui” e deixa outras rotas livres. Em troncos, o 600 também pode significar canais simultâneos esgotados, quando o SBC da operadora ou da empresa está configurado para responder assim. Um erro 600 SIP é menos comum que o 486, e por isso vale identificar qual equipamento o gerou.

Causas comuns no Brasil

- Canais simultâneos esgotados em um SBC configurado para responder 600 em vez de 486, para evitar que o PABX tente outras rotas.
- Limite de chamadas simultâneas por conta SIP atingido em um tronco de operadora (Vivo, Claro, Algar, Embratel ou outra).
- Plataforma de atendimento ou URA hospedada que responde 600 quando todas as posições estão em uso.
- Grupo de toque com todos os ramais ocupados, quando o sistema de destino decide que nenhum deles pode atender.
- Equipamento intermediário que converte o ocupado recebido de outra rede em 600, em vez de repassar o 486.

Como diagnosticar

1. Capture a chamada com `sngrep` e veja quem gerou o 600, pelos cabeçalhos Via, Server e User-Agent da resposta.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e procure `Reason: Q.850;cause=17` e um eventual `Retry-After`.
3. Rode `core show channels` no momento da falha para contar as chamadas ativas e comparar com o limite de canais da rota.

4. Confira no log se o PABX tentou outra rota depois da resposta. Se a rota de transbordo nunca foi usada, o 600 pode ser o motivo.
5. No 3CX, ative o log detalhado (Verbose) e veja no Activity Log qual tronco devolveu o 600.
6. Repita a ligação por outro tronco ou por um celular. Se completar, o problema está na capacidade da rota, não no destino.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A) e número de destino (B), no formato enviado no INVITE.
- Call-ID e a linha completa da resposta, como `SIP/2.0 600 Busy Everywhere`.
- Os cabeçalhos Reason e Retry-After, se vieram.
- Quantas tentativas falharam, em que intervalo, e quantas chamadas estavam ativas no tronco.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

O SIP 600 é mais grave que o 486?

Não necessariamente. Os dois dizem que o destino está ocupado. A diferença está no alcance: o 486 vale só para aquele ponto, enquanto o 600 avisa que nenhum outro ponto vai aceitar, então o proxy não deve tentar outras rotas. Se o seu PABX tem rota de transbordo, um 600 pode impedir que ela seja usada.

Que causa Q.850 acompanha o SIP 600?

Pela RFC 3398, um gateway que converte o SIP 600 para a rede telefônica usa a Q.850 cause 17 (User busy). No sentido contrário, a cause 17 vira 486, não 600. Por isso, um 600 que chega no seu PABX quase sempre foi gerado por um equipamento SIP, e não traduzido de uma central telefônica.

Uma chamada de teste real pega esse código?

Sim. Uma chamada de teste real recebe a resposta SIP final que a rede devolve, inclusive o 600. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 603 Decline: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 603 Decline significa que o aparelho do destino foi contatado, mas o usuário ou o sistema recusou a chamada de forma explícita, e nenhum outro ponto deve ser tentado. As causas mais comuns são a pessoa rejeitar a ligação ou um bloqueio de chamadas. Confira se a recusa veio do destino, do PABX ou da operadora.

SIP 603 na referência

Código	603
Nome oficial	Decline

Classe	6xx: falha global
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	21 (Call rejected)

Como o Monitor trata o SIP 603

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Em operação

Para "Outro": Com "Contar ocupado como alcançável" desmarcado: Fora do ar.

O que o Monitor registra para uma URA: “O telefone do outro lado recusou a chamada, mas este circuito deveria atender todas as chamadas sozinho (SIP 603).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 603 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 603 na prática?

O SIP 603 Decline é uma falha global da classe 6xx. Pela RFC 3261, o aparelho do destino foi contatado com sucesso, mas o usuário não quer ou não pode participar da chamada. A resposta pode trazer Retry-After com um horário melhor para ligar, e só deve ser enviada quando o destino sabe que nenhum outro ponto vai atender. Um proxy que recebe um 603 encerra as tentativas pendentes.

A diferença para um ocupado é a intenção: no 603, alguém ou alguma regra decidiu recusar. Na interligação com a rede telefônica, a RFC 3398 converte o 603 em Q.850 cause 21 (Call rejected). Um erro 603 SIP que aparece em toda chamada para um número costuma ser regra de bloqueio, não uma pessoa recusando. Existem códigos mais específicos para chamadas indesejadas, como o 607 Unwanted e o 608 Rejected, mas muitos equipamentos ainda usam o 603.

Causas comuns no Brasil

- Pessoa que recusou a chamada no celular, no aparelho IP ou no softphone.
- Lista de bloqueio ou regra de horário no PABX do destino (Asterisk, Issabel, FreePBX, 3CX, Intelbras) configurada para recusar.
- Destino que recusa chamadas sem identificação de número (anônimas) ou com número de origem não reconhecido.
- Aplicativo ou serviço de bloqueio de chamadas indesejadas no lado do destino, marcando o número de origem.

- URA ou plataforma de atendimento fora do horário configurada para recusar, em vez de tocar uma mensagem.

Como diagnosticar

1. Capture a chamada com `sngrep` e veja quem gerou o 603 pelos cabeçalhos Via, Server e User-Agent, e se houve toque (180 ou 183) antes da recusa.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e procure `Reason: Q.850;cause=21` e um eventual Retry-After.
3. Confira o número de origem (A) e o cabeçalho de privacidade no INVITE. Uma origem anônima ou num formato estranho é motivo comum de recusa.
4. Ligue para o mesmo número de outro tronco e de um celular. Se só um número de origem é recusado, a suspeita é bloqueio desse número.
5. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log se a recusa veio do tronco ou de uma regra interna.
6. Se o 603 vier do seu próprio PABX, revise listas de bloqueio, regras de horário e rotas de entrada.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 603 Decline` e o cabeçalho Reason, se veio.
- Se outros números de origem conseguem completar para o mesmo destino.
- Quantas tentativas foram recusadas e em que intervalo.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

Qual a diferença entre SIP 603 e SIP 486?

O 486 Busy Here diz que o destino está ocupado e não pode atender agora naquele ponto. O 603 Decline diz que o destino recusou a chamada de forma ativa, e que nenhum outro ponto vai atender. Dependendo da rede e do aparelho, apertar 'recusar' no celular pode chegar como 603 ou como 486.

Que causa Q.850 acompanha o SIP 603?

Pela RFC 3398, um gateway converte o SIP 603 em Q.850 cause 21 (Call rejected). No sentido contrário, a cause 21 normalmente vira 403 Forbidden, e o 603 pode ser usado quando a recusa partiu do próprio usuário. Um cabeçalho `Reason: Q.850;cause=21` confirma uma recusa.

Uma chamada de teste real pega esse código?

Sim. Uma chamada de teste real recebe a resposta SIP final que a rede devolve, inclusive o 603. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 604 Does Not Exist Anywhere: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

Resposta curta: SIP 604 Does Not Exist Anywhere significa que o servidor tem informação confiável de que o usuário ou número do Request-URI não existe em nenhum lugar. É a versão global do 404 Not Found. As causas mais comuns são número desativado, digitado errado ou em formato inválido. Confira o número enviado no INVITE antes de abrir chamado.

SIP 604 na referência

Código	604
Nome oficial	Does Not Exist Anywhere
Classe	6xx: falha global
Definido em	RFC 3261
Causas Q.850 que costumam vir junto	1 (Unallocated (unassigned) number)

Como o Monitor trata o SIP 604

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A chamada foi recusada, e a operadora disse que falharia em qualquer lugar (SIP 604).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 604 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 604 na prática?

O SIP 604 Does Not Exist Anywhere é uma falha global da classe 6xx. Pela RFC 3261, o servidor tem informação confiável de que o usuário indicado no Request-URI não existe em lugar nenhum. É uma afirmação mais forte que a do SIP 404, que só diz que o usuário não foi encontrado naquele domínio. Um proxy que recebe um 604 encerra as tentativas pendentes e não procura outras rotas.

Na interligação com a rede telefônica, a RFC 3398 converte o 604 em Q.850 cause 1 (Unallocated number). O erro 604 SIP é raro: a maioria das operadoras sinaliza número inexistente com 404. Quando aparece, vale conferir primeiro o número que saiu no INVITE, porque um formato errado produz o mesmo resultado que um número desativado.

Causas comuns no Brasil

- Número desativado ou nunca atribuído pela operadora.

- Formato errado no INVITE: faltando o DDD, o nono dígito do celular ou o 0800 completo, ou com código de país quando o tronco espera formato nacional.
- Manipulação de dígitos na rota de saída do PABX (Asterisk, Issabel, FreePBX, 3CX) cortando ou acrescentando dígitos a mais.
- Ramal ou usuário inexistente num PABX de destino configurado para responder 604 em vez de 404.
- Número portado recentemente cujo roteamento ainda não foi atualizado na rota usada.

Como diagnosticar

1. Abra a chamada no `sngrep` e leia o Request-URI e o cabeçalho To do INVITE. Confira o número dígito a dígito.
2. No Asterisk, Issabel ou FreePBX, ative `pjsip set logger on` (ou `sip set debug on` no chan_sip) e compare o número discado pelo ramal com o que saiu para o tronco.
3. Revise as regras de manipulação de dígitos da rota de saída, como prefixos acrescentados ou removidos.
4. Ligue para o mesmo número de um celular. Se completar, o problema está no formato ou na rota, não no número.
5. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log o número enviado ao tronco.
6. Procure `Reason: Q.850;cause=1` na resposta, que confirma número não alocado.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A) e número de destino (B), exatamente como saíram no Request-URI.
- Call-ID e a linha completa `SIP/2.0 604 Does Not Exist Anywhere`, com o cabeçalho Reason, se veio.
- Se o número completa a partir de um celular ou de outro tronco.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

Qual a diferença entre SIP 604 e SIP 404?

O 404 Not Found diz que o usuário não foi encontrado naquele domínio ou servidor. O 604 Does Not Exist Anywhere vai além: o servidor tem informação confiável de que o usuário não existe em lugar nenhum, então nenhuma outra rota deve ser tentada. Na prática, o 404 é muito mais comum em troncos brasileiros.

Que causa Q.850 acompanha o SIP 604?

Pela RFC 3398, um gateway converte o SIP 604 em Q.850 cause 1 (Unallocated number). No sentido contrário, a cause 1 vira 404, e não 604. Por isso, um 604 que chega ao seu PABX quase sempre foi gerado por um equipamento SIP, e não traduzido de uma central telefônica.

Uma chamada de teste real pega esse erro?

Sim. Uma chamada de teste real recebe a resposta SIP final que a rede devolve, inclusive o 604. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

CÓDIGOS SIP

SIP 606 Not Acceptable: o que significa e como resolver

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** SIP 606 Not Acceptable significa que o destino foi contatado, mas não aceitou aspectos da sessão proposta, como mídia, largura de banda ou endereçamento, e indica que nenhum outro ponto aceitaria. É a versão global do 488. A causa mais comum é codec ou SRTP incompatível. Leia o cabeçalho Warning e compare o SDP oferecido.

SIP 606 na referência

Código	606
Nome oficial	Not Acceptable
Classe	6xx: falha global
Definido em	RFC 3261

Como o Monitor trata o SIP 606

A leitura depende do que deve atender o número, a pergunta que a 2N5 responde ao cadastrar cada circuito. Estas são as regras que o produto aplica hoje, geradas da mesma função que julga cada chamada de teste.

O que deve atender o número	Leitura
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

O que o Monitor registra para uma URA: “A chamada foi recusada, e a operadora disse que falharia em qualquer lugar (SIP 606).”

Uma chamada lida como **Fora do ar** não alerta ninguém sozinha: ela é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente, com o código SIP e a causa Q.850 de cada chamada como evidência para a operadora. No ritmo padrão, cada circuito é testado a cada 15 minutos.

Se a operadora devolve o SIP 606 ao registro da conta de chamadas da 2N5, antes de qualquer chamada, o teste fica **sem visibilidade**: é um problema do lado da 2N5, não conta contra o circuito e não avisa o cliente.

O que significa o SIP 606 na prática?

O SIP 606 Not Acceptable é uma falha global da classe 6xx. Pela RFC 3261, o sistema do destino foi contatado com sucesso, mas alguns aspectos da descrição da sessão, como a mídia pedida, a largura de banda ou o estilo de endereçamento, não são aceitáveis. Ele indica que o destino quer se comunicar, mas não consegue suportar a sessão como foi descrita. A resposta pode trazer um ou mais cabeçalhos Warning explicando o motivo.

A diferença para o SIP 488 está no alcance: o 488 vale só para aquele destino, enquanto o 606 avisa que nenhum outro ponto deve aceitar, e o proxy encerra as tentativas pendentes. Na prática, o erro 606 SIP é raro em troncos brasileiros. Quando aparece, quase sempre vem de um SBC ou de uma

plataforma configurada para recusar a oferta de mídia de forma definitiva.

Causas comuns no Brasil

- Oferta sem G.711 lei A (PCMA), o codec da rede telefônica brasileira, para um SBC de operadora (Vivo, Claro, Algar, Embratel ou outra) que só aceita esse codec.
- Mídia criptografada (`RTP/SAVP`) oferecida a um destino que só aceita áudio sem criptografia, ou o contrário.
- Oferta só de vídeo, ou com fluxo de vídeo obrigatório, para um destino que só trata áudio.
- Softphone ou aparelho com Opus ou G.722 como únicos codecs, falando com PABX Asterisk, Issabel, FreePBX ou 3CX sem esses codecs no tronco.
- Banda declarada no SDP acima do que o destino aceita.

Como diagnosticar

1. Abra a chamada no `sngrep` e leia o Warning da resposta, por exemplo `Warning: 305 sbc.destino "Incompatible media format"`.
2. No INVITE, confira a linha `m=audio` e as linhas `a=rtpmap`. Payload 8 é PCMA, 0 é PCMU e 18 é G.729.
3. Confira o perfil de transporte da linha `m=audio`: `RTP/AVP` é áudio sem criptografia e `RTP/SAVP` é SRTP.
4. No Asterisk, Issabel ou FreePBX, rode `pjsip show endpoint <tronco>` e veja `allow` e `media_encryption` (no chan_sip, `sip show peer <tronco>`). Com `pjsip set logger on`, veja o SDP completo.
5. No 3CX, ative o log detalhado (Verbose) e confira no Activity Log quais codecs foram oferecidos.
6. Repita a chamada só com `alaw` no tronco. Se completar, ajuste a lista de codecs do aparelho ou do PABX.

O que mandar para a operadora

- Data e hora exatas com fuso, por exemplo 2026-10-07 14:32:10 -03:00.
- Número de origem (A), número de destino (B) e o Call-ID.
- A linha completa `SIP/2.0 606 Not Acceptable` e todos os cabeçalhos Warning.
- O SDP do INVITE enviado.
- Quantas chamadas falharam e se o problema começou depois de alguma mudança.
- O arquivo pcap da captura, se você tiver.

Perguntas frequentes

O que o cabeçalho Warning diz num SIP 606?

Ele explica por que a sessão não foi aceita. O código de três dígitos indica o motivo, por exemplo 304 para tipo de mídia indisponível, 305 para formato de mídia incompatível e 370 para banda insuficiente. O texto entre aspas depois do nome do servidor costuma trazer mais detalhes. Sem o Warning, compare o SDP enviado com o que o destino aceita.

Que causa Q.850 acompanha o SIP 606?

Pela RFC 3398, depende do Warning: o gateway usa a Q.850 cause 31 (Normal, unspecified) por padrão, ou a cause 65 (Bearer capability not implemented) quando o Warning trata de capacidade de portadora. Nenhuma causa Q.850 é convertida em 606 no sentido contrário; a cause 65 vira 488.

Uma chamada de teste real pega esse erro?

Sim. Uma chamada de teste real negocia a mídia com o destino como qualquer ligação, então recebe o 606 quando a sessão é recusada. Quando o resultado conta como falha, a chamada é repetida antes de qualquer alerta, e o alerta segue por e-mail.

REFERÊNCIA

Causas Q.850 (hangup cause): lista completa e mapa SIP

A causa Q.850 é o número que a rede de telefonia dá para o fim de uma chamada: 16 quando ela termina normalmente, 17 quando o número está ocupado, 34 quando não há canal livre. Ela viaja na mensagem de liberação dos troncos E1 e, nos troncos SIP, no cabeçalho `Reason: Q.850;cause=N`.

Onde aparece a causa Q.850?

> Nos troncos E1 (SS7/ISUP ou ISDN), a causa vem na mensagem de liberação da chamada. Nos troncos SIP, a operadora ou o SBC a repete no cabeçalho Reason da resposta (RFC 6432). No Asterisk, no Issabel e no FreePBX ela é a variável `HANGUPCAUSE` e o campo hangupcause do CDR.

As 72 causas da ITU-T Q.850

Causa	Nome oficial	Classe
Causa 1	Unallocated (unassigned) number	Evento normal (1 a 31)
Causa 2	No route to specified transit network (national use)	Evento normal (1 a 31)
Causa 3	No route to destination	Evento normal (1 a 31)
Causa 4	Send special information tone	Evento normal (1 a 31)
Causa 5	Misdialled trunk prefix (national use)	Evento normal (1 a 31)
Causa 6	Channel unacceptable	Evento normal (1 a 31)
Causa 7	Call awarded and being delivered in an established channel	Evento normal (1 a 31)
Causa 8	Pre-emption	Evento normal (1 a 31)
Causa 9	Pre-emption – circuit reserved for reuse	Evento normal (1 a 31)
Causa 13	Call completed elsewhere	Evento normal (1 a 31)
Causa 14	QoR: ported number	Evento normal (1 a 31)
Causa 16	Normal call clearing	Evento normal (1 a 31)
Causa 17	User busy	Evento normal (1 a 31)
Causa 18	No user responding	Evento normal (1 a 31)
Causa 19	No answer from user (user alerted)	Evento normal (1 a 31)
Causa 20	Subscriber absent	Evento normal (1 a 31)
Causa 21	Call rejected	Evento normal (1 a 31)
Causa 22	Number changed	Evento normal (1 a 31)
Causa 23	Redirection to new destination	Evento normal (1 a 31)
Causa 24	Call rejected due to feature at the destination	Evento normal (1 a 31)
Causa 25	Exchange – routing error	Evento normal (1 a 31)
Causa 26	Non-selected user clearing	Evento normal (1 a 31)
Causa 27	Destination out of order	Evento normal (1 a 31)
Causa 28	Invalid number format (address incomplete)	Evento normal (1 a 31)

Causa	Nome oficial	Classe
Causa 29	Facility rejected	Evento normal (1 a 31)
Causa 30	Response to STATUS ENQUIRY	Evento normal (1 a 31)
Causa 31	Normal, unspecified	Evento normal (1 a 31)
Causa 34	No circuit/channel available	Recurso indisponível (34 a 47)
Causa 38	Network out of order	Recurso indisponível (34 a 47)
Causa 39	Permanent frame mode connection out of service	Recurso indisponível (34 a 47)
Causa 40	Permanent frame mode connection operational	Recurso indisponível (34 a 47)
Causa 41	Temporary failure	Recurso indisponível (34 a 47)
Causa 42	Switching equipment congestion	Recurso indisponível (34 a 47)
Causa 43	Access information discarded	Recurso indisponível (34 a 47)
Causa 44	Requested circuit/channel not available	Recurso indisponível (34 a 47)
Causa 46	Precedence call blocked	Recurso indisponível (34 a 47)
Causa 47	Resource unavailable, unspecified	Recurso indisponível (34 a 47)
Causa 49	Quality of service not available	Serviço ou opção indisponível (49 a 63)
Causa 50	Requested facility not subscribed	Serviço ou opção indisponível (49 a 63)
Causa 53	Outgoing calls barred within CUG	Serviço ou opção indisponível (49 a 63)
Causa 55	Incoming calls barred within CUG	Serviço ou opção indisponível (49 a 63)
Causa 57	Bearer capability not authorized	Serviço ou opção indisponível (49 a 63)
Causa 58	Bearer capability not presently available	Serviço ou opção indisponível (49 a 63)
Causa 62	Inconsistency in designated outgoing access information and subscriber class	Serviço ou opção indisponível (49 a 63)
Causa 63	Service or option not available, unspecified	Serviço ou opção indisponível (49 a 63)
Causa 65	Bearer capability not implemented	Serviço ou opção não implementado (65 a 79)
Causa 66	Channel type not implemented	Serviço ou opção não implementado (65 a 79)
Causa 69	Requested facility not implemented	Serviço ou opção não implementado (65 a 79)
Causa 70	Only restricted digital information bearer capability is available (national use)	Serviço ou opção não implementado (65 a 79)
Causa 79	Service or option not implemented, unspecified	Serviço ou opção não implementado (65 a 79)
Causa 81	Invalid call reference value	Mensagem inválida (81 a 95)
Causa 82	Identified channel does not exist	Mensagem inválida (81 a 95)
Causa 83	A suspended call exists, but this call identity does not	Mensagem inválida (81 a 95)

Causa	Nome oficial	Classe
Causa 84	Call identity in use	Mensagem inválida (81 a 95)
Causa 85	No call suspended	Mensagem inválida (81 a 95)
Causa 86	Call with the requested call identity has been cleared	Mensagem inválida (81 a 95)
Causa 87	User not member of CUG	Mensagem inválida (81 a 95)
Causa 88	Incompatible destination	Mensagem inválida (81 a 95)
Causa 90	Non-existent CUG	Mensagem inválida (81 a 95)
Causa 91	Invalid transit network selection (national use)	Mensagem inválida (81 a 95)
Causa 95	Invalid message, unspecified	Mensagem inválida (81 a 95)
Causa 96	Mandatory information element is missing	Erro de protocolo (96 a 111)
Causa 97	Message type non-existent or not implemented	Erro de protocolo (96 a 111)
Causa 98	Message not compatible with call state or message type non-existent or not implemented	Erro de protocolo (96 a 111)
Causa 99	Information element/parameter non-existent or not implemented	Erro de protocolo (96 a 111)
Causa 100	Invalid information element contents	Erro de protocolo (96 a 111)
Causa 101	Message not compatible with call state	Erro de protocolo (96 a 111)
Causa 102	Recovery on timer expiry	Erro de protocolo (96 a 111)
Causa 103	Parameter non-existent or not implemented – passed on (national use)	Erro de protocolo (96 a 111)
Causa 110	Message with unrecognized parameter discarded	Erro de protocolo (96 a 111)
Causa 111	Protocol error, unspecified	Erro de protocolo (96 a 111)
Causa 127	Interworking, unspecified	Interfuncionamento (127)

De causa Q.850 para código SIP (RFC 3398, §7.2.4.1)

Causa Q.850	Resposta SIP	Observação
1 (unallocated number)	SIP 404 Not Found	
2 (no route to network)	SIP 404 Not Found	
3 (no route to destination)	SIP 404 Not Found	
16 (normal call clearing)	Nenhuma	(*) usually results in a BYE or CANCEL, no status code
17 (user busy)	SIP 486 Busy Here	
18 (no user responding)	SIP 408 Request Timeout	
19 (no answer from the user)	SIP 480 Temporarily Unavailable	
20 (subscriber absent)	SIP 480 Temporarily Unavailable	
21 (call rejected)	SIP 403 Forbidden	(+) if cause location is user, 603 could be given instead
22 (number changed (w/o diagnostic))	SIP 410 Gone	

Causa Q.850	Resposta SIP	Observação
22 (number changed (w/ diagnostic))	301 Moved Permanently	new number from diagnostic SHOULD go in Contact
23 (redirection to new destination)	SIP 410 Gone	
26 (non-selected user clearing)	SIP 404 Not Found	(=) ANSI: misrouted ported number
27 (destination out of order)	SIP 502 Bad Gateway	
28 (address incomplete)	SIP 484 Address Incomplete	
29 (facility rejected)	SIP 501 Not Implemented	
31 (normal unspecified)	SIP 480 Temporarily Unavailable	
34 (no circuit available)	SIP 503 Service Unavailable	
38 (network out of order)	SIP 503 Service Unavailable	
41 (temporary failure)	SIP 503 Service Unavailable	
42 (switching equipment congestion)	SIP 503 Service Unavailable	
47 (resource unavailable)	SIP 503 Service Unavailable	
55 (incoming calls barred within CUG)	SIP 403 Forbidden	
57 (bearer capability not authorized)	SIP 403 Forbidden	
58 (bearer capability not presently available)	SIP 503 Service Unavailable	
65 (bearer capability not implemented)	SIP 488 Not Acceptable Here	
70 (only restricted digital avail)	SIP 488 Not Acceptable Here	
79 (service or option not implemented)	SIP 501 Not Implemented	
87 (user not member of CUG)	SIP 403 Forbidden	
88 (incompatible destination)	SIP 503 Service Unavailable	
102 (recovery of timer expiry)	SIP 504 Server Time-out	
111 (protocol error)	SIP 500 Server Internal Error	
127 (interworking unspecified)	SIP 500 Server Internal Error	
Qualquer outra ((not listed))	SIP 500 Server Internal Error	default for unlisted causes (SHOULD)

Causa Q.850	Resposta SIP	Observação
44 (requested circuit or channel not available)	Nenhuma	untranslatable: should not result in any SIP status; originating switch retries another CIC

De código SIP para causa Q.850 (RFC 3398, §8.2.6.1)

Resposta SIP	Causa Q.850	Observação
SIP 400 Bad Request	41 (Temporary Failure)	
SIP 401 Unauthorized	21 (Call rejected)	(*) try to authenticate first
SIP 402 Payment required	21 (Call rejected)	
SIP 403 Forbidden	21 (Call rejected)	
SIP 404 Not found	1 (Unallocated number)	
SIP 405 Method not allowed	63 (Service or option unavailable)	
SIP 406 Not acceptable	79 (Service/option not implemented)	(+)
SIP 407 Proxy authentication required	21 (Call rejected)	(*) try to authenticate first
SIP 408 Request timeout	102 (Recovery on timer expiry)	
SIP 410 Gone	22 (Number changed (w/o diagnostic))	
SIP 413 Request Entity too long	127 (Interworking)	(+)
SIP 414 Request-URI too long	127 (Interworking)	(+)
SIP 415 Unsupported media type	79 (Service/option not implemented)	(+)
SIP 416 Unsupported URI Scheme	127 (Interworking)	(+)
SIP 420 Bad extension	127 (Interworking)	(+)
SIP 421 Extension Required	127 (Interworking)	(+)
SIP 423 Interval Too Brief	127 (Interworking)	(+)
SIP 480 Temporarily unavailable	18 (No user responding)	
SIP 481 Call/Transaction Does not Exist	41 (Temporary Failure)	
SIP 482 Loop Detected	25 (Exchange - routing error)	
SIP 483 Too many hops	25 (Exchange - routing error)	
SIP 484 Address incomplete	28 (Invalid Number Format)	(+)
SIP 485 Ambiguous	1 (Unallocated number)	
SIP 486 Busy here	17 (User busy)	
SIP 487 Request Terminated	Pelo cabeçalho Warning	
SIP 488 Not Acceptable here	Pelo cabeçalho Warning	default 31; 65 if Warning is about bearer capability

Resposta SIP	Causa Q.850	Observação
SIP 500 Server internal error	41 (Temporary failure)	
SIP 501 Not implemented	79 (Not implemented, unspecified)	
SIP 502 Bad gateway	38 (Network out of order)	
SIP 503 Service unavailable	41 (Temporary failure)	
SIP 504 Server time-out	102 (Recovery on timer expiry)	
SIP 505 Version Not Supported	127 (Interworking)	(+) RFC text prints 504; corrected to 505 by Errata ID 2161 (Held for Document Update)
SIP 513 Message Too Large	127 (Interworking)	(+)
SIP 600 Busy everywhere	17 (User busy)	
SIP 603 Decline	21 (Call rejected)	
SIP 604 Does not exist anywhere	1 (Unallocated number)	
SIP 606 Not acceptable	Pelo cabeçalho Warning	default 31; 65 if Warning is about bearer capability
Qualquer outro (not listed)	31 (Normal, unspecified)	default for unlisted status codes

Fontes: ITU-T Q.850 (10/18, com a emenda 1 de 04/19), RFC 3398 (com a errata) e RFC 6432, consultadas em 7 de outubro de 2026.

CAUSAS Q.850

Q.850 cause 1 (Unallocated (unassigned) number): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 1 (Unallocated (unassigned) number) indica que a rede que encerrou a chamada não tem esse número atribuído a nenhum assinante. Não é congestionamento nem falha de tronco: o número não existe ali. Costuma vir de número desativado ou de formato de discagem errado. Confira o número exatamente como saiu no INVITE.

Causa 1 na referência

Causa	1
Nome oficial (ITU-T Q.850)	Unallocated (unassigned) number
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 404 Not Found

Como o Monitor trata a causa 1

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 1 aparece como: “o número não está alocado”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 1 na prática?

A Q.850 cause 1, Unallocated (unassigned) number, informa que o número de destino chegou a uma central que não o tem atribuído. O formato pode estar correto e a rota até aquela central pode existir; o que falta é um assinante ativo com aquele número. A causa pertence à classe de eventos normais, então não indica pane de equipamento. Em troncos E1 com SS7, ela chega no parâmetro de causa da mensagem REL do ISUP; num E1 ISDN (PRI), no DISCONNECT ou no RELEASE do Q.931. Em SIP, a RFC 3398 (seção 7.2.4.1) converte a causa 1 em SIP 404 Not Found, e muitas operadoras repetem o valor original no cabeçalho `Reason: Q.850;cause=1` (RFC 6432). No sentido inverso, 404, 485 e 604 voltam como causa 1. No Asterisk ela aparece em `${HANGUPCAUSE}` e, onde o CDR grava o campo, como hangupcause 1.

Quando ela aparece

- Número desativado ou cancelado, inclusive um 0800 que saiu do ar por fim de contrato.
- Celular discado sem o nono dígito, ou fixo discado com um dígito a mais ou a menos.
- PABX (Asterisk, Issabel, FreePBX, 3CX) que normaliza o número de forma errada: tira o DDD, mantém o 0 de saída ou manda o código de seleção de prestadora (CSP) num tronco que espera o formato E.164.
- Faixa de DDR recém-contratada ou portada que ainda não foi ativada na central da operadora.
- Número portado em que a base de roteamento ainda aponta para a operadora antiga.

Como diagnosticar

1. Ligue para o mesmo número a partir de um celular. Se também não completa, o problema é o número, não o seu tronco.
2. Capture a sinalização com `pjsip set logger on` (ou `sip set debug on` no chan_sip) e copie o Request-URI e o cabeçalho To exatamente como saíram.
3. Compare o formato enviado com o que a operadora pede no contrato: `+5511...`, `11...` ou `0xx11...` com CSP.
4. No `sngrep`, abra a chamada e veja a resposta final: um 404 com `Reason: Q.850;cause=1` confirma que a recusa veio da rede.
5. No 3CX, ative o Verbose logging e confira no Activity Log o número que saiu pelo tronco depois das regras de discagem.
6. Se o número é seu (DDR), peça à operadora a confirmação de que a faixa está ativa e roteada para o seu tronco.

O que mandar para a operadora

- Data e hora de cada tentativa, com fuso (por exemplo, 2026-10-07 14:32, UTC−3).
- Número A (origem) e número B (destino) no formato em que saíram no INVITE.
- Call-ID e a linha completa da resposta, como `SIP/2.0 404 Not Found`, com o cabeçalho Reason.
- Se o número B é uma faixa de DDR sua, o número do contrato ou a designação do circuito.
- O pcap da chamada, se você tiver.

Perguntas frequentes

A cause 1 sempre significa que o número não existe?

Significa que a rede que encerrou não reconhece o número como atribuído. Na prática pode ser um número desativado, mas também um número válido enviado no formato errado (sem o nono dígito do celular, sem DDD, com um prefixo a mais) ou uma faixa de DDR que a operadora ainda não ativou na central dela.

Qual a diferença entre cause 1 e cause 3?

A cause 1 diz que o número não está atribuído. A cause 3 (No route to destination) diz que a rede não tem rota até o destino, mesmo que o número exista em outra rede. As duas viram SIP 404 Not Found pela RFC 3398, então só o cabeçalho Reason ou o trace do lado TDM mostra qual das duas aconteceu.

CAUSAS Q.850

Q.850 cause 3 (No route to destination): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 3 (No route to destination) indica que a rede que encerrou a chamada não tem caminho até a rede do número chamado, embora o número possa existir. Costuma aparecer com prefixos não liberados no plano contratado ou com rotas de interconexão ausentes. Teste o mesmo destino por outra operadora e envie o trace à sua.

Causa 3 na referência

Causa	3
Nome oficial (ITU-T Q.850)	No route to destination
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 404 Not Found

Como o Monitor trata a causa 3

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 3 na prática?

A Q.850 cause 3, No route to destination, diz que a central que recebeu a chamada não sabe como chegar à rede onde está o destino. Diferente da cause 1, ela não afirma que o número está desativado: o número pode funcionar normalmente quando discado por outra rede. A causa é da classe normal e viaja na mensagem REL do ISUP em links SS7, no DISCONNECT do ISDN num E1 PRI, ou num cabeçalho `Reason: Q.850;cause=3` (RFC 6432) em troncos SIP. A RFC 3398 (seção 7.2.4.1) converte a causa 3 em SIP 404 Not Found, a mesma resposta da causa 1, por isso o 404 sozinho não basta para

separar as duas. No Asterisk, a variável `${HANGUPCAUSE}` fica em 3. Atenção: em celulares e modems LTE, o “cause code 3” das mensagens EMM é de outra tabela (Illegal UE) e não tem relação com esta causa.

Quando ela aparece

- Destinos fora do plano contratado: números internacionais, 0300, 0500 ou 0900 sem liberação no tronco.
- Chamadas para uma operadora com a qual a sua não tem rota configurada para aquele prefixo.
- Prefixo novo ou recém-portado que a tabela de roteamento da operadora ainda não reconhece.
- SBC ou gateway intermediário sem rota de saída para o padrão discado, que encerra com a causa 3 em vez de repassar.
- PABX com a rota de saída errada, mandando o número por um tronco que só aceita chamadas locais.

Como diagnosticar

1. Disque o mesmo número por outra operadora ou por um celular. Se completar, o número existe e o problema é de rota.
2. Teste outros números do mesmo prefixo para saber se a falta de rota é do prefixo inteiro ou de um número só.
3. Ative `pjsip set logger on` e confira se o 404 traz `Reason: Q.850;cause=3`; sem o Reason, peça à operadora a causa original.
4. No FreePBX ou no Issabel, confira em Outbound Routes qual rota casou com o padrão discado e por qual tronco a chamada saiu.
5. No 3CX, ative o Verbose logging e veja no Activity Log qual tronco foi usado e a resposta recebida.
6. Num E1 ISDN, use `pri set debug on span 1` e leia o campo location da causa: ele mostra se a recusa veio da rede local, da rede de trânsito ou da rede remota.

O que mandar para a operadora

- Data e hora de cada tentativa, com fuso.
- Números A e B como saíram, e o prefixo afetado.
- Call-ID, a linha `SIP/2.0 404 Not Found` e o cabeçalho Reason recebido.
- O resultado do teste pelo outro caminho (o número completa por outra operadora ou pelo celular).
- O pedido explícito: confirmar se o prefixo está liberado no plano e roteado na interconexão.

Perguntas frequentes

Por que a operadora devolve 404 se o número existe?

Porque a RFC 3398 converte tanto a cause 1 (número não atribuído) quanto a cause 3 (sem rota) em SIP 404 Not Found. O 404 só diz que a rede não completou até aquele número. O cabeçalho Reason com cause=3, ou o trace do lado TDM, mostra que o número pode existir e que o que falta é a rota.

Liberar DDI ou 0300 no tronco resolve a cause 3?

Se o destino estava fora do plano contratado, sim: a operadora libera o prefixo e a chamada passa a ter rota. Se o prefixo já estava liberado, a falta de rota está mais adiante, numa interconexão ou numa tabela desatualizada, e só a operadora consegue corrigir. Por isso vale mandar exemplos de números e horários.

CAUSAS Q.850

Q.850 cause 16 (Normal call clearing): o que significa

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** Q.850 cause 16 (Normal call clearing) é o encerramento normal: uma das pontas desligou depois de a chamada ser estabelecida. Não indica falha. Vira problema quando muitas chamadas terminam com 16 em poucos segundos, sem áudio ou logo após o atendimento da URA. Nesse caso, veja quem mandou o BYE e se houve RTP nos dois sentidos.

Causa 16 na referência

Causa	16
Nome oficial (ITU-T Q.850)	Normal call clearing
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	Nenhuma: normalmente encerra a chamada com BYE ou CANCEL

Como o Monitor trata a causa 16

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 16 aparece como: “a chamada foi encerrada normalmente”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 16 na prática?

A Q.850 cause 16, Normal call clearing, indica que a chamada foi encerrada porque um dos usuários envolvidos pediu, ou seja, alguém desligou. É a causa mais comum em qualquer registro de chamadas e não representa falha. Num link SS7 ela segue na mensagem REL do ISUP; num E1 ISDN, no DISCONNECT do Q.931. Em SIP não existe resposta de erro equivalente: a RFC 3398 (seção 7.2.4.1) diz que a causa 16 normalmente resulta num BYE ou num CANCEL, muitas vezes com `Reason: Q.850;cause=16`. No Asterisk ela aparece como hangup cause 16 em `${HANGUPCAUSE}` e, no CDR, como hangupcause 16 quando o campo é gravado. Nos logs do 3CX e de outros PABX, a mesma causa costuma vir junto do lado que desligou. Em redes LTE, o “cause code 16” das mensagens EMM é outra coisa (MSC temporarily not reachable) e não deve ser confundido com esta causa.

Quando ela aparece

- Em toda chamada atendida que termina quando alguém desliga: é o caso normal.

- Em chamadas de 1 a 3 segundos após o 200 OK, quando a URA atende e derruba. A causa é normal, mas o atendimento não é.
- Quando há áudio só num sentido e a pessoa desliga por não ouvir nada: o registro mostra 16 e o defeito real é de mídia (NAT, firewall, SIP ALG).
- Quando um equipamento encerra por conta própria, por tempo máximo de chamada ou falta de RTP, e informa 16 no BYE, porque para a sinalização o encerramento foi ordenado.
- Em discadores que desligam ao detectar caixa postal ou silêncio.

Como diagnosticar

1. Separe as chamadas com causa 16 por duração. Um volume alto abaixo de 5 segundos merece atenção; o resto costuma ser normal.
2. No `sngrep`, veja quem mandou o BYE: o seu lado ou a operadora. Isso diz quem desligou.
3. Confira se houve RTP nos dois sentidos: no Asterisk, `rtp set debug on` mostra os pacotes; no `sngrep`, o fluxo exibe o RTP quando ele passa pela máquina.
4. Abra o BYE e leia o cabeçalho Reason. Um `cause=16` vindo da operadora logo após o atendimento indica que o destino desligou.
5. Se as quedas têm tempo fixo (por exemplo, sempre perto de 32 segundos), procure ACK perdido ou session timer: o desligamento é automático, mesmo que chegue com causa 16.

O que mandar para a operadora

- Em geral, nada: uma causa 16 isolada não é motivo de chamado.
- Se houver padrão, uma lista de chamadas curtas com data, hora e fuso, números A e B e a duração de cada uma.
- O Call-ID de cada exemplo e qual lado mandou o BYE, com o cabeçalho Reason.
- Se faltou áudio, o pcap com SIP e RTP mostrando o sentido sem pacotes.
- O horário em que o padrão começou e se ele se repete com o mesmo destino.

Perguntas frequentes

Hangup cause 16 no Asterisk é erro?

Não. No Asterisk, `${HANGUPCAUSE}` igual a 16 quer dizer que alguém desligou de forma ordenada, seja o seu usuário, seja o destino. É o valor mais comum em qualquer registro de chamadas. Só merece investigação quando aparece junto com duração muito curta, falta de áudio ou reclamações de queda, porque aí o desligamento normal pode ser consequência de outro problema.

Por que a cause 16 não tem código SIP de resposta?

Porque ela não é uma recusa. Pela RFC 3398, a causa 16 normalmente resulta num BYE, quando a chamada já foi atendida, ou num CANCEL, quando ainda estava tocando, sem código de status. O valor costuma vir dentro dessas mensagens no cabeçalho `Reason: Q.850;cause=16`, definido na RFC 3326.

Uma chamada de teste real ajuda a ver quando a cause 16 esconde um problema?

Ajuda, porque é uma chamada de verdade: além da resposta SIP final, ela verifica o áudio nas duas direções e mede a qualidade de voz (MOS-LQO). Assim, uma chamada que termina com causa 16 mas sem áudio não passa despercebida. Falhas são repetidas antes de virar alerta, e o alerta segue por e-mail.

CAUSAS Q.850

Q.850 cause 17 (User busy): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

Resposta curta: Q.850 cause 17 (User busy) indica que o destino não aceitou a chamada porque estava ocupado. É uma causa normal: a rede funcionou e o equipamento do destino é compatível. Vira problema quando um 0800, uma URA ou um tronco dá ocupado com frequência, o que costuma ser limite de canais esgotado. Compare as chamadas simultâneas com o contratado.

Causa 17 na referência

Causa	17
Nome oficial (ITU-T Q.850)	User busy
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 486 Busy Here

Como o Monitor trata a causa 17

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 17 aparece como: “o número estava ocupado”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 17 na prática?

A Q.850 cause 17, User busy, é usada quando o destino não pode receber outra chamada porque está ocupado. O equipamento chamado é compatível e a rede funcionou; quem recusou foi o destino. Pela RFC 3398 (seção 7.2.4.1), a causa 17 vira SIP 486 Busy Here, e no caminho inverso tanto o 486 quanto o SIP 600 Busy Everywhere voltam como 17. Em links SS7 ela vem na REL do ISUP; em E1 ISDN, no DISCONNECT; em SIP, às vezes num `Reason: Q.850;cause=17`. No Asterisk, `${HANGUPCAUSE}` fica em 17 e o `DIALSTATUS` costuma ser BUSY. Muitos PABX respondem 486 também quando atingem um limite de chamadas simultâneas, então “ocupado” nem sempre significa uma pessoa ao telefone: pode ser só capacidade esgotada.

Quando ela aparece

- Pessoa já em outra chamada, sem chamada em espera.
- Usuário de celular que recusa a chamada: muitas redes devolvem ocupado nesse caso.
- Ramal com “não perturbe” configurado para responder ocupado.
- Limite de chamadas simultâneas atingido no ramal, no tronco SIP contratado ou na licença do PABX.
- 0800 ou URA com todos os canais em uso no horário de pico.
- Fila de atendimento configurada para dar ocupado quando lota.

Como diagnosticar

1. Ligue de outra linha no mesmo momento. Se der ocupado sempre, desconfie de limite, não de uma pessoa ocupada.
2. No Asterisk, `core show channels` mostra quantas chamadas estão ativas; compare com o número de canais do contrato.
3. No `sngrep`, veja de onde veio o 486: do seu PABX, do SBC ou da operadora. Os cabeçalhos Server ou User-Agent da resposta ajudam.
4. Confira os limites de chamadas configurados no ramal e no tronco (FreePBX, Issabel) e na licença do 3CX, quando ela limita chamadas simultâneas.
5. Veja se o ocupado se concentra em horários de pico, o que indica falta de capacidade.

O que mandar para a operadora

- Data, hora e fuso das tentativas que deram ocupado.
- Números A e B e quantas tentativas seguidas falharam.
- Call-ID, a linha `SIP/2.0 486 Busy Here` e o Reason recebido.
- Quantas chamadas simultâneas havia no seu lado no momento (saída do `core show channels`).
- Se o destino é um 0800 seu, o número de canais contratado para ele.

Perguntas frequentes

Cause code 17 no celular é a mesma coisa que Q.850 cause 17?

Não. Em redes móveis LTE, o 'cause code 17' que aparece em logs de modem ou de celular vem das causas EMM da 3GPP e significa falha de rede (Network failure). A Q.850 cause 17 é a causa de ocupado da telefonia, usada no ISUP, no ISDN e no cabeçalho Reason do SIP. Os números coincidem, as tabelas não.

Ocupado no meu 0800 é sempre culpa da operadora?

Não necessariamente. Se o 486 sai do seu PABX ou da sua URA, o limite é seu: canais, licença ou configuração da fila. Se sai da operadora antes de chegar ao seu equipamento, pode ser o limite de canais do contrato do 0800. O trace mostra quem respondeu, e é por ele que se decide para quem abrir o chamado.

CAUSAS Q.850

Q.850 cause 18 (No user responding): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 18 (No user responding) indica que o destino não respondeu ao pedido de chamada, nem com toque nem com atendimento, dentro do tempo previsto. Não é ocupado nem recusa: o aparelho simplesmente não reagiu. Em SIP costuma ser um ramal registrado que parou de responder, por NAT ou firewall. Confira o registro e o tráfego.

Causa 18 na referência

Causa	18
Nome oficial (ITU-T Q.850)	No user responding

Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 408 Request Timeout

Como o Monitor trata a causa 18

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 18 aparece como: “nenhum aparelho respondeu”.

A causa 18 também decide a leitura de um **SIP 480**, que sozinho não diz se o destino tocou ou se nada respondeu:

O que deve atender o número	SIP 480 com causa 18
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 18 na prática?

A Q.850 cause 18, No user responding, é usada quando o destino não responde ao pedido de estabelecimento com uma indicação de alerta (toque) ou de atendimento dentro do tempo previsto. A diferença para a causa 19 é que, na 19, o telefone tocou e ninguém atendeu; na 18, nem o toque foi confirmado. Pela RFC 3398 (seção 7.2.4.1), a causa 18 vira SIP 408 Request Timeout. No caminho inverso, a RFC converte o SIP 480 Temporarily Unavailable em 18, por isso um 480 da operadora pode aparecer no seu PABX como causa 18. Em SS7 ela vem na REL do ISUP; em SIP, num `Reason: Q.850;cause=18` (RFC 6432). No Asterisk, `${HANGUPCAUSE}` fica em 18 e, onde o CDR grava o campo, aparece como hangupcause 18.

Quando ela aparece

- Ramal SIP registrado atrás de NAT cujo mapeamento expirou: o INVITE não chega e ninguém responde.
- Softphone de celular em segundo plano que não acorda a tempo.
- Telefone IP desligado da tomada antes de o registro expirar.
- Router com SIP ALG que altera ou descarta o INVITE.
- Celular sem sinal, em redes que devolvem 18 em vez de 20.
- PABX do cliente, atrás de um 0800, que recebe o INVITE e não devolve nem 100 Trying.

Como diagnosticar

1. No `sngrep`, veja se o destino respondeu algo: sem 100 Trying nem 180 Ringing, o INVITE provavelmente não chegou.
2. No Asterisk, `pjsip show contacts` mostra se o contato está disponível no qualify; `pjsip show registrations` mostra o registro do seu tronco com a operadora.
3. Ative `qualify_frequency` no AOR (PJSIP) ou `qualify=yes` (chan_sip) para detectar contatos mortos antes da chamada.

4. Desative o SIP ALG no router e ajuste o keepalive de NAT do telefone.
5. Se o 408 vem da operadora, verifique se o INVITE saiu do seu firewall com `tcpdump -i any port 5060`.

O que mandar para a operadora

- Data, hora e fuso de cada tentativa.
- Números A e B.
- Call-ID e a resposta final recebida (`SIP/2.0 408 Request Timeout` ou 480), com o Reason.
- Se houve 100 Trying ou 180 Ringing antes da falha.
- O pcap mostrando que o INVITE saiu da sua rede.

Perguntas frequentes

Qual a diferença entre cause 18 e cause 19?

Na cause 18 (No user responding), o destino não confirmou nem o toque dentro do tempo. Na cause 19 (No answer from user, user alerted), o telefone tocou e ninguém atendeu. A primeira aponta para um equipamento inalcançável ou mudo; a segunda, para ninguém disponível. Pela RFC 3398, a 18 vira SIP 408 e a 19 vira SIP 480.

Por que um SIP 480 virou cause 18 no meu PABX?

Porque a RFC 3398 converte o SIP 480 Temporarily Unavailable em Q.850 cause 18 quando a chamada passa de SIP para a rede de telefonia. Se a operadora mandou o cabeçalho Reason, ele traz a causa original e é melhor confiar nele do que na tradução da tabela, que pode esconder uma causa 20 ou 31.

CAUSAS Q.850

Q.850 cause 20 (Subscriber absent): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 20 (Subscriber absent) indica que o assinante não está alcançável: celular desligado ou sem sinal, ou usuário não registrado em nenhuma interface. É uma causa normal e não aponta falha do tronco. Vira problema quando acontece num ramal ou destino que deveria estar sempre registrado, ou em muitos números ao mesmo tempo.

Causa 20 na referência

Causa	20
Nome oficial (ITU-T Q.850)	Subscriber absent
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 480 Temporarily Unavailable

Como o Monitor trata a causa 20

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora.

A causa 20 também decide a leitura de um **SIP 480**, que sozinho não diz se o destino tocou ou se nada respondeu:

O que deve atender o número	SIP 480 com causa 20
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 20 na prática?

A Q.850 cause 20, Subscriber absent, é usada quando a estação móvel saiu da rede, quando não há contato de rádio com ela ou quando um usuário não está endereçável em nenhuma interface usuário-rede. Em telefonia IP, o equivalente direto é um ramal sem registro ativo. A causa é da classe normal: a rede funcionou e encontrou o assinante ausente. Pela RFC 3398 (seção 7.2.4.1), a causa 20 vira SIP 480 Temporarily Unavailable. Ela chega na REL do ISUP em links SS7 e, em SIP, pode vir num `Reason: Q.850;cause=20` (RFC 6432). No Asterisk, `${HANGUPCAUSE}` fica em 20, e o CDR mostra hangupcause 20 quando a instalação grava esse campo. Como o mesmo 480 também é usado para outras situações, só o Reason confirma que se trata de assinante ausente.

Quando ela aparece

- Celular desligado, sem bateria ou fora da área de cobertura.
- Celular em modo avião ou sem chip ativo.
- Ramal SIP sem registro: telefone desligado, softphone fechado ou registro expirado.
- Ramal remoto que perdeu a conexão de internet.
- Chamada para um número móvel que a operadora de destino não consegue localizar no momento.

Como diagnosticar

1. Confirme se o destino é celular ou ramal. Num celular desligado, a causa é esperada e não há nada a corrigir no tronco.
2. Para ramais, use `pjsip show contacts` (ou `sip show peers` no chan_sip) e veja se o ramal tem contato registrado.
3. Veja o tempo de expiração do registro e se o telefone renova antes de expirar.
4. No `sngrep`, confira se o 480 veio com `Reason: Q.850;cause=20` e de qual equipamento.
5. No 3CX, o painel de ramais mostra quais estão registrados; cruze com o horário da falha.
6. Se a causa aparece para muitos números diferentes ao mesmo tempo, não é ausência de assinante: investigue a rota.

O que mandar para a operadora

- Em geral, nada: assinante ausente é uma situação do destino.
- Se muitos números distintos retornam 20 ao mesmo tempo: data, hora e fuso, e a lista de números B.
- Call-ID, a linha `SIP/2.0 480 Temporarily Unavailable` e o Reason.

- O teste por outra linha mostrando que os destinos estavam ligados e completavam.

Perguntas frequentes

Celular desligado sempre retorna cause 20?

Não sempre. Depende de como a operadora de destino trata o caso: algumas devolvem a causa 20, outras tocam um anúncio de desligado ou fora da área antes de encerrar, e outras usam a causa 18 ou 31. Em chamadas para celular, o que chega ao seu PABX depende da interconexão e de como cada rede traduz a causa para SIP.

Cause code 20 num modem 4G é a mesma coisa?

Não. Os 'cause codes' das mensagens EMM e ESM em LTE são de outra tabela, definida pela 3GPP, com outros significados. A Q.850 cause 20 é da telefonia: aparece no ISUP, no ISDN e no cabeçalho Reason do SIP. Se o número aparece num log de modem ou de celular, consulte a tabela da 3GPP, não a Q.850.

CAUSAS Q.850

Q.850 cause 21 (Call rejected): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 21 (Call rejected) indica que o equipamento que encerrou recusou a chamada, embora não estivesse ocupado nem fosse incompatível. A recusa pode vir do usuário ou da rede. Em troncos SIP é comum por falha de autenticação, IP não liberado ou número de origem não aceito. Confira as credenciais e o número A enviado.

Causa 21 na referência

Causa	21
Nome oficial (ITU-T Q.850)	Call rejected
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 403 Forbidden

Como o Monitor trata a causa 21

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 21 aparece como: “a chamada foi rejeitada”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 21 na prática?

A Q.850 cause 21, Call rejected, indica que o equipamento que envia a causa não quer aceitar a chamada, mesmo podendo, porque não está ocupado nem é incompatível. A recusa pode ser do próprio usuário ou da rede, por regras de bloqueio. Pela RFC 3398 (seção 7.2.4.1), a causa 21 vira SIP 403 Forbidden; se a localização da causa for o usuário, o gateway pode mandar SIP 603 Decline. No

sentido inverso, 401, 402, 403, 407 e 603 voltam como 21, o que explica por que erros de autenticação aparecem como chamada rejeitada no PABX. A causa chega na REL do ISUP, no DISCONNECT do ISDN ou num `Reason: Q.850;cause=21` (RFC 6432). No Asterisk, `${HANGUPCAUSE}` fica em 21, e no CDR aparece como hangupcause 21 quando o campo é gravado.

Quando ela aparece

- Senha ou usuário do tronco errados, ou registro expirado: o 401 ou 407 sem nova autenticação vira 21.
- IP do seu PABX não liberado na operadora, que responde 403.
- Número de origem (From ou P-Asserted-Identity) que não pertence ao tronco contratado.
- Destino com bloqueio de chamadas, como lista de bloqueio ou restrição a chamadas anônimas.
- Destinos fora do plano, como DDI, quando a operadora responde 403 em vez de 404.
- Pessoa no celular que recusa a chamada, em redes que usam 21 nesse caso.

Como diagnosticar

1. Veja a resposta SIP original no `sngrep`: 401 ou 407 indica autenticação, 403 indica permissão, 603 indica recusa do destino.
2. Confira `pjsip show registrations` (ou `sip show registry` no chan_sip) e o status do tronco no FreePBX, no Issabel ou no 3CX.
3. Compare o número A enviado no From e no P-Asserted-Identity com os números do contrato.
4. Teste outro destino pelo mesmo tronco. Se todos falham, é o tronco; se só um falha, é o destino.
5. Leia o Warning ou o texto do Reason: muitas operadoras explicam ali o motivo da recusa.

O que mandar para a operadora

- Data, hora e fuso das tentativas.
- Números A e B exatamente como saíram, incluindo From e P-Asserted-Identity.
- Call-ID e a linha `SIP/2.0 403 Forbidden` (ou 603), com o Reason e o Warning.
- O IP público de onde a chamada saiu.
- Se o tronco estava registrado no momento da falha.

Perguntas frequentes

Por que erro de senha aparece como cause 21?

Porque a RFC 3398 converte os SIP 401 Unauthorized e 407 Proxy Authentication Required em Q.850 cause 21 quando a autenticação não é refeita com sucesso. O PABX ou o gateway, ao traduzir a recusa para a telefonia, mostra chamada rejeitada. A causa real está na resposta SIP, por isso vale olhar a sinalização antes de culpar o destino.

Qual a diferença entre 403 e 603 na cause 21?

A RFC 3398 converte a cause 21 em SIP 403 Forbidden por padrão. Quando a causa vem com a localização usuário, ou seja, foi o próprio destino que recusou, o gateway pode usar SIP 603 Decline. Na prática, um 403 sugere bloqueio da rede ou do tronco, e um 603 sugere recusa do destino.

CAUSAS Q.850

Q.850 cause 27 (Destination out of order): o que significa

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** Q.850 cause 27 (Destination out of order) indica que o destino não pode ser alcançado porque a interface até ele não está funcionando: link físico caído, PABX desligado ou tronco do cliente sem resposta. É uma falha real, comum em 0800 e URA que terminam num PABX próprio. Verifique o equipamento e o link do destino.

Causa 27 na referência

Causa	27
Nome oficial (ITU-T Q.850)	Destination out of order
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 502 Bad Gateway

Como o Monitor trata a causa 27

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 27 aparece como: “o destino está fora de serviço”.

A causa 27 também decide a leitura de um **SIP 480**, que sozinho não diz se o destino tocou ou se nada respondeu:

O que deve atender o número	SIP 480 com causa 27
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 27 na prática?

A Q.850 cause 27, Destination out of order, indica que o destino não pode ser alcançado porque a interface até ele não está funcionando direito. A mensagem de sinalização não conseguiu ser entregue ao usuário remoto, por exemplo por falha na camada física ou de enlace, ou porque o equipamento do usuário está desconectado. Diferente das causas de ocupado ou ausente, aqui há uma falha. Pela RFC 3398 (seção 7.2.4.1), a causa 27 vira SIP 502 Bad Gateway. No sentido inverso, a mesma RFC converte o 502 em causa 38, então a causa pode mudar ao atravessar dois gateways. Ela chega na REL do ISUP, no DISCONNECT do ISDN e num `Reason: Q.850;cause=27`. No Asterisk, `${HANGUPCAUSE}` fica em 27. Em LTE, o “cause code 27” das mensagens ESM (Missing or unknown APN) não tem relação com esta causa.

Quando ela aparece

- E1 do PABX do cliente com alarme ou sem sincronismo: a central da operadora vê o link caído.
- Tronco SIP entre a operadora e o PABX do cliente sem resposta (OPTIONS sem retorno), marcado como fora de serviço.

- Link de internet do site do cliente caído, num 0800 ou numa URA que termina no PABX local.
- PABX desligado, reiniciando ou com o serviço SIP parado.
- Firewall do cliente bloqueando o IP da operadora depois de uma mudança de regra.

Como diagnosticar

1. Confirme no PABX de destino se ele está no ar e com o serviço rodando (`core show uptime` no Asterisk).
2. Num E1 via DAHDI, use `dahdi show status` para ver alarmes e `pri show spans` para o estado do canal D.
3. Num tronco SIP, verifique se as OPTIONS da operadora estão chegando e sendo respondidas com 200 OK; no `sngrep`, filtre pelo método OPTIONS.
4. Teste o link de internet do site e as regras do firewall para os IPs de sinalização e de mídia da operadora.
5. No 3CX, confira o status do tronco no painel e o Activity Log no horário da falha.
6. Se tudo estiver no ar do seu lado, peça à operadora o estado do circuito visto da central dela.

O que mandar para a operadora

- Data, hora e fuso do início da falha, e se ela continua.
- O número chamado (por exemplo, o 0800) e os números A usados nos testes.
- Call-ID e a resposta recebida (`SIP/2.0 502 Bad Gateway`), com o Reason.
- A designação do circuito E1 ou a identificação do tronco SIP.
- O estado do seu lado: alarmes do E1, status das OPTIONS, IP público atual.

Perguntas frequentes

A cause 27 é falha minha ou da operadora?

Depende de onde está o destino. Se o número termina num PABX seu, a causa indica que a rede não consegue entregar a chamada a ele: link, equipamento ou firewall do seu lado, ou o circuito entre os dois. Se o destino é de terceiros, a falha está no equipamento deles. O trace e o campo location da causa ajudam a separar.

Uma chamada de teste real pega a cause 27 num 0800?

Pega, porque é uma chamada real feita ao número: ela recebe a mesma resposta SIP final que um cliente receberia quando o destino está fora de serviço. Uma falha é repetida antes de virar alerta, para não avisar por um evento isolado, e o alerta segue por e-mail.

CAUSAS Q.850

Q.850 cause 31 (Normal, unspecified): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 31 (Normal, unspecified) é uma causa genérica: informa um evento normal quando nenhuma outra causa da classe normal se aplica. Por si só não indica falha. O problema é que muitos gateways a usam como valor padrão e escondem o motivo real. Procure a resposta SIP original e o Reason no trecho anterior.

Causa 31 na referência

Causa	31
Nome oficial (ITU-T Q.850)	Normal, unspecified
Classe	Evento normal (1 a 31)
Resposta SIP pela RFC 3398	SIP 480 Temporarily Unavailable

Como o Monitor trata a causa 31

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 31 aparece como: “uma falha de rede não especificada”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 31 na prática?

A Q.850 cause 31, Normal, unspecified, serve para relatar um evento normal apenas quando nenhuma outra causa da classe normal se aplica. Em outras palavras, é a causa de quem não sabe ou não diz o motivo. Pela RFC 3398 (seção 7.2.4.1), a causa 31 vira SIP 480 Temporarily Unavailable. No sentido inverso ela é ainda mais comum: a RFC define 31 como valor padrão para qualquer resposta SIP que não esteja na tabela, e também para 488 e 606 quando o Warning não trata de capacidade de portadora. Por isso uma causa 31 no seu PABX pode vir de dezenas de respostas SIP diferentes. Ela aparece na REL do ISUP, num `Reason: Q.850;cause=31` e, no Asterisk, em `${HANGUPCAUSE}`. Em LTE, o “cause code 31” das mensagens ESM (Request rejected, unspecified) é de outra tabela.

Quando ela aparece

- Gateway SIP-TDM que recebe uma resposta SIP sem correspondência na RFC 3398 e aplica o padrão 31.
- Falha de negociação de mídia (488 ou 606) sem Warning sobre portadora.
- Operadoras que usam 31 como resposta genérica para qualquer recusa.
- Chamadas para celular desligado, em redes que não detalham o motivo.
- Equipamentos antigos que não implementam causas mais específicas.

Como diagnosticar

1. Não pare na causa 31: encontre a resposta SIP original com `pjsip set logger on` (ou `sip set debug on`) ou no `sngrep`.
2. Se a 31 veio da operadora num Reason, peça a ela a causa ou a resposta original da rede de destino.
3. Agrupe as chamadas com causa 31 por destino e horário. Um destino só sugere o lado de lá; muitos destinos sugerem a rota.

4. Veja se havia 488 ou 606 com Warning: aí o problema é de codec, não de rede.
5. No Asterisk 11 ou mais novo, a função `HANGUPCAUSE` com o tipo `tech` guarda a resposta SIP de cada canal discado; grave-a no log ao lado da causa.
6. No 3CX, ative o Verbose logging para que o Activity Log mostre a resposta SIP completa.

O que mandar para a operadora

- Data, hora e fuso das tentativas.
- Números A e B.
- Call-ID, a resposta SIP recebida e o Reason com cause=31.
- O pedido explícito da causa original no trecho dela, já que a 31 não identifica o motivo.
- O pcap, se tiver, e a lista de destinos afetados.

Perguntas frequentes

A cause 31 é erro?

Por definição, não: ela pertence à classe normal e diz apenas que não há causa mais específica. Na prática, aparece muito em falhas reais, porque gateways a usam como valor padrão quando não sabem traduzir uma resposta SIP. Se as chamadas com causa 31 não completam, trate como falha e procure a resposta original.

Qual a diferença entre cause 16 e cause 31?

A cause 16 (Normal call clearing) diz que alguém desligou uma chamada estabelecida. A cause 31 (Normal, unspecified) diz que houve um evento normal sem causa específica, e costuma aparecer em chamadas que nem chegaram a completar. A 16 é o fim esperado de uma conversa; a 31 pede investigação quando se repete.

CAUSAS Q.850

Q.850 cause 34 (No circuit/channel available): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 34 (No circuit/channel available) indica que não havia circuito ou canal adequado livre para completar a chamada naquele momento. É falta de recurso, não número errado. Em troncos SIP e E1 costuma ser limite de canais simultâneos esgotado, seu ou da operadora. Compare as chamadas ativas com o contratado e tente de novo.

Causa 34 na referência

Causa	34
Nome oficial (ITU-T Q.850)	No circuit/channel available
Classe	Recurso indisponível (34 a 47)
Resposta SIP pela RFC 3398	SIP 503 Service Unavailable

Como o Monitor trata a causa 34

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 34 aparece como: “nenhum circuito ou canal estava disponível”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 34 na prática?

A Q.850 cause 34, No circuit/channel available, indica que não há circuito ou canal apropriado disponível para tratar a chamada no momento. Ela abre a classe de recursos indisponíveis: o número pode estar certo e a rota existir, mas faltou capacidade em algum trecho. Pela RFC 3398 (seção 7.2.4.1), a causa 34 vira SIP 503 Service Unavailable, a mesma resposta das causas 38, 41, 42 e 47. Em E1 com SS7 ela chega na REL do ISUP e, num E1 ISDN, no DISCONNECT; em SIP, num `Reason: Q.850;cause=34` (RFC 6432), às vezes junto com `Retry-After`. No Asterisk, `${HANGUPCAUSE}` fica em 34, o CDR mostra hangupcause 34 quando grava o campo, e o `DIALSTATUS` costuma ser CONGESTION. No 3CX, a falha aparece no Activity Log com a resposta 503 recebida do tronco.

Quando ela aparece

- Tronco SIP com todos os canais contratados em uso.
- E1 com os 30 canais ocupados, ou com parte dos canais bloqueados.
- Picos de discador ou de campanha que ultrapassam o limite do tronco.
- Rota de interconexão da operadora congestionada para um destino específico.
- Gateway GSM ou E1 com portas indisponíveis.

Como diagnosticar

1. No momento da falha, rode `core show channels` no Asterisk e compare o total de chamadas com os canais do contrato.
2. Veja de quem é o 503: do seu SBC, do seu PABX ou da operadora. No `sngrep`, olhe o User-Agent ou o Server da resposta.
3. Verifique se a resposta traz `Retry-After` e respeite o intervalo antes de tentar de novo.
4. Num E1, `pri show spans` e `dahdi show status` mostram se há canais bloqueados ou alarmes.
5. Separe por destino: se só um prefixo falha, a falta de canais está na interconexão, não no seu tronco.

O que mandar para a operadora

- Data, hora e fuso, de preferência com o início e o fim do período com falhas.
- Números A e B e quantas tentativas falharam.
- Call-ID, a linha `SIP/2.0 503 Service Unavailable` e o Reason com cause=34.
- Quantas chamadas simultâneas você tinha no momento e quantas o contrato prevê.
- Os prefixos de destino afetados.

Perguntas frequentes

Cause 34 significa que preciso contratar mais canais?

Às vezes. Se no momento da falha você estava usando todos os canais contratados, sim, o limite é seu. Se havia canais sobrando e a causa veio da operadora, a falta de circuito está dentro da rede dela ou numa interconexão, e quem resolve é ela. Por isso vale anotar quantas chamadas estavam ativas quando a falha ocorreu.

Qual a diferença entre cause 34 e cause 41?

Ambas viram SIP 503. A cause 34 diz especificamente que faltou circuito ou canal livre, ou seja, capacidade. A cause 41 diz que houve uma falha temporária de rede, sem ligação com capacidade. Na prática, a 34 costuma acompanhar picos de tráfego, enquanto a 41 aparece em instabilidades e também como tradução de SIP 500 e 503.

CAUSAS Q.850

Q.850 cause 38 (Network out of order): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 38 (Network out of order) indica que a rede não está funcionando corretamente e que a condição deve durar um tempo relativamente longo, então repetir na hora não deve resolver. É uma falha real, não do destino. Pode estar no seu link, no SBC ou na rede da operadora. Identifique quem gerou a causa e abra chamado.

Causa 38 na referência

Causa	38
Nome oficial (ITU-T Q.850)	Network out of order
Classe	Recurso indisponível (34 a 47)
Resposta SIP pela RFC 3398	SIP 503 Service Unavailable

Como o Monitor trata a causa 38

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 38 aparece como: “a rede está fora de serviço”.

A causa 38 também decide a leitura de um **SIP 480**, que sozinho não diz se o destino tocou ou se nada respondeu:

O que deve atender o número	SIP 480 com causa 38
Uma saudação ou mensagem gravada (a URA)	Fora do ar
Um tom de teste ou serviço de eco	Fora do ar
Outro: pode tocar ou ser atendido	Fora do ar

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 38 na prática?

A Q.850 cause 38, Network out of order, indica que a rede não está funcionando corretamente e que a condição deve persistir por um período relativamente longo. A própria definição diz que tentar de novo imediatamente provavelmente não vai funcionar. Isso a separa da cause 41, que descreve uma falha passageira. Pela RFC 3398 (seção 7.2.4.1), a causa 38 vira SIP 503 Service Unavailable; no sentido inverso, o SIP 502 Bad Gateway volta como 38. Ela chega na REL do ISUP em links SS7, no DISCONNECT do ISDN e num `Reason: Q.850;cause=38` em troncos SIP. No Asterisk, `${HANGUPCAUSE}` fica em 38 e o CDR mostra hangupcause 38 quando o campo é gravado. Em LTE, o "cause code 38" das mensagens ESM é de outra tabela da 3GPP e não tem relação com esta causa.

Quando ela aparece

- Rompimento de fibra ou falha de transmissão na rede da operadora.
- SBC ou central da operadora fora do ar, com o tráfego sem rota alternativa.
- E1 com alarme no lado da operadora.
- Gateway intermediário que recebe um 502 de outro e o converte em 38.
- Link de internet do seu site caído, quando o SBC local responde em nome da rede.

Como diagnosticar

1. Veja quem gerou a causa: no `sngrep`, a resposta 503 ou 502 mostra o User-Agent ou o Server de quem respondeu.
2. Teste vários destinos. Se todos falham pelo mesmo tronco, a falha é de rede, não do destino.
3. Confira o link: perda de pacotes e latência até o IP de sinalização da operadora, com `ping` e `mtr`.
4. Verifique `pjsip show registrations` e o status do tronco no FreePBX, no Issabel ou no 3CX.
5. Num E1, `dahdi show status` mostra alarmes vermelhos (perda de sinal local) ou amarelos (o lado remoto não recebe o seu sinal).

O que mandar para a operadora

- Data, hora e fuso do início da falha, e se ela continua.
- Números de teste A e B e a lista de destinos que falharam.
- Call-ID, a resposta recebida e o Reason com cause=38.
- O resultado do `mtr` até o IP de sinalização da operadora.
- A designação do circuito ou a identificação do tronco, e os alarmes do E1, se houver.

Perguntas frequentes

Devo repetir a chamada quando recebo cause 38?

Repetir uma vez não faz mal, mas a definição da cause 38 diz que a condição deve durar, então tentativas imediatas em sequência tendem a falhar do mesmo jeito. Se houver rota alternativa, como outro tronco ou outra operadora, é melhor desviar o tráfego para ela enquanto a falha é tratada.

Qual a diferença entre cause 38 e cause 27?

A cause 27 (Destination out of order) diz que a interface até o destino falhou, ou seja, o problema está perto de quem recebe. A cause 38 diz que a própria rede está com falha. Pela RFC 3398, a 27 vira SIP 502 e a 38 vira SIP 503. Num 0800 que termina no seu PABX, a 27 aponta para o seu lado; a 38, para a

rede.

CAUSAS Q.850

Q.850 cause 41 (Temporary failure): o que significa

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** Q.850 cause 41 (Temporary failure) indica que a rede não está funcionando corretamente, mas que a condição deve durar pouco, então uma nova tentativa logo em seguida pode completar. É uma das causas mais vistas porque os SIP 400, 481, 500 e 503 viram 41. Procure a resposta SIP original para achar o motivo real.

Causa 41 na referência

Causa	41
Nome oficial (ITU-T Q.850)	Temporary failure
Classe	Recurso indisponível (34 a 47)
Resposta SIP pela RFC 3398	SIP 503 Service Unavailable

Como o Monitor trata a causa 41

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 41 aparece como: “uma falha temporária de rede”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 41 na prática?

A Q.850 cause 41, Temporary failure, indica que a rede não está funcionando corretamente e que a condição provavelmente não vai durar muito: o usuário pode tentar outra chamada quase imediatamente. Pela RFC 3398 (seção 7.2.4.1), a causa 41 vira SIP 503 Service Unavailable. O que a torna tão frequente é o caminho inverso: a mesma RFC converte em 41 os SIP 400 Bad Request, 481 Call/Transaction Does Not Exist, 500 Server Internal Error e 503 Service Unavailable. Assim, uma causa 41 no seu PABX pode ser, na origem, um erro de formato de mensagem ou uma falha interna de um servidor SIP. Ela chega na REL do ISUP, no DISCONNECT do ISDN e num `Reason: Q.850;cause=41`. No Asterisk, `${HANGUPCAUSE}` fica em 41, e o CDR mostra hangupcause 41 quando grava o campo.

Quando ela aparece

- Reinício ou sobrecarga momentânea de um SBC ou proxy da operadora.
- Erro 500 em algum servidor SIP no caminho, traduzido para 41 por um gateway.
- Mensagem SIP malformada (400) gerada pelo seu PABX, por exemplo com um cabeçalho inválido.
- Troca de servidor da operadora durante uma manutenção.
- Oscilação breve do link entre o seu site e a operadora.

Como diagnosticar

1. Tente de novo em alguns segundos. Se completar, registre o horário e acompanhe a frequência.
2. Ache a resposta SIP original no `sngrep` ou com `pjsip set logger on`: 400, 481, 500 e 503 levam a investigações diferentes.
3. Se for 400, leia a linha de status e o Warning: muitas operadoras dizem ali qual cabeçalho rejeitaram.
4. Se for 503, veja se há `Retry-After` e respeite o intervalo.
5. No 3CX, ative o Verbose logging para registrar a resposta completa no Activity Log.
6. Se as falhas se repetem no mesmo horário, cruze com as janelas de manutenção da operadora.

O que mandar para a operadora

- Data, hora e fuso de cada falha, e a frequência (por exemplo, quantas por hora).
- Números A e B.
- Call-ID e a linha de status SIP completa recebida, com o Reason e o Warning.
- Se uma nova tentativa logo em seguida completou.
- O pcap da chamada que falhou.

Perguntas frequentes

Se a cause 41 é temporária, preciso abrir chamado?

Uma ocorrência isolada, que completa na tentativa seguinte, normalmente não. Se a causa 41 se repete várias vezes por dia, ou sempre no mesmo destino, ela deixa de ser passageira na prática, e vale abrir chamado com os horários, os Call-IDs e a resposta SIP original de cada falha.

Um teste de chamada real separa falha passageira de falha que dura?

Uma chamada de teste real recebe a resposta SIP final da rede, como qualquer chamada. Quando ela falha, a tentativa é repetida antes de virar alerta. Assim, uma falha que some na repetição não gera aviso, e uma que persiste vira alerta enviado por e-mail.

CAUSAS Q.850

Q.850 cause 47 (Resource unavailable, unspecified): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 47 (Resource unavailable, unspecified) indica que algum recurso necessário para a chamada estava indisponível, sem que outra causa da classe de recursos se aplique. É uma falta de recurso genérica: canais de mídia, transcodificação, licenças ou capacidade de um gateway. Descubra qual equipamento gerou a causa e confira os limites dele.

Causa 47 na referência

Causa	47
Nome oficial (ITU-T Q.850)	Resource unavailable, unspecified
Classe	Recurso indisponível (34 a 47)
Resposta SIP pela RFC 3398	SIP 503 Service Unavailable

Como o Monitor trata a causa 47

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 47 na prática?

A Q.850 cause 47, Resource unavailable, unspecified, é usada para relatar um evento de recurso indisponível quando nenhuma outra causa dessa classe se aplica. É a causa genérica do grupo que inclui a 34 (sem circuito), a 38 (rede fora de serviço), a 41 (falha temporária) e a 42 (congestionamento). Pela RFC 3398 (seção 7.2.4.1), a causa 47 vira SIP 503 Service Unavailable, então só o cabeçalho `Reason: Q.850;cause=47` (RFC 6432) ou o trace TDM a distingue das outras. Ela chega na REL do ISUP em links SS7 e no DISCONNECT do ISDN. No Asterisk, `${HANGUPCAUSE}` fica em 47, e o CDR mostra hangupcause 47 quando o campo é gravado. Como é inespecífica, o mais útil é descobrir qual equipamento a gerou.

Quando ela aparece

- Gateway ou SBC sem recursos de DSP para transcodificar, por exemplo de G.729 para G.711.
- Servidor de mídia ou URA sem portas livres para tocar o anúncio.
- Licenças de chamadas simultâneas esgotadas num gateway ou SBC.
- Falta de memória ou de portas RTP livres num equipamento sobrecarregado.
- Gateway GSM ou E1 que usa 47 para qualquer porta indisponível.

Como diagnosticar

1. No `sngrep`, veja quem respondeu o 503 com cause=47, pelo User-Agent ou pelo Server.
2. Se foi o seu equipamento, confira a transcodificação: no Asterisk, `core show translation` mostra os caminhos entre codecs e `core show channels` as chamadas ativas.
3. Compare os codecs oferecidos no SDP com os aceitos do outro lado; usar o mesmo codec nas duas pontas evita transcodificação.
4. Verifique os limites de licença e a faixa de portas RTP (`rtpstart` e `rtpend` no `rtp.conf`).
5. Correlacione as falhas com os picos de chamadas simultâneas.

O que mandar para a operadora

- Data, hora e fuso das falhas.
- Números A e B.
- Call-ID, a linha `SIP/2.0 503 Service Unavailable` e o Reason com cause=47.
- Os codecs oferecidos no seu INVITE (linhas `m=` e `a=rtpmap` do SDP).
- Quantas chamadas simultâneas havia no seu lado no momento.

Perguntas frequentes

Qual a diferença entre cause 34 e cause 47?

A cause 34 diz especificamente que faltou circuito ou canal. A cause 47 diz que faltou algum recurso, sem dizer qual. Ambas viram SIP 503 pela RFC 3398. Quando o equipamento sabe que o problema é canal, deveria usar a 34; a 47 aparece quando o limite é outro, como transcodificação ou licença.

A cause 47 pode ser problema de codec?

Indiretamente, sim. Se não há codec em comum e o gateway precisa transcodificar, ele gasta DSP ou CPU com isso. Quando esse recurso acaba, a chamada pode falhar com cause 47. Já quando não existe nenhum codec aceitável, a causa esperada é outra, como a 65, que vira SIP 488 Not Acceptable Here.

CAUSAS Q.850

Q.850 cause 65 (Bearer capability not implemented): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 65 (Bearer capability not implemented) indica que o equipamento que encerrou não suporta a capacidade de portadora pedida, como uma chamada de dados ou um formato de mídia. Em troncos SIP, quase sempre é falta de codec em comum ou fax T.38 não aceito. Compare o SDP do INVITE com o que a operadora aceita.

Causa 65 na referência

Causa	65
Nome oficial (ITU-T Q.850)	Bearer capability not implemented
Classe	Serviço ou opção não implementado (65 a 79)
Resposta SIP pela RFC 3398	SIP 488 Not Acceptable Here

Como o Monitor trata a causa 65

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 65 na prática?

A Q.850 cause 65, Bearer capability not implemented, indica que o equipamento que envia a causa não implementa a capacidade de portadora solicitada. Na telefonia TDM, a portadora diz se a chamada é de voz, de áudio de 3,1 kHz ou de dados digitais sem restrição. Em SIP, esse papel fica com a descrição de mídia no SDP. Pela RFC 3398 (seção 7.2.4.1), a causa 65 vira SIP 488 Not Acceptable Here. No sentido inverso, um 488 ou um 606 Not Acceptable cujo Warning trate de capacidade de portadora volta como 65; sem esse Warning, o padrão é 31. A causa aparece na REL do ISUP, no DISCONNECT do ISDN e num `Reason: Q.850;cause=65`. No Asterisk, `${HANGUPCAUSE}` fica em 65, e o CDR mostra hangupcause 65 quando grava o campo.

Quando ela aparece

- Nenhum codec em comum: o PABX oferece só G.729 e a operadora aceita só G.711 A-law (PCMA), o padrão no Brasil.
- Re-INVITE para fax T.38 num tronco que não aceita T.38.
- Chamada de dados ISDN (64 kbit/s sem restrição) enviada para um destino só de voz.
- Vídeo ou outra mídia oferecida num tronco só de áudio, sem uma linha de áudio compatível.
- Gateway antigo que não implementa o formato de portadora pedido.

Como diagnosticar

1. No `sngrep`, abra o INVITE e veja as linhas `m=audio` e `a=rtpmap` do SDP.
2. Leia o Warning do 488: os códigos 304 (Media type not available) e 305 (Incompatible media format) apontam para a mídia.
3. No Asterisk, confira `allow` e `disallow` do endpoint com `pjsip show endpoint nome-do-tronco` e garanta que `alaw` está na lista.
4. No 3CX, confira a ordem de codecs configurada no tronco e compare com a lista da operadora.
5. Para fax, teste com T.38 desligado (G.711 em passthrough) ou confirme com a operadora se T.38 é suportado.
6. Num E1 ISDN, `pri set debug on span 1` mostra o Bearer Capability enviado no SETUP.

O que mandar para a operadora

- Data, hora e fuso das tentativas.
- Números A e B e o tipo de chamada (voz, fax, dados).
- Call-ID, a linha `SIP/2.0 488 Not Acceptable Here`, o Warning e o Reason.
- O SDP completo do INVITE ou do re-INVITE recusado.
- O pedido explícito da lista de codecs e do suporte a T.38 no tronco.

Perguntas frequentes

Cause 65 é a mesma coisa que SIP 488?

Quase. Pela RFC 3398, a cause 65 vira SIP 488 Not Acceptable Here, mas o 488 só volta como cause 65 quando o Warning fala de capacidade de portadora; sem isso, vira cause 31. Então um 488 pode chegar à telefonia como 65 ou como 31, dependendo do que o equipamento que recusou escreveu no Warning.

Por que o fax falha com cause 65 e a voz funciona?

Porque o fax costuma trocar a mídia no meio da chamada, com um re-INVITE pedindo T.38. Se o tronco ou o gateway do outro lado não aceita T.38, ele recusa a nova mídia, e a causa pode ser 65. A voz em G.711 continua funcionando porque usa um formato que os dois lados aceitam.

CAUSAS Q.850

Q.850 cause 88 (Incompatible destination): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

Resposta curta: Q.850 cause 88 (Incompatible destination) indica que o destino recebeu um pedido de chamada com atributos de compatibilidade que ele não consegue atender, como o tipo de terminal ou a taxa de dados. É comum ao misturar voz, fax e dados. Confira o tipo de chamada enviado, a portadora pedida e que terminal está ligado no número.

Causa 88 na referência

Causa	88
Nome oficial (ITU-T Q.850)	Incompatible destination
Classe	Mensagem inválida (81 a 95)
Resposta SIP pela RFC 3398	SIP 503 Service Unavailable

Como o Monitor trata a causa 88

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 88 na prática?

A Q.850 cause 88, Incompatible destination, indica que o equipamento de destino recebeu um pedido de chamada com compatibilidade de camada baixa, compatibilidade de camada alta ou outros atributos, como taxa de dados, que ele não consegue atender. Diferente da cause 65, que fala de portadora não implementada, a 88 aponta um descasamento entre o que a chamada pede e o tipo de terminal no destino. Pertence à classe de mensagens inválidas da Q.850. Pela RFC 3398 (seção 7.2.4.1), a causa 88 vira SIP 503 Service Unavailable, então do lado SIP ela se confunde com falhas de capacidade. Ela chega na REL do ISUP, no DISCONNECT do ISDN e num `Reason: Q.850;cause=88` (RFC 6432). No Asterisk, `${HANGUPCAUSE}` fica em 88, e o CDR mostra hangupcause 88 quando grava o campo.

Quando ela aparece

- Chamada de dados ISDN (64 kbit/s sem restrição) para um telefone analógico ou um destino só de voz.
- Chamada de voz para uma linha configurada só para fax ou dados.
- Gateway ISDN que repassa uma compatibilidade de camada alta (HLC) que o terminal de destino não aceita.
- Terminais ISDN antigos com configuração específica, como fax grupo 4 ou videofone.
- Gateways SIP-ISDN que montam o SETUP com uma portadora diferente da esperada pelo destino.

Como diagnosticar

1. Num E1 ISDN, ative `pri set debug on span 1` e leia no SETUP os campos Bearer Capability, Low Layer Compatibility e High Layer Compatibility.
2. Confirme com o dono do número que tipo de terminal está ligado nele.
3. No gateway SIP-ISDN, verifique como ele preenche a portadora: muitos têm opção para forçar voz (speech) ou áudio de 3,1 kHz.

4. No Asterisk com DAHDI, a variável de canal `TRANSFERCAPABILITY` define a portadora das chamadas de saída; confirme o valor usado.
5. No `sngrep`, veja se o 503 veio com `Reason: Q.850;cause=88`, para separá-lo de um 503 por falta de capacidade.

O que mandar para a operadora

- Data, hora e fuso das tentativas.
- Números A e B e o tipo de chamada pretendido (voz, fax, dados).
- Call-ID, a resposta `SIP/2.0 503 Service Unavailable` e o Reason com cause=88.
- O trace do SETUP com o Bearer Capability, se a chamada sai por E1 ISDN.
- O pedido para confirmar o tipo de terminal provisionado no número de destino.

Perguntas frequentes

Por que a cause 88 vira SIP 503 e não 488?

Porque é o que a tabela da RFC 3398 define: a cause 88 vira SIP 503 Service Unavailable, enquanto a cause 65 vira 488. Na prática, isso faz um problema de compatibilidade parecer um problema de capacidade no lado SIP. Só o cabeçalho Reason com cause=88, ou o trace TDM, mostra o motivo real.

A cause 88 aparece em troncos SIP puros?

Raramente. Ela nasce em redes com sinalização ISDN ou ISUP, onde a chamada carrega atributos de compatibilidade. Num tronco SIP, você normalmente a vê quando a chamada atravessa um gateway para a rede TDM e o destino lá rejeita os atributos. Se o trecho for todo SIP, o comum é um 488 com Warning.

CAUSAS Q.850

Q.850 cause 102 (Recovery on timer expiry): o que significa

Por Equipe 2N5 Atualizado em 20 de outubro de 2026

> **Resposta curta:** Q.850 cause 102 (Recovery on timer expiry) indica que um procedimento de recuperação de erro começou porque um temporizador do protocolo expirou: alguma mensagem esperada não chegou a tempo. Em troncos SIP costuma ser um INVITE sem resposta, por firewall, NAT, SIP ALG ou pacote UDP grande demais. Siga a sinalização e veja onde ela para.

Causa 102 na referência

Causa	102
Nome oficial (ITU-T Q.850)	Recovery on timer expiry
Classe	Erro de protocolo (96 a 111)
Resposta SIP pela RFC 3398	SIP 504 Server Time-out

Como o Monitor trata a causa 102

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora. Nas telas em português, a causa 102 aparece como: “um temporizador

do protocolo expirou”.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 102 na prática?

A Q.850 cause 102, Recovery on timer expiry, indica que um procedimento foi iniciado pela expiração de um temporizador, dentro dos procedimentos de tratamento de erro. Em outras palavras, um equipamento esperou uma mensagem que não veio e desistiu. Pertence à classe de erros de protocolo. Pela RFC 3398 (seção 7.2.4.1), a causa 102 vira SIP 504 Server Time-out (a RFC escreve “504 Gateway timeout”); no sentido inverso, o SIP 408 Request Timeout e o 504 voltam como 102. Em SIP, o temporizador típico é o Timer B do INVITE, de 64 vezes o T1, ou 32 segundos com o T1 padrão de 500 ms (RFC 3261). A causa chega na REL do ISUP e num `Reason: Q.850;cause=102`. No Asterisk, `${HANGUPCAUSE}` fica em 102, e o CDR mostra hangupcause 102 quando grava o campo.

Quando ela aparece

- Firewall bloqueando a resposta da operadora ou o próprio INVITE de saída.
- NAT sem mapeamento para a porta SIP, ou SIP ALG do router alterando as mensagens.
- INVITE com SDP grande demais (muitos codecs) que passa do MTU, é fragmentado em UDP e tem um fragmento perdido.
- DNS do tronco resolvendo para um IP antigo da operadora.
- Servidor SIP intermediário que não responde e não manda nem 100 Trying.

Como diagnosticar

1. No `sngrep`, veja se o INVITE foi retransmitido várias vezes sem resposta: isso confirma que nada voltou.
2. Capture na interface externa com `tcpdump -i any -s 0 -w chamada.pcap port 5060` para saber se o INVITE saiu e se alguma resposta chegou.
3. Desative o SIP ALG do router e confira as regras de NAT e firewall para os IPs da operadora.
4. Se o INVITE passa de cerca de 1.300 bytes, reduza os codecs oferecidos ou use TCP no tronco.
5. Confira o DNS do domínio do tronco e o IP para onde o INVITE está indo de fato.
6. No 3CX, o Activity Log com Verbose logging mostra se o tronco recebeu alguma resposta antes do timeout.

O que mandar para a operadora

- Data, hora e fuso das tentativas.
- Números A e B.
- Call-ID e o que você recebeu: nenhuma resposta, `SIP/2.0 408 Request Timeout` ou 504, com o Reason.
- O IP público de origem e o IP de destino para onde o INVITE foi enviado.
- O pcap mostrando as retransmissões do INVITE.

Perguntas frequentes

Por que a chamada demora cerca de 32 segundos antes de falhar com cause 102?

Porque o INVITE em SIP sobre UDP é retransmitido até o Timer B expirar, e o Timer B vale 64 vezes o T1. Com o T1 padrão de 500 ms, isso dá 32 segundos. Se nenhuma resposta final chega nesse intervalo, a transação falha, e o gateway informa a cause 102 para o lado da telefonia.

Uma chamada de teste real ajuda com falhas de timeout?

Ajuda, porque ela passa pelo mesmo caminho de sinalização de uma chamada comum e recebe a resposta SIP final, ou a falta dela. Uma falha é repetida antes de virar alerta, o que evita aviso por um pacote perdido isolado, e o alerta segue por e-mail.

CAUSAS Q.850

Q.850 cause 127 (Interworking, unspecified): o que significa

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Q.850 cause 127 (Interworking, unspecified) indica que a chamada passou por uma interconexão com uma rede que não fornece causas para o que faz, então o motivo exato é desconhecido. Não aponta um defeito específico. É comum em gateways entre SIP, ISDN e sinalização R2. Descubra em que trecho a chamada falhou e qual resposta veio dali.

Causa 127 na referência

Causa	127
Nome oficial (ITU-T Q.850)	Interworking, unspecified
Classe	Interfuncionamento (127)
Resposta SIP pela RFC 3398	SIP 500 Server Internal Error

Como o Monitor trata a causa 127

Quando a operadora informa a causa Q.850 no cabeçalho `Reason` da resposta SIP, o Monitor a guarda junto com o código SIP em cada chamada de teste, e ela aparece na evidência do incidente, pronta para o chamado na operadora.

Como qualquer falha, uma chamada de teste lida como Fora do ar é repetida 3 vezes, a cada 2 minutos, e só 4 falhas seguidas abrem um incidente.

O que significa a causa 127 na prática?

A Q.850 cause 127, Interworking, unspecified, indica que houve interfuncionamento com uma rede que não fornece causas para as ações que toma, de modo que a causa exata da mensagem não é conhecida. É a única causa da classe de interfuncionamento na Q.850. Pela RFC 3398 (seção 7.2.4.1), a causa 127 vira SIP 500 Server Internal Error. No sentido inverso, várias respostas SIP sem equivalente na telefonia voltam como 127: 413, 414, 416, 420, 421, 423, 505 e 513. Ou seja, problemas de extensões SIP (cabeçalho Require), de tamanho de mensagem ou de versão podem chegar à telefonia como 127. A causa aparece na REL do ISUP, num `Reason: Q.850;cause=127` (RFC 6432) e, no Asterisk, em `${HANGUPCAUSE}`, além do campo hangupcause do CDR quando ele é gravado.

Quando ela aparece

- Chamada que atravessa um trecho com sinalização R2 MFC, ainda comum em E1 no Brasil, que não transporta causas Q.850.
- Gateway que recebe SIP 420 Bad Extension ou 421 Extension Required por causa de `Require: 100rel` ou `Require: timer`.
- Mensagem SIP grande demais, respondida com 513 Message Too Large.
- Request-URI longo demais (414) ou esquema de URI não suportado (416).
- Equipamentos de fabricantes diferentes em sequência, cada um traduzindo a causa do anterior.

Como diagnosticar

1. Siga a chamada trecho a trecho no `sngrep` ou no pcap e encontre a primeira resposta de erro.
2. Se a primeira resposta for 420 ou 421, confira os cabeçalhos Require e Supported do INVITE; no PJSIP, teste com `100rel` e `timers` desligados no endpoint.
3. Se for 513, reduza o tamanho do INVITE (menos codecs ou cabeçalhos) ou use TCP.
4. Num E1 com R2, veja no gateway qual sinal B o destino devolveu e como o gateway o traduziu.
5. No 3CX, o Activity Log com Verbose logging mostra a resposta exata do tronco antes da tradução.
6. Peça ao responsável por cada gateway a causa ou a resposta que ele recebeu antes de gerar a 127.

O que mandar para a operadora

- Data, hora e fuso das tentativas.
- Números A e B.
- Call-ID, a linha `SIP/2.0 500 Server Internal Error` e o Reason com cause=127.
- O INVITE completo, com Require, Supported e o tamanho da mensagem.
- O pedido explícito da resposta ou do sinal original no trecho em que a operadora fez a interconexão.

Perguntas frequentes

Cause 127 quer dizer que a operadora tem um erro interno?

Não necessariamente. Pela RFC 3398, a cause 127 vira SIP 500 Server Internal Error, o que parece falha interna, mas a causa só diz que a chamada passou por uma rede que não informou o motivo. O erro real pode estar em qualquer trecho, inclusive numa extensão SIP recusada ou numa mensagem grande demais.

Por que vejo cause 127 em troncos E1 com R2?

Porque a sinalização R2 MFC não carrega causas Q.850: ela usa sinais B, como assinante livre, ocupado ou congestionamento. O gateway que liga o R2 ao ISDN ou ao SIP precisa traduzir esses sinais, e quando não há tradução clara, ou quando o destino simplesmente libera a chamada, ele pode usar a cause 127.

Glossário

Definições curtas e exemplos dos termos de telefonia e voz sobre IP: MOS, MOS-LQO, jitter, SIP ALG, URA, DDR, 0800, tronco SIP, SLA e outros.

GLOSSÁRIO

ASR e ACD: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

> **Resposta curta:** ASR (Answer Seizure Ratio) é a porcentagem de tentativas de chamada que foram atendidas, e ACD (Average Call Duration) é a duração média das chamadas atendidas. Os dois saem dos registros de chamadas (CDR) da operadora ou do PABX.

Em inglês: ASR (Answer Seizure Ratio) and ACD (Average Call Duration)

O que são ASR e ACD?

ASR e ACD são os dois indicadores mais antigos da qualidade de uma rota de voz, calculados a partir dos registros de chamadas, os CDR.

O **ASR** (Answer Seizure Ratio, da recomendação ITU-T E.411) é a porcentagem das tentativas de chamada que foram atendidas: chamadas atendidas ÷ chamadas tentadas × 100. O **ACD** (Average Call Duration) é a duração média das chamadas atendidas: tempo total de conversa ÷ número de chamadas atendidas.

As operadoras definem o ASR de formas ligeiramente diferentes. Algumas tiram do cálculo as chamadas que o destino recusou, como ocupado, e a diferença muda o número. Confira a definição no contrato antes de comparar rotas.

O que uma variação indica

- **ASR em queda brusca:** a rota pode ter parado de completar chamadas, total ou parcialmente. É o sinal para olhar os códigos de resposta, como SIP 503.
- **ACD muito curto:** as chamadas atendem e caem logo, o que costuma indicar áudio mudo, SIP ALG ou problema de codec.
- **ACD muito longo:** ligações presas, por exemplo uma chamada que não desligou do outro lado.

Os dois olham o conjunto, e não uma chamada. Eles escondem a falha do 0800 que ninguém ligou de madrugada e não dizem o que ouviu quem ligou.

Na prática

Em um dia, um tronco SIP fez 1.000 tentativas de chamada e 600 foram atendidas, com 30.000 segundos de conversa no total (números ilustrativos).

Indicador	Cálculo	Resultado
ASR	600 ÷ 1.000 × 100	60%
ACD	30.000 s ÷ 600	50 s

Se amanhã o ASR cair para 20% sem mudança no tráfego, a rota tem um problema. Se cair para 20% porque a campanha ligou para uma lista ruim, o tronco está bem.

Como o Monitor usa isso

O Monitor não calcula ASR nem ACD, porque não analisa o tráfego dos seus clientes. Ele faz o caminho contrário: liga para um número que você controla, de fora, e informa se a chamada completou, com o código SIP quando não completa. Use o ASR do seu CDR para ver que algo mudou e a chamada de teste para saber se o circuito ainda completa. Veja o monitoramento sintético, o post dial delay e o monitoramento de troncos SIP e VoIP.

Perguntas frequentes

Qual é um ASR bom?

Não existe um número bom para todos. O ASR depende do tipo de tráfego: chamadas para clientes que não atendem baixam o índice sem nenhuma falha de rede. Compare o ASR de uma rota com o dela mesma em dias parecidos, e investigue quando ele cai de repente, porque a queda brusca é o sinal útil.

Um ASR baixo significa que o tronco está com problema?

Nem sempre. Um ASR baixo pode vir de falha do tronco, mas também de um número chamado ocupado, de uma campanha para uma lista ruim ou de uma rota barata e instável. O ASR avisa que algo mudou; uma chamada de teste a um número que você controla mostra se o tronco ainda completa chamadas.

GLOSSÁRIO

Codecs de voz: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Codecs de voz são os algoritmos que codificam a voz em dados digitais para transmissão numa chamada e a decodificam no destino, como G.711, G.729 e Opus.

Em inglês: voice codecs (G.711, G.729, Opus)

O que são codecs de voz?

Codec de voz é o algoritmo que transforma o som da voz em bits para viajar pela rede e reconstrói o som do outro lado. Toda chamada VoIP usa um codec, e as duas pontas precisam usar o mesmo. A escolha define quanta banda a chamada consome, a qualidade do áudio e o quanto ela resiste a perda de pacotes.

Os três codecs mais encontrados em telefonia são:

- G.711 (ITU-T): não comprime, amostra a voz a 8 kHz e gera 64 kbit/s. Tem duas variantes, µ-law e A-law; o Brasil usa A-law (PCMA). É o padrão de fato em troncos SIP.
- G.729 (ITU-T): comprime para 8 kbit/s. Economiza banda, mas perde qualidade e distorce tons DTMF enviados dentro do áudio.
- Opus (RFC 6716): codec aberto e adaptativo, de 6 a 510 kbit/s, com banda de até 48 kHz. Comum em WebRTC e aplicativos.

O codec é combinado no início da chamada pelo SDP, dentro da mensagem SIP. Quem liga oferece uma lista de codecs; quem atende escolhe um da lista. Se nenhum serve, a chamada falha.

Na prática

Banda por sentido na camada IP, com pacotes de 20 ms (40 bytes de cabeçalho IP, UDP e RTP por pacote, sem contar Ethernet):

Codec	Áudio	Carga por pacote	Banda IP por sentido
G.711	64 kbit/s	160 bytes	80 kbit/s
G.729	8 kbit/s	20 bytes	24 kbit/s
Opus	6 a 510 kbit/s	variável	variável

Um link que carrega 10 chamadas simultâneas em G.711 precisa de cerca de 800 kbit/s em cada sentido só para a voz. Em G.729, cerca de 240 kbit/s. Repare que, no G.729, o cabeçalho pesa o dobro do áudio.

Como o Monitor usa isso

Quando o destino não aceita nenhum dos codecs oferecidos na chamada de teste, a chamada termina com SIP 488 e o Monitor conta o circuito como fora do ar. Veja monitoramento de troncos SIP.

Perguntas frequentes

Qual codec usar em VoIP: G.711 ou G.729?

O G.711 não comprime a voz e entrega a qualidade da telefonia clássica, ao custo de 64 kbit/s de áudio por sentido. O G.729 usa 8 kbit/s, mas perde qualidade e atrapalha o envio de DTMF dentro do áudio. Com banda sobrando, o G.711 é a escolha mais simples. Com banda curta, o G.729 cabe melhor. O que importa é que as duas pontas aceitem o mesmo.

O que acontece quando as duas pontas não têm codec em comum?

A negociação no SDP falha e a chamada não se completa. Normalmente o destino responde com SIP 488 Not Acceptable Here. Um SBC no caminho pode resolver transcodificando, mas cada transcodificação custa processamento e um pouco de qualidade. Para corrigir de vez, alinhe a lista de codecs do PABX com a da operadora.

GLOSSÁRIO

DDR: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** DDR (Discagem Direta a Ramal) é o serviço que associa números públicos a ramais de um PABX, para que quem liga de fora chegue direto ao ramal sem passar por telefonista ou URA.

Em inglês: DID (Direct Inward Dialing)

O que é DDR?

DDR (Discagem Direta a Ramal, ou DID em inglês) é o serviço da operadora que entrega à empresa uma faixa de números públicos, como (11) 3456-7000 a 7099, e permite que cada número chegue direto a um ramal do PABX IP. Quem liga para (11) 3456-7012 fala com o ramal 7012 sem passar pela recepção ou pela URA.

Ramal é o número interno de cada telefone, softphone ou grupo dentro da central. O DDR é a ponte entre o número público e esse ramal.

A faixa DDR chega à empresa por um tronco SIP ou um tronco E1. Em cada chamada, a operadora informa qual número foi discado: no SIP, no Request-URI e no cabeçalho To; no E1, no número de B. O PABX lê esse número, geralmente os últimos quatro dígitos, e procura o ramal correspondente no plano de discagem.

A falha mais comum está nesse acordo de dígitos. Se a operadora muda o formato enviado, o PABX deixa de reconhecer o número: a chamada vai para a regra padrão, cai na telefonista ou é recusada. O tronco continua em pé, o ramal continua registrado, e só a ligação de fora revela o problema.

Na prática

Uma faixa DDR de 100 números com o PABX lendo quatro dígitos:

Número discado	Dígitos recebidos	Destino no PABX
(11) 3456-7000	7000	URA da recepção
(11) 3456-7012	7012	Ramal 7012, financeiro
(11) 3456-7050	7050	Grupo de suporte
(11) 3456-7012, depois de mudança na operadora	+551134567012	Regra padrão: telefonista

Na última linha, nada mudou dentro da empresa, mas o financeiro deixou de receber ligações diretas. Ligações internas para o 7012 continuam funcionando, o que atrasa a percepção do problema. Por isso o teste precisa vir de fora, pelo número público.

Como o Monitor usa isso

Qualquer número discável pode ser monitorado, inclusive ramais alcançáveis por DDR. O teste disca o número público do ramal, como um cliente faria, e passa pela operadora, pelo tronco e pelo plano de discagem do PABX. Veja o monitoramento de troncos SIP.

Perguntas frequentes

Qual a diferença entre DDR e ramal?

O ramal é o número interno de um telefone dentro do PABX, como 7012, discado entre colegas. O DDR é o número público que leva a esse ramal, como (11) 3456-7012, discado por quem está fora. Todo DDR aponta para um ramal, um grupo ou uma URA, mas nem todo ramal tem DDR: muitos só recebem ligações transferidas pela recepção.

Por que a ligação para o DDR cai na telefonista?

Normalmente porque o PABX não reconheceu o número recebido e usou a regra padrão de entrada. Isso acontece quando a operadora passa a enviar outra quantidade de dígitos, por exemplo o número completo com +55 em vez dos quatro finais, ou quando o ramal foi removido sem atualizar o plano de

discagem. O registro de chamadas do PABX mostra o número que chegou.

GLOSSÁRIO

DTMF: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** DTMF (Dual-Tone Multi-Frequency) é o sistema que representa cada tecla do telefone pela soma de duas frequências, usado para discar e para escolher opções em URAs.

Em inglês: DTMF (Dual-Tone Multi-Frequency)

O que é DTMF?

DTMF (Dual-Tone Multi-Frequency) é o sistema de tons das teclas do telefone. Cada tecla gera duas frequências ao mesmo tempo, uma de um grupo baixo e outra de um grupo alto, e quem recebe identifica a tecla pela combinação. É com DTMF que se navega numa URA, se digita um ramal ou se confirma uma senha por telefone.

	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Na telefonia tradicional, os tons iam dentro do próprio áudio. No VoIP há três formas de transportá-los:

- No áudio (in-band): o tom vai como som dentro do RTP. Funciona bem em G.711, mas codecs comprimidos como o G.729 deformam o tom e a tecla se perde.
- RFC 4733 (telephone-event): cada tecla vira um evento próprio no fluxo RTP, com um tipo de carga combinado no SDP. Substitui a RFC 2833 e é o método mais comum em troncos SIP.
- SIP INFO: a tecla viaja como uma mensagem SIP, fora do áudio. Depende de todos os equipamentos no caminho repassarem a mensagem.

Na prática

Ao apertar a tecla 5, o telefone gera 770 Hz e 1336 Hz juntos. Um cliente liga para o 0800 da empresa e a URA diz “para financeiro, digite 2”. O que acontece depende do método:

Telefone envia	URA espera	Resultado
RFC 4733	RFC 4733	Tecla 2 reconhecida
No áudio, G.711	No áudio	Tecla 2 reconhecida
No áudio, G.729	No áudio	Tom deformado, tecla ignorada
RFC 4733	No áudio	Tecla nunca chega

Como o Monitor usa isso

Em circuitos de tom de teste ou eco, o Monitor envia tons de teste e confere se eles voltam. Em URAs, a chamada de teste escuta a saudação esperada. Veja monitoramento de 0800 e URA.

Perguntas frequentes

Por que a URA não reconhece as teclas digitadas?

Quase sempre porque as duas pontas usam métodos diferentes de DTMF. Se o telefone envia RFC 4733 e a URA espera os tons dentro do áudio, ou o contrário, os dígitos se perdem. Codecs comprimidos como o G.729 também deformam tons enviados no áudio. Confira no SDP se o telephone-event foi negociado e use o mesmo método nas duas pontas.

Qual o melhor método de DTMF em VoIP?

Na maioria dos troncos SIP, a RFC 4733, que manda cada tecla como um evento no fluxo RTP, com tipo de carga negociado no SDP. Ela não depende do codec e chega no mesmo ritmo do áudio. O DTMF no áudio só é confiável com G.711, e o SIP INFO exige que todos os equipamentos no caminho o repassem.

GLOSSÁRIO

Early media: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Early media é o áudio enviado ao chamador antes de a chamada ser atendida, normalmente após uma resposta SIP 183 Session Progress, como o tom de chamada ou uma mensagem da operadora.

Em inglês: early media (SIP 183 Session Progress)

O que é early media?

Early media é o áudio que o chamador ouve antes de a chamada ser atendida. No SIP, ele normalmente começa com uma resposta 183 Session Progress que traz um SDP: a rede abre o fluxo RTP antes do 200 OK e toca algo para quem ligou. O modelo está descrito na RFC 3960.

O conteúdo pode ser o tom de chamada gerado pela operadora, uma música de espera, um aviso como “esta chamada pode ser gravada” ou uma mensagem de erro, como “o número chamado não existe” ou “este telefone está desligado ou fora da área de cobertura”. Para o ouvido humano, tudo isso é som. Para a sinalização, a chamada ainda não foi atendida.

Isso cria uma armadilha para qualquer teste automático. Se o teste considera “ouvi áudio” como sucesso, uma mensagem da operadora dizendo que o número está fora de serviço passa como chamada boa. O que define o atendimento é o 200 OK, e o que define se o destino certo respondeu é o conteúdo do áudio.

Na prática

Uma chamada para um número cujo tronco caiu pode correr assim:

Tempo	Mensagem	O que o chamador ouve
0,0 s	INVITE enviado	Nada
0,2 s	100 Trying	Nada
1,1 s	183 Session Progress com SDP	“O número chamado não está disponível”
9,0 s	480 Temporarily Unavailable	Fim da chamada

Em nenhum momento houve 200 OK. Um teste que só procura áudio veria 8 segundos de voz e marcaria a linha como funcionando. A resposta final, 480, conta a história real. Algumas operadoras chegam a atender com 200 OK só para tocar a mensagem, e aí só o conteúdo do áudio revela a falha.

Como o Monitor usa isso

Para um circuito de saudação, uma mensagem gravada no lugar do toque de chamada geralmente é a operadora falando por um número que ela não conseguiu alcançar, e o Monitor conta isso como falha. Veja monitoramento de 0800 e URA.

Perguntas frequentes

Qual a diferença entre 180 Ringing e 183 Session Progress?

O 180 Ringing apenas avisa que o destino está tocando; quem liga gera o tom de chamada localmente. O 183 Session Progress costuma trazer um SDP e abrir o áudio antes do atendimento, para que a rede toque o próprio tom, um anúncio ou uma mensagem de erro. Nenhum dos dois significa que a chamada foi atendida.

Ouvir áudio significa que a chamada foi atendida?

Não. Com early media, o chamador ouve som antes de qualquer 200 OK. Esse som pode ser o tom de chamada, uma música ou uma gravação como "o número chamado não está disponível". A chamada só foi atendida quando chega a resposta 200 OK ao INVITE.

GLOSSÁRIO

Janela de manutenção: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Janela de manutenção é um período agendado e combinado em que um serviço pode ficar indisponível para trabalho planejado, sem que as falhas desse intervalo sejam tratadas como incidente.

Em inglês: maintenance window

O que é uma janela de manutenção?

Janela de manutenção é um intervalo de tempo marcado com antecedência para trabalho que pode derrubar o serviço: atualizar o PABX IP, trocar o firewall, migrar um tronco SIP de operadora ou mudar o roteamento de um 0800. Durante a janela, uma queda é esperada e não deve ser tratada como incidente.

A janela resolve dois problemas. O primeiro é operacional: sem ela, cada teste que falha durante a manutenção dispara alertas, acorda o plantão e treina a equipe a ignorar avisos. O segundo é contratual: muitos contratos de SLA separam a indisponibilidade programada, avisada antes, da indisponibilidade não programada.

Uma boa janela tem início e fim definidos, cobre apenas os circuitos afetados e termina com uma verificação. Cobrir tudo “por garantia” esconde falhas reais em linhas que nada tinham a ver com a manutenção. E uma janela que termina sem teste deixa passar o caso mais comum: a manutenção acabou, mas a linha não voltou.

Na prática

A operadora vai migrar o tronco SIP da matriz no sábado, das 23:00 à 01:00. A empresa tem três circuitos monitorados:

Circuito	Na janela?	Falha às 00:30	Falha às 01:15
0800 que chega pelo tronco da matriz	Sim	Sem incidente	Incidente
Ramal DDR na matriz	Sim	Sem incidente	Incidente
URA da filial, em outro tronco	Não	Incidente	Incidente

A falha da filial às 00:30 é real e precisa alertar, mesmo com a manutenção em andamento na matriz. Já a falha das 01:15 nos circuitos da matriz indica que a migração terminou sem que o tronco voltasse.

Como o Monitor usa isso

Uma janela de manutenção cobre os circuitos escolhidos em um horário definido. Falhas que acontecem dentro dela não abrem incidentes, e os demais circuitos continuam alertando normalmente. Quando a janela termina, os testes seguintes voltam a abrir incidentes se a falha continuar. Veja alertas e escalonamento.

Perguntas frequentes

Manutenção programada conta no SLA?

Depende do contrato. É comum que a manutenção programada, avisada com a antecedência definida no acordo e feita dentro de um horário combinado, fique fora do cálculo de disponibilidade. Fora dessas condições, a indisponibilidade costuma contar normalmente. Vale ler a cláusula com atenção: antecedência do aviso, duração máxima, quantas janelas por mês e quem pode solicitá-las.

Qual o melhor horário para uma janela de manutenção?

O horário com menos chamadas para os circuitos afetados, que nem sempre é a madrugada. Um 0800 de suporte 24 horas pode ter movimento à noite, enquanto uma URA de agendamento quase não recebe ligações no domingo. Confira o volume de chamadas antes de marcar, deixe uma margem para atrasos e teste as linhas logo depois que a janela termina.

GLOSSÁRIO

Jitter: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Jitter é a variação no intervalo de chegada dos pacotes de uma chamada de voz, que obriga o receptor a segurar pacotes num buffer antes de tocar o áudio.

Em inglês: jitter

O que é jitter?

Jitter é a variação no tempo de chegada dos pacotes de voz. Numa chamada VoIP, o telefone envia um pacote RTP em intervalos fixos, normalmente a cada 20 ms. Se a rede entregasse todos com o mesmo atraso, eles chegariam também a cada 20 ms. Na prática, filas em roteadores, Wi-Fi e enlaces congestionados fazem uns chegarem antes e outros depois. Essa irregularidade é o jitter.

Para tocar a voz sem engasgos, o receptor guarda os pacotes num buffer de jitter e os libera no ritmo certo. O buffer resolve variações pequenas, mas cobra um preço: cada milissegundo de buffer é um milissegundo a mais de atraso na conversa. Se um pacote chega depois do momento em que deveria tocar, ele é descartado, e o ouvinte percebe um corte, igual ao de uma perda de pacotes.

O RTCP, o protocolo de controle que acompanha o RTP, informa uma estimativa do jitter de chegada calculada pelo método da RFC 3550.

Latência

Latência é o atraso de um pacote de uma ponta à outra, sem considerar a variação. A ITU-T G.114 recomenda não passar de 400 ms de atraso em um sentido para o planejamento geral de redes e observa que, abaixo de 150 ms, a maioria das aplicações tem interatividade praticamente transparente. Acima disso, as pessoas começam a falar ao mesmo tempo e a esperar a resposta do outro lado. O atraso total soma a rede, o codec e o buffer de jitter.

Na prática

Um telefone envia quatro pacotes, um a cada 20 ms. Veja quando chegam:

Pacote	Enviado (ms)	Chegou (ms)	Atraso (ms)
1	0	40	40
2	20	75	55
3	40	72	32
4	60	110	50

O atraso varia entre 32 e 55 ms, uma oscilação de 23 ms. Com um buffer de 30 ms, todos tocam no tempo, e o atraso percebido fica em torno de 70 ms, bem abaixo dos 150 ms da G.114. Se um quinto pacote chegasse com 100 ms de atraso, ele estouraria o buffer e viraria um corte no áudio.

Como o Monitor usa isso

O agente de circuitos de dados que a 2N5 instala em cada site mede a latência, a perda de pacotes e o jitter do link de internet daquele local, e mostra gráficos das últimas 100 horas. Assim dá para ver se o link estava instável no horário em que a voz piorou. Veja circuitos de dados.

Perguntas frequentes

Qual o jitter aceitável em VoIP?

Não existe um único limite em norma. O que importa é se o jitter cabe no buffer do telefone ou do PABX. Um buffer de 60 ms absorve variações menores que isso, mas acrescenta 60 ms ao atraso da chamada. Quando o jitter passa do tamanho do buffer, pacotes chegam tarde demais, são descartados e o efeito é o mesmo de uma perda de pacotes.

Jitter e latência são a mesma coisa?

Não. Latência é quanto tempo um pacote leva de uma ponta à outra. Jitter é o quanto esse tempo varia de um pacote para o seguinte. Uma rede pode ter latência alta e estável, com pouco jitter, ou latência baixa com muito jitter. A primeira atrapalha a conversa; a segunda corta o áudio.

GLOSSÁRIO

Monitoramento sintético: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

> **Resposta curta:** Monitoramento sintético, ou de chamadas sintéticas, é o teste em que um sistema faz chamadas reais, em horários marcados, para um número ou circuito e registra se a chamada completou, o que atendeu e como estava o áudio.

Em inglês: synthetic monitoring (synthetic calls)

O que é monitoramento sintético?

Monitoramento sintético é monitorar um serviço fazendo o que um usuário faria, em vez de esperar que um usuário apareça. Na telefonia, isso são as chamadas sintéticas: ligações de teste reais, disparadas por um sistema em horários marcados, para um 0800, uma URA ou um tronco SIP. Cada chamada registra se completou, quem atendeu, se havia áudio nos dois sentidos e como estava a qualidade.

O adjetivo vem do monitoramento de sites e de redes, onde um teste simula o acesso de um usuário. Entre quem opera redes de voz, o nome mais comum é monitoramento ativo. Os dois descrevem a mesma ideia e se opõem ao monitoramento passivo, que analisa as chamadas que os clientes já fizeram, por captura de SIP e RTP ou por relatórios de CDR.

Sintético ou passivo

Pergunta	Passivo	Sintético
Analisa chamadas reais de clientes	Sim	Não: faz as próprias chamadas
Vê o 0800 que ninguém ligou de madrugada	Não, só vê o que passa	Sim, a chamada de teste liga
Mede a qualidade do áudio recebido	Pela rede, em geral estimada	Pelo áudio de cada chamada de teste
Prova a quem a falha pertence	Depende do que foi capturado	Traz a resposta da rota a cada chamada

Um não substitui o outro. O passivo mostra o que os clientes viveram; o sintético mostra o que um cliente viveria agora, inclusive quando ninguém ligou.

Na prática

Um circuito é testado a cada 15 minutos, por exemplo. Às 3h10 a rota da operadora para de completar chamadas. No monitoramento passivo, nada aparece até alguém ligar, e de madrugada pode ser tarde. No sintético, a chamada de 3h15 falha, é repetida, e quatro chamadas seguidas com falha abrem um incidente com o código SIP recebido, antes do primeiro cliente reclamar.

Como o Monitor usa isso

O Monitor é um serviço de monitoramento sintético: a 2N5 liga para cada circuito de voz no ritmo combinado, confere a resposta, o áudio e a mensagem, repete a chamada que falha e só então abre o incidente. Veja o guia de chamadas sintéticas e o monitoramento de troncos SIP e VoIP.

Perguntas frequentes

Monitoramento sintético é o mesmo que monitoramento ativo?

Na telefonia, na prática, sim. Os dois nomes descrevem testes que o próprio monitoramento inicia, em oposição ao monitoramento passivo, que só observa as chamadas que os clientes já fizeram. Sintético é o termo herdado do monitoramento de sites e de redes; ativo é o mais usado por quem opera redes de voz.

Uma chamada sintética conta como chamada real?

Sim, no sentido que importa: ela atravessa a operadora, a rota e o atendimento como uma ligação de cliente, e por isso encontra falhas que o equipamento não vê. O que a torna sintética é só quem a inicia, um sistema, e o roteiro, que é sempre o mesmo, o que permite comparar uma chamada com a anterior.

GLOSSÁRIO

MOS: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** MOS (Mean Opinion Score) é a nota de 1 a 5, definida pela ITU-T P.800, que expressa a qualidade de voz percebida por quem ouve uma chamada.

Em inglês: MOS (Mean Opinion Score)

O que é MOS?

MOS (Mean Opinion Score) é uma nota de 1 a 5 que resume como as pessoas percebem a qualidade de uma chamada de voz. A escala vem da ITU-T P.800: 5 é excelente, 4 bom, 3 razoável, 2 ruim e 1 péssimo. Na origem, a nota saía de testes com ouvintes reais, que avaliavam amostras de áudio; a média dessas avaliações é o MOS.

Nota	Qualidade (ITU-T P.800)
5	Excelente
4	Boa
3	Razoável
2	Ruim

Nota	Qualidade (ITU-T P.800)
1	Péssima

Ninguém reúne um painel de ouvintes para cada ligação. Por isso a ITU-T P.800.1 separa os tipos de MOS pela origem da nota: MOS-LQS é a nota subjetiva de escuta, dada por pessoas; MOS-LQO é a nota objetiva, calculada por um algoritmo que compara o áudio recebido com o original; MOS-LQE é uma estimativa de escuta; e MOS-CQE é a estimativa conversacional que sai de um modelo de rede. Quando um relatório mostra “MOS 4,1”, a primeira pergunta é: qual MOS? Uma nota estimada a partir de números de rede e uma nota medida no áudio podem divergir bastante na mesma chamada.

Fator R e E-model

O E-model, da ITU-T G.107, é um modelo de planejamento de rede. Ele começa com um fator R e desconta penalidades por atraso, perda de pacotes, codec e eco. Com os parâmetros padrão, R fica em torno de 93,2. A norma traz a fórmula que converte R em MOS:

Fator R	MOS-CQE
90	4,34
80	4,03
70	3,60
60	3,10
50	2,58

MOS-CQE

MOS-CQE é a nota conversacional estimada, a saída do E-model expressa na escala MOS. O máximo é 4,5. Ela nunca ouve o áudio: calcula a nota a partir de parâmetros como atraso, perda e codec. Serve bem para dimensionar uma rede, mas não percebe uma chamada muda, um lado sem áudio ou uma mensagem gravada da operadora no lugar da pessoa chamada.

Na prática

Suponha que um equipamento de rede informe R = 80 para uma chamada. Pela tabela da G.107, isso equivale a MOS-CQE de 4,03, uma chamada “boa”. Agora suponha que essa chamada caiu numa gravação da operadora dizendo que o número não está disponível. Os pacotes chegaram em ordem, sem perda e com pouco jitter, então o E-model continua mostrando 4,03. Para quem ligou, a chamada falhou.

O inverso também acontece. Uma rede com 0% de perda pode entregar um áudio cortado por um transcodificador mal configurado. O E-model não vê o problema, porque ele está no conteúdo do áudio, não nos pacotes. Só uma nota medida sobre o som recebido, comparado com o som esperado, mostra esses dois casos.

Como o Monitor usa isso

O Monitor nunca estima MOS a partir de números de rede. Ele mede o MOS-LQO no próprio áudio recebido nas chamadas de teste. Os detalhes de como a nota é calculada estão em qualidade de voz com MOS-LQO e no verbete MOS-LQO.

Perguntas frequentes

Qual é um MOS bom em VoIP?

Na escala da ITU-T P.800, 4 significa bom e 3 significa razoável. O MOS-CQE do E-model chega no máximo a 4,5, então uma nota acima de 4 já está perto do melhor que o modelo permite. Notas medidas no áudio, como o MOS-LQO, dependem do algoritmo e da banda do codec, por isso só faz sentido comparar notas do mesmo tipo.

MOS e fator R são a mesma coisa?

Não. O fator R é a saída do E-model (ITU-T G.107), numa escala que chega a cerca de 93,2 com os parâmetros padrão. Ele é convertido em MOS-CQE por uma fórmula da própria norma: R 80 equivale a 4,03 e R 70 a 3,60. O fator R é uma estimativa de planejamento de rede, não uma nota tirada do áudio.

GLOSSÁRIO

MOS-LQO: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** MOS-LQO é a nota de 1 a 5, definida na ITU-T P.800.1, que um algoritmo calcula comparando o áudio recebido numa chamada com o áudio de referência que deveria ter chegado.

Em inglês: MOS-LQO (Mean Opinion Score, Listening Quality Objective)

O que é MOS-LQO?

MOS-LQO (Mean Opinion Score, Listening Quality Objective) é uma nota de 1 a 5 calculada por um algoritmo a partir do áudio real de uma chamada. O algoritmo recebe dois arquivos, o áudio de referência e o áudio que chegou do outro lado, e mede o quanto o segundo se afastou do primeiro. O resultado é expresso na mesma escala da MOS da ITU-T P.800, onde 5 é excelente e 1 é péssimo.

A sigla vem da ITU-T P.800.1, que classifica as notas MOS pela origem. “LQ” indica qualidade de escuta (listening quality) e “O” indica objetiva, ou seja, calculada por máquina sobre o som. Ela se opõe à LQS, dada por ouvintes, e às notas estimadas, como a MOS-CQE do E-model, que nunca ouvem o áudio.

Medido ou estimado

A diferença prática é o que cada nota consegue ver. Uma nota estimada olha para os pacotes: atraso, perda e jitter. Uma nota medida olha para o som. Se a chamada chega muda, se só um lado tem áudio, se a operadora toca uma mensagem no lugar do destino ou se um transcodificador distorce a voz, os pacotes podem estar perfeitos e a nota estimada continua alta. O MOS-LQO cai, porque o som recebido não se parece com o esperado.

Os algoritmos mais conhecidos para MOS-LQO são o PESQ e o POLQA, normas da ITU, e o ViSQOL, de código aberto.

Na prática

Imagine três chamadas para o mesmo número, todas com 0% de perda de pacotes e jitter abaixo de 5 ms:

Chamada	O que aconteceu	Rede	MOS-LQO
A	Áudio limpo	Normal	Alto
B	Áudio passou por dois transcodificadores	Normal	Mais baixo
C	Operadora tocou “número indisponível”	Normal	Muito baixo

Pela rede, as três chamadas são iguais. Pelo áudio, só a chamada A entregou o que deveria. É essa diferença que justifica medir em vez de estimar.

Como o Monitor usa isso

O Monitor mede o MOS-LQO em toda chamada de teste atendida. Ele compara o áudio recebido com a gravação esperada, a referência gravada quando o circuito é configurado, usando um modelo perceptual de qualidade de escuta com referência (ITU-T P.800.1). Os limites padrão: a partir de 3,8 a chamada é saudável; abaixo de 3,0 ela conta como degradada; entre 3,0 e 3,8 passa com uma observação. Veja qualidade de voz com MOS-LQO.

Perguntas frequentes

Qual a diferença entre MOS-LQO e MOS-CQE?

O MOS-LQO é medido: um algoritmo compara o áudio recebido com o áudio original e dá a nota. O MOS-CQE é estimado: o E-model da ITU-T G.107 calcula a nota a partir de atraso, perda e codec, sem ouvir nada. Por isso o MOS-CQE pode dar nota boa para uma chamada que caiu numa gravação da operadora, e o MOS-LQO não.

Um MOS-LQO de um algoritmo vale para outro?

Não diretamente. PESQ, POLQA e ViSQOL produzem notas na mesma escala de 1 a 5, mas cada um tem seu mapeamento e seu teto. O ViSQOL no modo de fala chega a 5,0, enquanto o modo de áudio fica perto de 4,75. Compare notas do mesmo algoritmo, no mesmo modo, para tirar conclusões.

GLOSSÁRIO

MTTR e MTTA: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** MTTR e MTTA são médias de tempo por incidente: o MTTA mede quanto a equipe leva para reconhecer o alerta, e o MTTR quanto leva para restabelecer o serviço.

Em inglês: MTTR (Mean Time to Repair) and MTTA (Mean Time to Acknowledge)

O que são MTTR e MTTA?

MTTA (Mean Time to Acknowledge) é o tempo médio entre o alerta de um incidente e o momento em que alguém o reconhece e assume. MTTR é o tempo médio até o serviço voltar a funcionar. A sigla MTTR tem variações (Mean Time to Repair, to Restore, to Recover, to Resolve), e por isso cada empresa precisa dizer de onde a contagem começa e onde termina.

Os dois números respondem perguntas diferentes. O MTTA mostra se o alerta chega a alguém: um tronco que cai às 2h da manhã e só é reconhecido às 7h tem um problema de alerta, não de reparo. O MTTR mostra quanto o cliente final fica sem atendimento, somando reação, diagnóstico, contato com a operadora e correção.

Em contratos, aparecem como prazos de atendimento e de reparo ao lado do SLA de disponibilidade. Um ponto comum de confusão: o MTTR pode ser medido a partir do início real da falha ou a partir da detecção. Se a detecção depende de um cliente reclamar, o MTTR oficial parece curto enquanto a queda real foi bem mais longa.

Na prática

Quatro incidentes em um mês, contados a partir da detecção:

Incidente	Até o reconhecimento	Até a volta do serviço
A, tronco SIP, 08:00	6 min	40 min
B, URA, 10:30	2 min	15 min
C, 0800, 02:10	25 min	95 min
D, ramal DDR, 16:45	3 min	10 min

MTTA = (6 + 2 + 25 + 3) ÷ 4 = 9 minutos. MTTR = (40 + 15 + 95 + 10) ÷ 4 = 40 minutos. O incidente C, de madrugada, puxa as duas médias para cima. Sem ele, o MTTA cairia para cerca de 4 minutos, sinal de que o problema está no alerta fora do horário.

Como o Monitor usa isso

O relatório mostra o tempo médio até o primeiro reconhecimento de cada incidente, que é o MTTA, e o tempo fora do ar de cada incidente. Assim dá para ver se a demora está em alguém perceber o alerta ou em resolver a falha. Veja alertas e escalonamento.

Perguntas frequentes

Qual a diferença entre MTTR e MTTA?

O MTTA termina quando alguém assume o incidente, ou seja, reconhece o alerta. O MTTR termina quando o serviço volta a funcionar. O MTTA mede a reação da equipe e do processo de alerta; o MTTR mede a reação mais o diagnóstico e o reparo. Um MTTA alto quase sempre indica alerta que ninguém viu, enviado para a pessoa errada ou fora do horário.

Como reduzir o MTTA?

Mandando o alerta para quem pode agir, pelo canal que essa pessoa vê fora do horário comercial, e escalando para o próximo da lista quando ninguém reconhece em poucos minutos. Também ajuda reduzir alarmes falsos, porque uma equipe que recebe muitos alertas sem problema real passa a ignorá-los. Medir o MTTA por incidente mostra onde o processo trava.

GLOSSÁRIO

Número 0800: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Número 0800 é o código de acesso não geográfico em que a chamada é gratuita para quem liga e o assinante do número paga pela ligação, conforme a numeração da Anatel.

Em inglês: toll-free number (0800)

O que é um número 0800?

Número 0800 é o código de acesso em que quem liga não paga nada e o assinante do número paga a chamada. A regra está na Resolução Anatel nº 749/2022, art. 18. Costuma ser escrito como 0800 123 4567 e é usado em SAC, ouvidoria, suporte técnico e vendas.

O 0800 não é geográfico: ele não pertence a uma cidade nem a uma linha física. Quando alguém disca, a rede da operadora traduz o 0800 para um destino real, normalmente um tronco SIP ou E1 da empresa, que entrega a chamada ao PABX e à URA.

Essa tradução cria um ponto de falha que o monitoramento interno não vê. O tronco pode estar registrado, o PABX ligado e a URA funcionando, e mesmo assim o 0800 falhar porque o roteamento na operadora foi alterado, o número foi desativado por engano ou o destino configurado ficou errado. Quem liga ouve uma mensagem da operadora, e a empresa percebe só quando o volume da fila cai ou chegam reclamações por outros canais.

Por ser gratuito, o 0800 é também o número que o cliente usa quando algo já deu errado. Uma queda nele costuma afetar justamente quem mais precisa de atendimento.

Na prática

Há duas formas de testar um 0800, e elas não medem a mesma coisa:

Teste	Operadora traduz o 0800?	Tronco e PABX	URA
Ligar para o número de destino direto	Não	Sim	Sim
Ligar para o 0800	Sim	Sim	Sim

Exemplo: o 0800 123 4567 aponta para o 11 3456-7000. Se a operadora troca o destino por engano para 11 3456-7100, o teste no número direto continua passando, e só a ligação para o 0800 revela a falha. Do lado da empresa, nada muda: o tronco segue registrado e a URA atende quem consegue chegar.

Como o Monitor usa isso

Qualquer número discável pode ser monitorado, inclusive 0800. O teste disca o próprio 0800, como um cliente faria, e assim passa pela tradução na operadora, pelo tronco, pelo PABX e pela URA, testando o caminho completo que o cliente usa. Veja o monitoramento de 0800 e URA.

Perguntas frequentes

Quem paga a ligação para 0800?

O assinante do número, ou seja, a empresa que contratou o 0800. Pela Resolução Anatel nº 749/2022, art. 18, a chamada para 0800 é gratuita para quem liga. Por isso o 0800 é comum em SAC, ouvidoria e suporte. O custo para a empresa cresce com o volume e a duração das chamadas, o que é um motivo a mais para que cada ligação seja atendida.

Por que meu 0800 funciona de um telefone e falha de outro?

Porque o 0800 é roteado pela rede da operadora, e esse roteamento pode variar conforme a origem da chamada, como a rede ou a região de quem liga. Uma configuração errada pode afetar só uma parte das chamadas. Também pode acontecer de o destino aceitar a chamada de uma rede e recusar de outra por codec ou limite de canais.

GLOSSÁRIO

Números 0300 e 0303: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Números 0300 e 0303 são códigos de acesso nacionais de custo compartilhado, em que o valor da chamada é dividido entre quem liga e o assinante do número, segundo a numeração da Anatel.

Em inglês: shared-cost numbers (0300 and 0303)

O que são os números 0300 e 0303?

São códigos de acesso nacionais de custo compartilhado: o valor da chamada é dividido entre quem liga e o assinante do número. A regra está na Resolução Anatel nº 749/2022, art. 18, a mesma que define o 0800 como gratuito para quem liga.

Os dois têm usos diferentes. O 0300 é um número para receber chamadas: atendimento ao cliente, suporte, centrais de informação, em que a empresa quer um número único nacional sem arcar com todo o custo como no 0800. O 0303 identifica quem faz chamadas em grande volume. Pelo Ato Anatel nº 12.712/2024, ele é obrigatório para quem faz mais de 10 mil chamadas em pelo menos um dia do mês, como em telemarketing, cobrança e pedido de doações. O número aparece na tela de quem recebe a ligação.

Como o 0800, o 0300 é traduzido pela rede da operadora para um destino real, normalmente um tronco da empresa que entrega a chamada ao PABX e à URA. O roteamento na operadora é um ponto de falha que não aparece no monitoramento do PABX.

Na prática

Comparação entre os números de acesso mais comuns:

Número	Quem paga	Uso típico
0800	Assinante	SAC, ouvidoria, suporte
0300	Custo compartilhado	Atendimento com número nacional
0303	Custo compartilhado	Chamadas em massa: telemarketing, cobrança, doações
4004, 4003, 3003	Quem liga, em geral como chamada local, segundo as operadoras	Número único nacional

Os números 4004, 4003 e 3003 não são uma categoria da numeração da Anatel; veja números 4004, 4003 e 3003. Na escolha entre eles, pesa quem a empresa quer que arque com o custo da ligação e se o número será usado para receber ou para fazer chamadas.

Como o Monitor usa isso

Qualquer número discável pode ser monitorado, inclusive 0300 e 0303. O teste disca o próprio número, como um cliente faria, e passa pela tradução na operadora, pelo tronco e pela URA, testando o caminho completo que o cliente usa. Veja o monitoramento de 0800 e URA.

Perguntas frequentes

Quem é obrigado a usar 0303?

Pelo Ato Anatel nº 12.712/2024, quem faz mais de 10 mil chamadas em pelo menos um dia do mês precisa usar o código 0303. Isso alcança atividades como telemarketing, cobrança e pedido de doações. Com o 0303 na tela, quem recebe a ligação sabe de antemão que se trata de uma chamada desse tipo e pode decidir se atende.

Qual a diferença entre 0300 e 0800?

Quem paga. No 0800, a chamada é gratuita para quem liga e o assinante paga tudo. No 0300, o custo é compartilhado entre quem liga e o assinante, conforme a Resolução Anatel nº 749/2022, art. 18. Os dois são números nacionais roteados pela operadora até o destino real da empresa, e os dois podem falhar no roteamento sem que o PABX perceba.

GLOSSÁRIO

Números 4004, 4003 e 3003: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Números 4004, 4003 e 3003 são códigos de acesso fixos de oito dígitos que operadoras vendem como número único nacional, discado sem DDD nas localidades que a operadora atende.

Em inglês: single national number (4004, 4003, 3003)

O que são os números 4004, 4003 e 3003?

São números fixos de oito dígitos, no formato 4004-1234, que as operadoras vendem como número único nacional. A empresa divulga um só número, e quem liga disca sem DDD nas localidades atendidas pela operadora. Ao contrário do 0800 e do 0300, eles não são uma categoria da numeração da Anatel: são um produto das operadoras. Segundo elas, quem liga normalmente paga o valor de uma chamada local.

Por trás do número, a operadora configura o mesmo código em cada área local onde oferece o serviço e encaminha todas as chamadas para o destino real da empresa, em geral um tronco SIP ou E1 que entrega a ligação ao PABX e à URA.

Esse desenho tem uma consequência para quem monitora. O número é um só, mas o roteamento é configurado por localidade. Uma mudança errada pode fazer o 4004 funcionar para quem liga de São Paulo e falhar para quem liga de Recife. Também pode haver diferença entre chamadas de telefone fixo e de celular, conforme a forma de discagem que a operadora aceita em cada caso.

Na prática

Três formas de publicar um número de atendimento:

Número	Quem paga	Formato	Alcance
0800 123 4567	Assinante	Código não geográfico	Nacional
4004-1234	Quem liga, em geral como chamada local	Oito dígitos, sem DDD	Localidades da operadora
(11) 3456-7000	Quem liga, conforme a distância	Número fixo com DDD	Uma área local

Exemplo: uma empresa troca o destino do 4004 de um tronco antigo para um novo. Se a operadora atualiza 20 localidades e esquece uma, as chamadas daquela cidade caem enquanto as demais funcionam.

Como o Monitor usa isso

Qualquer número discável pode ser monitorado, inclusive 4004, 4003 e 3003. O teste disca o próprio número, como um cliente faria, e passa pelo roteamento da operadora, pelo tronco e pela URA, testando o caminho completo que o cliente usa. Veja o monitoramento de 0800 e URA.

Perguntas frequentes

4004 é a mesma coisa que 0800?

Não. O 0800 é uma categoria da numeração da Anatel, gratuita para quem liga. Os números 4004, 4003 e 3003 não são uma categoria da Anatel: são números fixos de oito dígitos que as operadoras vendem como número único nacional. Em vez de a empresa pagar a ligação, quem liga normalmente paga uma chamada local, como as operadoras descrevem o serviço.

Ligar para 4004 é de graça?

Em geral, não. As operadoras descrevem o serviço como um número em que quem liga paga o valor de uma chamada local, mesmo estando em outra cidade. O custo exato depende do plano de quem liga e da origem da chamada. Para atendimento gratuito ao cliente, o número indicado é o 0800, pago pelo assinante.

GLOSSÁRIO

PABX IP: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** PABX IP é a central telefônica privada de uma empresa que funciona sobre rede IP, conectando ramais, troncos e URA e roteando chamadas internas e externas com SIP e RTP.

Em inglês: IP PBX

O que é um PABX IP?

PABX IP é a central telefônica privada de uma empresa que usa a rede de dados em vez de fiação telefônica. Ela registra os ramais (telefones IP, softphones e adaptadores para aparelhos analógicos), conecta a empresa à operadora por troncos SIP ou, por meio de um gateway, por troncos E1, e decide para onde cada chamada vai.

A sinalização entre ramais, central e operadora usa SIP, e o áudio viaja em pacotes RTP. Sobre essa base, o PABX oferece os recursos de sempre: URA, filas de atendimento, transferência, siga-me, correio de voz, gravação e o mapeamento de números DDR para ramais.

O PABX IP pode ser um servidor ou appliance dentro da empresa, uma máquina virtual em data center ou um serviço hospedado. Em todos os casos, ele é só uma parte do caminho. Uma chamada que vem de fora passa pela operadora, pelo tronco, pelo firewall ou SBC, pela central e só então chega ao ramal ou à URA. Monitorar CPU, memória e processos da central mostra que o servidor está ligado, mas não que uma ligação de cliente completa com áudio nos dois sentidos.

Na prática

Um escritório com 40 ramais, um tronco SIP com 10 canais e uma faixa DDR de 11 3456-7000 a 7039. Uma ligação externa para 11 3456-7012 percorre:

Trecho	O que pode falhar
Operadora	Roteamento do número, portabilidade, canais
Tronco SIP	Registro, autenticação, limite de canais
Firewall ou SBC	NAT, SIP ALG, portas RTP bloqueadas
PABX IP	Plano de discagem, mapeamento DDR, codecs
Ramal 7012	Ramal desregistrado, aparelho desligado

Com o PABX em pé, qualquer um desses trechos pode derrubar a chamada.

Como o Monitor usa isso

O Monitor funciona com qualquer PABX porque liga para números, como um cliente faria. Não há integração, agente ou configuração na central: o teste disca o número público, e o resultado mostra se a chamada completou passando por todo o caminho. Veja o monitoramento de troncos SIP.

Perguntas frequentes

Preciso integrar o monitoramento de chamadas ao meu PABX IP?

Não quando o teste é feito por chamadas reais. Uma chamada de teste liga para o número público, como faria um cliente, e percorre operadora, tronco, PABX e ramal ou URA. Por isso não depende de marca, versão ou API da central, e também detecta falhas que estão fora do PABX, como roteamento na operadora ou problemas no link de internet.

Qual a diferença entre PABX IP e PABX em nuvem?

A função é a mesma: ramais, filas, URA e roteamento. No PABX IP local, o servidor fica na empresa e a equipe cuida de hardware, atualizações e link. No PABX em nuvem, o provedor hospeda a central e os ramais se registram pela internet. Nos dois casos, a chamada depende de tronco, rede e configuração, e pode falhar mesmo com a central ligada.

GLOSSÁRIO

Perda de pacotes: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Perda de pacotes é a fração dos pacotes de uma chamada VoIP que não chega ao destino ou chega tarde demais para ser tocada, causando cortes no áudio.

Em inglês: packet loss

O que é perda de pacotes?

Perda de pacotes é a parte dos pacotes de voz que sai de uma ponta da chamada e não chega à outra. Numa chamada VoIP, a voz é cortada em pedaços de 20 ms e cada pedaço viaja num pacote RTP. Se um pacote se perde, aquele trecho de som não existe no destino. A taxa é expressa em porcentagem: pacotes perdidos divididos pelos pacotes enviados.

Os pacotes se perdem por congestionamento, quando um roteador descarta o que não cabe na fila; por erros em enlaces de rádio ou Wi-Fi; e por jitter excessivo, quando o pacote chega depois da hora de tocar e o receptor o joga fora. Como o RTP corre sobre UDP, não há retransmissão: em voz, um pacote atrasado não serve mais.

Os codecs tentam disfarçar a falha com ocultação de perda (packet loss concealment), que repete ou interpola o som vizinho. Isso funciona para pacotes isolados. Em rajadas, quando vários pacotes seguidos somem, a ocultação não tem o que copiar e o ouvinte percebe palavras picotadas.

Na prática

Com pacotes de 20 ms, cada sentido da chamada envia 50 pacotes por segundo, ou 3.000 por minuto.

Perda	Pacotes perdidos por minuto	Áudio perdido por minuto
0,5%	15	0,3 s
1%	30	0,6 s
3%	90	1,8 s
5%	150	3,0 s

Os mesmos 30 pacotes perdidos em um minuto soam diferente conforme a distribuição. Espalhados, são cortes de 20 ms que a ocultação esconde. Juntos, são 0,6 s de silêncio de uma vez, o suficiente para apagar uma palavra como “confirmado”.

Como o Monitor usa isso

O agente de circuitos de dados que a 2N5 instala em cada site mede a perda de pacotes, a latência e o jitter do link de internet daquele local, com gráficos das últimas 100 horas. Numa chamada de voz, os pacotes perdidos aparecem como áudio picotado e derrubam o MOS-LQO medido. Veja circuitos de dados.

Perguntas frequentes

Quanta perda de pacotes uma chamada VoIP aguenta?

Depende do codec e de como a perda se distribui. Codecs com ocultação de perda disfarçam pacotes isolados, e 1% espalhado pela chamada pode passar quase despercebido. A mesma taxa concentrada em rajadas, vários pacotes seguidos, apaga sílabas inteiras. Por isso a taxa média sozinha não basta: é preciso olhar o áudio que chegou.

Perda de pacotes e jitter estão ligados?

Sim. Quando o jitter passa do tamanho do buffer do receptor, os pacotes que chegam atrasados são descartados. Para quem ouve, um pacote que chegou tarde demais e um pacote que nunca chegou dão o mesmo resultado: um corte. Muitos equipamentos contam os dois juntos na perda total.

GLOSSÁRIO

POLQA e PESQ: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** POLQA (ITU-T P.863) e PESQ (ITU-T P.862) são normas da ITU que calculam uma nota MOS-LQO comparando o áudio recebido numa chamada com o áudio de referência.

Em inglês: POLQA (Perceptual Objective Listening Quality Analysis) and PESQ (Perceptual Evaluation of Speech Quality)

O que são POLQA e PESQ?

POLQA e PESQ são algoritmos padronizados pela ITU para calcular a qualidade de voz de uma chamada a partir do áudio. Os dois são de referência completa: comparam o áudio que chegou do outro lado com o áudio original e devolvem uma nota MOS-LQO, na escala de 1 a 5 da MOS.

O PESQ (Perceptual Evaluation of Speech Quality) é a ITU-T P.862, criada para voz em banda estreita, a telefonia clássica de 8 kHz. Durante muitos anos foi a referência do setor para medir qualidade de voz de forma objetiva. Em 5 de janeiro de 2024 a ITU retirou a P.862 e passou a indicar a P.863 em seu lugar.

O POLQA (Perceptual Objective Listening Quality Analysis) é a ITU-T P.863, a sucessora. Ela cobre também voz em banda larga e superlarga, o que importa para codecs modernos, e lida melhor com distorções que o PESQ avaliava mal. O POLQA é distribuído sob licença comercial.

Os dois dependem de um modelo de como o ouvido humano percebe distorções. A nota não diz o que deu errado; diz o quanto o som recebido se afastou do original aos ouvidos de um ouvinte médio.

Na prática

Algoritmo	Origem	Situação	Acesso
PESQ	ITU-T P.862	Retirado em 5/1/2024	Implementações antigas ainda circulam
POLQA	ITU-T P.863	Norma vigente	Licença comercial
ViSQOL	Google Research	Mantido, versão v3	Código aberto

Um exemplo de por que não misturar notas: um relatório de 2019 mostra MOS 3,9 calculado com PESQ, e um teste de hoje mostra 3,6 com outro algoritmo. A queda de 0,3 pode não significar nada, porque cada algoritmo tem seu mapeamento e seu teto. Para acompanhar a evolução de uma linha, o algoritmo e o modo precisam ser sempre os mesmos.

Como o Monitor usa isso

O Monitor não usa POLQA nem PESQ. Ele mede MOS-LQO com um modelo perceptual de qualidade de escuta com referência, comparando o áudio recebido em cada chamada de teste atendida com a gravação de referência do circuito. O motivo de explicar as três opções aqui é que muitas notas de mercado vêm do PESQ ou do POLQA. Veja qualidade de voz com MOS-LQO.

Perguntas frequentes

O PESQ ainda pode ser usado?

Implementações do PESQ continuam circulando e muitos relatórios antigos usam suas notas. Mas a ITU retirou a ITU-T P.862 em 5 de janeiro de 2024 e indica a P.863, o POLQA, como substituta. Para um processo novo, o PESQ não é mais a norma vigente, e suas notas não devem ser comparadas diretamente com as do POLQA.

POLQA e ViSQOL dão a mesma nota?

Não necessariamente. Os dois comparam o áudio recebido com a referência e devolvem MOS-LQO de 1 a 5, mas usam modelos diferentes de percepção e mapeamentos diferentes para a escala. A mesma chamada pode receber notas distintas. Compare sempre notas do mesmo algoritmo e do mesmo modo.

GLOSSÁRIO

Post dial delay (PDD): definição e exemplo na prática

Por Equipe 2N5 Atualizado em 14 de outubro de 2026

> **Resposta curta:** Post dial delay (PDD) é o intervalo entre o instante em que a chamada é pedida, ao terminar de discar, e o primeiro sinal de que o destino está sendo chamado, o toque ou a mensagem inicial que o chamador ouve.

Em inglês: post-dial delay (PDD)

O que é post dial delay?

Post dial delay, ou PDD, é o tempo que o chamador espera em silêncio depois de discar. Ele começa quando a chamada é pedida, ao terminar de discar, e termina quando chega o primeiro sinal de que o destino está sendo chamado: o toque de chamada, ou a mensagem inicial de uma URA ou da operadora. Em SIP, é o tempo entre o INVITE e a primeira resposta provisória, como 180 Ringing ou 183 Session Progress. A RFC 6076, que define as métricas de desempenho do SIP, dá a esse tempo o nome de Session Request Delay.

O PDD pesa mais do que parece. Passados alguns segundos de silêncio, o chamador acha que a ligação não está funcionando e desliga. Para quem tem um 0800 ou uma central de atendimento, cada desistência assim é um cliente que tentou e não conseguiu falar.

O que aumenta o PDD

- **Rotas com várias operadoras em sequência**, cada uma somando um pouco de tempo.
- **Consulta de portabilidade** lenta antes de a chamada ser roteada.

- **Rota alternativa:** quando o primeiro destino falha, o equipamento tenta o seguinte antes de o chamador ouvir qualquer coisa.
- **Resolução de DNS demorada** ou equipamento de borda sobrecarregado.

Um tronco SIP pode estar registrado e completar todas as chamadas e ainda assim ter um PDD ruim, e é por isso que o PDD aparece como queixa de cliente antes de aparecer como queda.

Na prática

Veja o que o chamador vive em duas chamadas ao mesmo número (valores ilustrativos):

Chamada	Último dígito	Primeiro toque	PDD	O que o chamador percebe
A	0 s	2 s	2 s	A ligação começa normalmente
B	0 s	11 s	11 s	Silêncio longo; muita gente desliga

As duas completam. Só quem mede o tempo até o primeiro toque percebe a diferença.

Como o Monitor usa isso

O Monitor liga para cada circuito de voz como um cliente, e uma chamada que demora demais para completar acaba contando como falha, com o código SIP e a causa Q.850 que a rota devolveu. O Monitor não publica o PDD como uma métrica à parte. Use o PDD do seu CDR para olhar a tendência, e a chamada de teste para confirmar, de fora, se o número continua completando. Veja o monitoramento de troncos SIP e VoIP e o monitoramento sintético.

Perguntas frequentes

O que é post dial delay e qual é o normal?

Post dial delay (PDD) é o silêncio entre o último dígito discado e o primeiro toque. Não há um valor único em norma para todo tipo de chamada: costuma ser de poucos segundos e varia com o número de operadoras no caminho e com a consulta de portabilidade. O que vale é a linha de base do próprio circuito: se um número que levava poucos segundos passa a levar muito mais, algo mudou na rota.

O que aumenta o post dial delay em um tronco SIP?

Rotas com várias operadoras em sequência, consulta de portabilidade lenta, falha em um destino que obriga a tentar uma rota alternativa, resolução de DNS demorada e equipamento sobrecarregado. Em cada caso, o chamador ouve silêncio entre o último dígito e o primeiro toque, e muitos desistem antes.

GLOSSÁRIO

Registro SIP: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Registro SIP é o processo em que um telefone, PABX ou tronco envia a mensagem REGISTER ao registrador para informar seu endereço atual e poder receber chamadas da sua conta.

Em inglês: SIP registration (REGISTER)

O que é registro SIP?

Registro SIP é a forma de um telefone, PABX ou tronco SIP avisar ao registrador onde está. O equipamento envia uma requisição REGISTER, definida na RFC 3261, com sua conta e seu endereço IP e porta. O registrador guarda esse vínculo por um tempo, informado no campo Expires, e encaminha para esse endereço as chamadas destinadas à conta.

O fluxo comum tem quatro passos: o equipamento envia REGISTER; o registrador responde 401 Unauthorized com um desafio; o equipamento reenvia o REGISTER com a resposta calculada a partir da senha; o registrador confirma com 200 OK. Antes de o prazo vencer, o equipamento registra de novo. Se o registro expira e não é renovado, as chamadas de entrada deixam de chegar.

Muitos equipamentos usam também o SIP OPTIONS (RFC 3261, seção 11) como keep-alive: uma pergunta periódica que, respondida com 200 OK, indica que o outro lado está vivo. O tráfego regular ainda mantém aberto o mapeamento de NAT no roteador, o que evita problemas com SIP ALG e firewalls.

Registro e OPTIONS testam a sinalização até o registrador. Eles não passam pelo roteamento da operadora, pelo limite de canais, pelos codecs nem pelo áudio.

Na prática

O que cada verificação prova sobre um tronco:

Verificação	Resposta esperada	Prova que
REGISTER	200 OK, com Expires de 3600 s, por exemplo	Credenciais aceitas e registrador alcançável
OPTIONS	200 OK	O outro lado responde à sinalização
Chamada real	200 OK e áudio nos dois sentidos	Chamadas completam com voz

Um tronco pode passar nas duas primeiras linhas o dia inteiro e falhar na terceira, por exemplo com 503 Service Unavailable quando os canais acabam. No PABX, o tronco continua aparecendo como registrado durante toda a falha.

Como o Monitor usa isso

Um tronco pode estar registrado e não completar chamadas, por isso o teste é uma chamada real. Quando a própria conta de chamadas da 2N5 não consegue se registrar, o teste é marcado como “sem visibilidade” e nunca é atribuído à linha do cliente. Veja o monitoramento de troncos SIP.

Perguntas frequentes

Tronco registrado significa que está funcionando?

Não necessariamente. O registro mostra que o PABX consegue falar com o registrador da operadora e que as credenciais foram aceitas. As chamadas ainda podem falhar por limite de canais, codec incompatível, roteamento errado na operadora ou áudio bloqueado por NAT. Só uma chamada real, com resposta SIP final e áudio nos dois sentidos, mostra que o tronco funciona.

Para que serve o SIP OPTIONS?

É uma requisição definida na RFC 3261, seção 11, para perguntar a outro equipamento quais recursos ele suporta. Na prática, PABX e SBC enviam OPTIONS periodicamente como keep-alive: se recebem 200 OK, consideram o outro lado ativo. O envio regular também mantém aberto o mapeamento de NAT

no roteador. Um OPTIONS respondido não prova que chamadas completam.

GLOSSÁRIO

RTP: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** RTP (Real-time Transport Protocol), definido na RFC 3550, é o protocolo que transporta o áudio de uma chamada VoIP em pacotes numerados e marcados com o tempo.

Em inglês: RTP (Real-time Transport Protocol)

O que é RTP?

RTP (Real-time Transport Protocol) é o protocolo que carrega a voz de uma chamada VoIP. Enquanto o SIP combina a chamada, o RTP leva o áudio em si, em pacotes pequenos enviados num ritmo fixo, geralmente um a cada 20 ms. Ele é definido na RFC 3550 e corre sobre UDP.

Cada pacote RTP tem um cabeçalho de 12 bytes com quatro informações principais: o tipo de carga, que indica o codec; o número de sequência, que permite perceber pacotes perdidos ou fora de ordem; o carimbo de tempo, usado para tocar o áudio no ritmo certo e calcular o jitter; e o SSRC, que identifica a fonte do fluxo. Cada sentido da chamada é um fluxo separado, com suas próprias portas, combinadas no SDP.

RTCP

O RTCP (RTP Control Protocol), definido na mesma RFC 3550, viaja ao lado do RTP e não carrega voz. Ele envia relatórios periódicos com pacotes enviados, fração de perda e jitter de chegada. Tradicionalmente usa a porta ímpar seguinte à do RTP.

SRTP

O SRTP (Secure RTP), da RFC 3711, cifra a carga de áudio e autentica os pacotes. Quem captura o tráfego vê os cabeçalhos, mas não ouve a conversa.

Na prática

Uma chamada de teste de cerca de 7 segundos com pacotes de 20 ms gera uns 350 pacotes por sentido. Um registro como “RTP 343 enviados / 340 recebidos” mostra:

Medida	Valor
Pacotes enviados	343
Pacotes recebidos	340
Perdidos	3 (0,9%)
Áudio perdido	cerca de 60 ms

Se o lado recebido mostrasse 0, a chamada teria sido atendida sem áudio naquele sentido, um caso típico de NAT ou SIP ALG.

Como o Monitor usa isso

A evidência de cada incidente mostra os pacotes RTP enviados e recebidos em cada chamada de teste, por exemplo “RTP 343 sent / 340 received”. O Monitor verifica que o áudio corre nos dois sentidos, então uma chamada atendida mas muda de um lado não passa como saudável. Veja qualidade de voz com MOS-LQO.

Perguntas frequentes

Por que a chamada conecta mas fica sem áudio?

Porque o SIP e o RTP seguem caminhos diferentes. O SIP pode estabelecer a chamada normalmente enquanto os pacotes RTP são bloqueados por um firewall, mandados para um IP privado por causa de NAT ou reescritos por um SIP ALG. O resultado é uma chamada atendida, muda nos dois sentidos ou em um só.

Qual a diferença entre RTP e SRTP?

O SRTP (RFC 3711) é o RTP com criptografia, autenticação e proteção contra repetição de pacotes. O formato e o ritmo dos pacotes são os mesmos; a diferença é que a carga de áudio viaja cifrada e não pode ser ouvida por quem capturar o tráfego. As chaves são combinadas na sinalização da chamada.

GLOSSÁRIO

SBC: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SBC (Session Border Controller) é o equipamento ou software na borda de uma rede VoIP que controla, protege e adapta a sinalização SIP e o áudio que entram e saem.

Em inglês: SBC (Session Border Controller)

O que é SBC?

SBC (Session Border Controller) é o equipamento que fica na fronteira entre duas redes VoIP, normalmente entre o PABX da empresa e o tronco SIP da operadora. Toda chamada que entra ou sai passa por ele, tanto a sinalização SIP quanto o áudio RTP. Pode ser um appliance físico, uma máquina virtual ou um software no próprio servidor de telefonia.

As funções mais comuns de um SBC são:

- Esconder a topologia: substitui IPs internos por um endereço público, para que a operadora não veja a rede da empresa.
- Atravessar NAT: corrige endereços no SIP e no SDP, o trabalho que um SIP ALG tenta fazer e muitas vezes faz mal.
- Segurança: bloqueia varreduras, tentativas de fraude e excesso de mensagens.
- Normalizar: ajusta cabeçalhos para que equipamentos de fabricantes diferentes se entendam.
- Transcodificar: converte entre codecs quando as pontas não têm um em comum.
- Controlar admissão: limita quantas chamadas simultâneas passam.

Por estar no meio de tudo, o SBC é também um ponto onde uma chamada pode falhar: uma regra errada, uma licença esgotada ou um certificado vencido bloqueiam o tráfego.

Na prática

Um INVITE sai do PABX e passa pelo SBC antes de chegar à operadora:

Campo	Saindo do PABX	Saindo do SBC
IP no Contact	10.0.0.5	203.0.113.10
IP de mídia no SDP	10.0.0.5	203.0.113.10
Porta RTP	12000	40000
Codecs oferecidos	G.711, G.729	G.711

A operadora só enxerga o endereço público e o codec que o SBC deixou passar. Se a porta 40000 estiver bloqueada no firewall, a chamada é atendida e fica muda.

Como o Monitor usa isso

Não há nada a instalar no SBC. O Monitor liga para o número a partir de fora, como um cliente qualquer faria, então a chamada de teste passa pelo SBC do mesmo jeito que uma chamada real. Veja monitoramento de troncos SIP.

Perguntas frequentes

Preciso de um SBC para ter um tronco SIP?

Nem sempre. Muitos PABX IP falam direto com a operadora. O SBC passa a valer a pena quando a empresa precisa esconder a rede interna, controlar quantas chamadas entram, ligar equipamentos com dialetos SIP diferentes ou transcodificar entre codecs. Algumas operadoras também colocam o próprio SBC na frente do tronco.

O SBC pode causar chamada sem áudio?

Sim. Se o SBC reescreve o SDP com um IP ou uma porta errada, ou se o firewall à frente dele bloqueia a faixa de portas RTP, a chamada é atendida e o áudio não passa em um ou nos dois sentidos. A sinalização mostra 200 OK, então só um teste que confere o áudio revela o problema.

GLOSSÁRIO

SIP: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP (Session Initiation Protocol), definido na RFC 3261, é o protocolo de sinalização que estabelece, modifica e encerra chamadas de voz sobre redes IP.

Em inglês: SIP (Session Initiation Protocol)

O que é SIP?

SIP (Session Initiation Protocol) é o protocolo que abre, controla e encerra chamadas VoIP. Ele faz o papel da sinalização da telefonia tradicional: avisa que há uma ligação, faz o destino tocar, informa o atendimento e marca o fim. O SIP é definido na RFC 3261 e usa mensagens de texto parecidas com as do HTTP, enviadas normalmente pela porta 5060.

As requisições SIP se chamam métodos. Os mais usados são INVITE (iniciar uma chamada), ACK (confirmar a resposta final), BYE (encerrar), CANCEL (desistir antes do atendimento), REGISTER (registrar um telefone ou tronco) e OPTIONS (consultar se o outro lado responde).

Cada requisição recebe respostas numeradas em seis classes: 1xx provisórias, como 180 Ringing; 2xx sucesso, como 200 OK; 3xx redirecionamento; 4xx erro do lado de quem chamou ou do destino, como 486 Busy Here; 5xx falha do servidor, como 503; e 6xx falha global. A resposta final de uma chamada é a que melhor diz o que aconteceu. A lista completa está em códigos SIP.

SDP

O SIP não carrega áudio. Ele leva, dentro do INVITE e da resposta, uma descrição da mídia em SDP (Session Description Protocol), da RFC 4566, hoje substituída pela RFC 8866. O SDP diz o IP e a porta onde cada lado espera receber o RTP e quais codecs aceita. Um lado oferece, o outro responde, e a voz passa a correr pelo caminho combinado.

Na prática

Uma chamada bem-sucedida troca estas mensagens:

Passo	De	Mensagem
1	Quem liga	INVITE com SDP
2	Destino	100 Trying
3	Destino	180 Ringing
4	Destino	200 OK com SDP
5	Quem liga	ACK
6	Qualquer lado	BYE
7	O outro lado	200 OK

Se o destino estiver ocupado, o passo 4 vira 486 Busy Here e a resposta pode trazer no cabeçalho Reason a causa Q.850 17, usuário ocupado, conforme a RFC 6432.

Como o Monitor usa isso

O Monitor lê a resposta SIP final e a causa Q.850 de toda chamada de teste. Com os dois, o incidente diz se o destino recusou, se a rede falhou ou se o número não existe. Veja monitoramento de troncos SIP.

Perguntas frequentes

Qual a diferença entre SIP e RTP?

O SIP é a sinalização: diz quem liga para quem, se o destino toca, se atende e quando a chamada termina. O RTP transporta o áudio. Os dois seguem caminhos e portas diferentes, por isso uma chamada pode ser atendida no SIP e mesmo assim ficar sem voz, quando o RTP é bloqueado ou

desviado no caminho.

O que é a causa Q.850 numa resposta SIP?

É um código numérico herdado da telefonia ISDN que explica por que a chamada terminou, como 16 para desligamento normal ou 17 para usuário ocupado. Muitas operadoras o enviam no cabeçalho Reason da resposta SIP, conforme a RFC 6432. Ele completa o código SIP, que às vezes é genérico demais para diagnosticar a falha.

GLOSSÁRIO

SIP ALG: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SIP ALG (Application Layer Gateway) é uma função de roteadores e firewalls que reescreve endereços dentro das mensagens SIP para atravessar o NAT, frequentemente quebrando o áudio das chamadas.

Em inglês: SIP ALG (Application Layer Gateway)

O que é SIP ALG?

SIP ALG (Application Layer Gateway) é uma função de roteadores e firewalls que abre as mensagens SIP e troca os endereços IP privados de dentro delas pelo IP público da conexão. A ideia é ajudar a chamada a atravessar o NAT. Na prática, muitas implementações reescrevem campos errados, deixam outros sem corrigir ou quebram mensagens que o PABX ou o SBC já tinham ajustado. O resultado clássico é áudio mudo em um sentido, chamadas que caem sozinhas e ramais que perdem o registro.

É comum o SIP ALG vir ligado de fábrica em roteadores domésticos e de pequenas empresas. Quando a telefonia IP começa a falhar depois de trocar o roteador ou o link, o ALG é um dos primeiros suspeitos.

NAT

NAT (Network Address Translation) é o que permite vários equipamentos com IP privado, como 192.168.0.20, saírem para a internet com um único IP público. O roteador troca o endereço no cabeçalho do pacote. O problema é que o SIP repete endereços dentro da própria mensagem, nos cabeçalhos Via e Contact e no SDP, que indica para onde mandar o RTP. Se esses endereços internos chegam à operadora sem correção, ela manda o áudio para um IP privado que não existe na internet.

Na prática

Sintoma	Causa provável
Chamada atendida, um lado não ouve	IP privado ou porta errada no SDP
Chamada cai depois de cerca de 32 segundos	ACK não chega; o destino desiste após 64 × T1 (RFC 3261)
Ramal perde o registro de tempos em tempos	ALG fecha ou altera a sessão do REGISTER
Funciona em um link e falha em outro	Roteadores diferentes, um com ALG ligado

Para desativar, procure na página do roteador ou firewall por SIP ALG, SIP Helper ou inspeção SIP, desligue e reinicie. Em equipamentos baseados em Linux, a função costuma ser o módulo de conntrack de SIP.

Como o Monitor usa isso

Uma chamada de teste que conecta mas fica sem áudio em um dos sentidos é detectada como áudio de mão única e conta como falha, mesmo com a resposta SIP 200 OK. Veja monitoramento de troncos SIP.

Perguntas frequentes

Como desativar o SIP ALG no roteador?

Entre na página de administração do roteador ou firewall e procure em NAT, firewall ou configurações avançadas por SIP ALG, SIP Helper, SIP Passthrough ou inspeção SIP. Desmarque a opção, salve e reinicie o equipamento. Se o roteador foi entregue pela operadora e a opção não aparece, peça o desligamento ao suporte ou o modo bridge. Depois, faça uma chamada de teste nos dois sentidos.

Devo sempre desativar o SIP ALG?

Na maioria dos casos, sim, desde que algo cuide do NAT corretamente: o PABX configurado com o IP público, telefones com STUN ou um SBC. Sem nenhum desses, desativar o ALG pode deixar os telefones atrás do NAT sem áudio. Teste antes e depois da mudança.

GLOSSÁRIO

SLA: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** SLA (Acordo de Nível de Serviço) é o compromisso contratual que define o nível mínimo de um serviço, como 99,9% de disponibilidade, e como ele é medido e apurado.

Em inglês: Service Level Agreement

O que é SLA?

SLA (Service Level Agreement, ou Acordo de Nível de Serviço) é a parte do contrato que diz quanto o serviço precisa funcionar e o que acontece quando não funciona. Em telefonia, o número central é a disponibilidade: a porcentagem do tempo em que a linha, o tronco ou o 0800 recebeu e completou chamadas.

A fórmula é simples: disponibilidade = (tempo total − tempo indisponível) ÷ tempo total × 100. O difícil é o resto do acordo. Um SLA bem escrito define o período de apuração (mês ou ano), o que conta como indisponível (sem tom, sem áudio, chamada recusada), quem mede, o que fica de fora (como a janela de manutenção programada) e a compensação, geralmente desconto na fatura.

Outros indicadores costumam aparecer ao lado da disponibilidade, como o tempo de reação e de reparo, medidos por MTTA e MTTR. Sem medição independente, a empresa depende do relatório da própria operadora para saber se o SLA foi cumprido.

Na prática

Quanto tempo fora do ar cada meta permite:

SLA	Máximo por mês (30 dias)	Máximo por ano (365 dias)
99%	7 h 12 min	3 dias 15 h 36 min
99,5%	3 h 36 min	43 h 48 min
99,9%	43 min 12 s	8 h 45 min 36 s
99,99%	4 min 19 s	52 min 34 s

A diferença entre anual e mensal pesa: com 99,9% anual, uma queda de 6 horas em março não viola o contrato, mas violaria um SLA mensal de 99,9%. Faça a conta na calculadora de SLA e veja o método completo no guia de SLA de telefonia.

Como o Monitor usa isso

Os relatórios de SLA são mensais e trazem o número dos últimos 12 meses, que decide um SLA anual, e o do mês, como referência. Períodos em que o monitoramento ficou sem visibilidade por causa da 2N5 ficam fora do cálculo, para não pesar contra a linha do cliente nem a favor dela.

Perguntas frequentes

Como calcular a disponibilidade de um tronco?

Divida o tempo em que o tronco funcionou pelo tempo total do período e multiplique por 100. Em um mês de 30 dias (43.200 minutos) com 90 minutos fora do ar, a disponibilidade é (43.200 − 90) ÷ 43.200 × 100 = 99,79%. O ponto decisivo é como o tempo fora do ar é medido: por chamadas reais, por chamados abertos ou pelo relatório da própria operadora.

SLA anual ou mensal: qual é melhor para o cliente?

O mensal costuma proteger mais. Com 99,9%, o mensal tolera cerca de 43 minutos por mês, enquanto o anual tolera cerca de 8 horas e 45 minutos no ano inteiro. Uma única queda de 6 horas cabe no anual, mas viola o mensal com folga. No anual, a apuração precisa acompanhar os últimos 12 meses para saber se a meta ainda está de pé.

GLOSSÁRIO

STIR/SHAKEN: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** STIR/SHAKEN é o conjunto de padrões que assina digitalmente o número de origem de uma chamada SIP, para que a rede de destino possa verificar se o identificador de chamadas é legítimo.

Em inglês: STIR/SHAKEN (Secure Telephone Identity Revisited / Signature-based Handling of Asserted information using toKENs)

O que é STIR/SHAKEN?

STIR/SHAKEN é um conjunto de padrões para combater a falsificação do número de origem em chamadas SIP. A operadora de origem assina digitalmente o número de quem liga, e a rede de destino confere essa assinatura antes de entregar a chamada. STIR é a parte do IETF, com os protocolos; SHAKEN é o modelo de uso que define como as operadoras aplicam esses protocolos.

Quatro RFCs formam a base. A RFC 8224 define o cabeçalho Identity, que leva a assinatura dentro da mensagem INVITE. A RFC 8225 define o PASSporT, um token assinado com o número de origem, o número de destino e o horário. A RFC 8226 define os certificados que provam que quem assina tem direito sobre os números. A RFC 8588 acrescenta a extensão SHAKEN, com o nível de atestação e um identificador de origem.

Na verificação, a rede de destino baixa o certificado indicado no cabeçalho, confere a assinatura, checa se o horário é recente e compara os números do token com os da chamada. O resultado pode virar um selo de verificado na tela, um aviso de chamada suspeita ou um bloqueio, conforme a política de cada operadora.

Na prática

Campos principais de um PASSporT com a extensão SHAKEN:

Campo	Exemplo	Significado
attest	A	Nível de atestação: A, B ou C
orig	5511345670000	Número de origem
dest	5521987650000	Número de destino
iat	1759838400	Horário da assinatura, em segundos Unix
origid	identificador único	Ponto da rede onde a chamada entrou

Se o token chega com `iat` antigo ou com um `orig` diferente do número da chamada, a verificação falha, mesmo com a assinatura correta. Isso evita que um token válido seja copiado e reaproveitado em outra chamada.

Como o Monitor usa isso

O Monitor não assina nem autentica o identificador de chamadas. As chamadas de teste verificam se o número atende, qual foi a resposta SIP final e se o áudio passa. A assinatura STIR/SHAKEN fica com a operadora que origina a chamada. Veja o monitoramento de troncos SIP.

Perguntas frequentes

O que significam as atestações A, B e C?

São os níveis de confiança que a operadora de origem declara, definidos na RFC 8588. A (completa): a operadora conhece o cliente e sabe que ele pode usar o número. B (parcial): conhece o cliente, mas não pode garantir o número. C (gateway): a chamada chegou de outra rede, como um gateway internacional, e a operadora não sabe de onde ela veio.

STIR/SHAKEN impede chamadas com número falso?

Não sozinho. Ele dá à rede de destino uma informação verificável sobre o número de origem e sobre o nível de confiança da operadora que assinou. O que fazer com essa informação, como exibir um selo de verificado, marcar a chamada como suspeita ou bloqueá-la, é decisão de cada operadora. Uma chamada com número falso ainda pode chegar com atestação C.

GLOSSÁRIO

Tronco E1: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Tronco E1 é o circuito digital de 2,048 Mbit/s entre a operadora e o PABX que transporta até 30 canais de voz simultâneos, com sinalização ISDN ou R2.

Em inglês: E1 trunk

O que é um tronco E1?

Tronco E1 é uma conexão digital dedicada entre a operadora e o PABX da empresa, com taxa de 2,048 Mbit/s. Ela é dividida em 32 intervalos de tempo de 64 kbit/s: o intervalo 0 cuida do sincronismo, o intervalo 16 leva a sinalização e os 30 restantes levam um canal de voz cada. Por isso um E1 comporta até 30 chamadas simultâneas.

Existem duas formas de sinalização. No ISDN (PRI), o intervalo 16 transporta mensagens como SETUP, CONNECT e RELEASE, e o motivo do encerramento de cada chamada vem como uma causa Q.850 na mensagem de liberação, como 17 (ocupado) ou 34 (sem circuito disponível). No R2, muito usado no Brasil, a sinalização é feita por sinais de linha e de registro, com um conjunto menor de informações sobre o motivo da falha.

O E1 é anterior à telefonia IP, mas continua presente em muitas empresas, muitas vezes ligado a um PABX IP por um gateway. As causas Q.850 do ISDN são as mesmas que o SIP leva no cabeçalho Reason, o que facilita comparar falhas entre os dois tipos de tronco.

Na prática

Comparação entre E1 e tronco SIP:

Característica	E1	Tronco SIP
Meio	Circuito físico dedicado	Rede IP ou internet
Capacidade	30 canais por E1	Definida em contrato
Crescimento	De 30 em 30 canais	Por alteração no contrato
Sinalização	ISDN ou R2	SIP
Motivo da falha	Causa Q.850 (ISDN)	Resposta SIP e causa Q.850
Pontos sensíveis	Sincronismo, cabo, equipamento	Link, NAT, SIP ALG, codecs

Com 30 canais ocupados, a próxima chamada que chega recebe ocupado, com causa Q.850 34 no ISDN. No R2, a mesma situação aparece como um sinal de ocupado, sem a causa detalhada.

Como o Monitor usa isso

O Monitor liga para o número, então funciona da mesma forma se o número estiver em um tronco E1 ou SIP. O teste não depende do tipo de tronco: ele mostra se a chamada completou e por que falhou. Veja o monitoramento de troncos SIP.

Perguntas frequentes

E1 ou SIP: qual escolher?

O E1 tem capacidade fixa de 30 canais, circuito físico dedicado e qualidade previsível, mas exige instalação e cresce de 30 em 30 canais. O tronco SIP usa a rede de dados, aumenta canais por contrato e costuma custar menos, mas depende do link, do firewall e da configuração de NAT. Muitas empresas migram para SIP e mantêm o E1 como contingência.

Quantas chamadas simultâneas cabem em um E1?

Até 30. O E1 tem 32 intervalos de tempo de 64 kbit/s: o intervalo 0 serve para sincronismo, o intervalo 16 leva a sinalização e os outros 30 levam voz. Se a empresa precisa de 45 chamadas simultâneas, precisa de dois E1, ou de um E1 somado a um tronco SIP. A 31ª chamada recebe sinal de ocupado.

GLOSSÁRIO

Tronco SIP: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** Tronco SIP é a conexão de voz entre o PABX de uma empresa e a operadora feita por rede IP, com sinalização SIP e áudio em RTP, no lugar de linhas físicas ou E1.

Em inglês: SIP trunk

O que é um tronco SIP?

Tronco SIP é a conexão entre o PABX IP da empresa e a operadora feita pela rede de dados, seja pela internet, seja por um link dedicado. A sinalização usa SIP e a voz viaja em pacotes RTP. Ele substitui as linhas analógicas e o tronco E1: os canais deixam de ser físicos e passam a ser definidos em contrato.

A operadora identifica o tronco de duas formas: por registro SIP, com usuário e senha, ou por endereço IP, quando aceita chamadas apenas de IPs conhecidos. Entre o PABX e a internet costuma haver um firewall ou um SBC, que cuida de NAT, segurança e normalização das mensagens.

Cada chamada depende de várias coisas ao mesmo tempo: o link de internet, a autenticação, o limite de canais, a negociação de codecs e a passagem do RTP nos dois sentidos. Por isso um tronco SIP pode aparecer como registrado no PABX e, ainda assim, não completar chamadas ou completar sem áudio. A resposta SIP final de cada chamada mostra em qual dessas etapas a falha aconteceu.

Na prática

Falhas comuns de tronco SIP e a resposta que costumam gerar:

Sintoma	Resposta SIP típica	Causa provável
Chamada recusada logo no início	401 Unauthorized	Credenciais ou desafio de autenticação

Sintoma	Resposta SIP típica	Causa provável
Recusa em horário de pico	503 Service Unavailable	Limite de canais ou operadora indisponível
Recusa logo após a oferta	488 Not Acceptable Here	Nenhum codec em comum
Atende, mas um lado não ouve	200 OK	NAT ou SIP ALG alterando o SDP
Destino não atende	480 Temporarily Unavailable	Ramal ou destino fora do ar

A lista completa está em códigos SIP.

Como o Monitor usa isso

Uma chamada de teste real para um número do tronco passa por tudo de uma vez: autenticação, roteamento, limite de canais, codecs e áudio nos dois sentidos. A resposta SIP final dessa chamada diz em que ponto ela parou. Veja o monitoramento de troncos SIP.

Perguntas frequentes

Como saber se o tronco SIP está funcionando?

Fazendo uma chamada real por ele e conferindo três coisas: a resposta SIP final, o áudio nos dois sentidos e a qualidade da voz. O status de registrado no PABX só mostra que a sinalização chegou ao registrador. O tronco pode estar registrado e recusar chamadas por limite de canais, por codec incompatível ou por erro de roteamento na operadora.

Quantos canais preciso em um tronco SIP?

O número de chamadas simultâneas no horário de pico, com folga. Se o pico real é de 18 chamadas ao mesmo tempo, um contrato de 20 canais fica no limite; quando ele é atingido, a operadora recusa a próxima chamada, muitas vezes com 503 ou 486. O registro de chamadas do PABX mostra o pico real de cada dia.

GLOSSÁRIO

URA: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** URA (Unidade de Resposta Audível) é o sistema que atende chamadas sem atendente humano, toca mensagens gravadas e encaminha quem liga conforme as teclas DTMF ou a fala.

Em inglês: IVR (Interactive Voice Response)

O que é uma URA?

URA telefônica (Unidade de Resposta Audível, ou IVR em inglês) é o sistema que atende a ligação sem atendente humano, toca uma saudação gravada e oferece um menu como “digite 1 para financeiro, 2 para suporte”. Quem liga responde com as teclas do telefone, enviadas como tons DTMF, ou falando, nas URAs com reconhecimento de voz. A URA então transfere a chamada para uma fila, um ramal ou um serviço automático, como a segunda via de um boleto.

A URA costuma ficar dentro do PABX IP ou de uma plataforma de contact center, atrás de um número 0800, 0300 ou 4004. Por isso uma falha pode estar em vários pontos: no roteamento do número na operadora, no tronco, no PABX ou na própria aplicação da URA. Para quem liga, essas falhas parecem iguais: chamada muda, sinal de ocupado, mensagem da operadora ou saudação errada.

Uma característica ajuda muito no teste: a URA atende toda chamada. Ela não fica ocupada como uma pessoa nem deixa de atender porque saiu para almoçar. Se a ligação dá ocupado ou toca até cair, isso por si só já é sinal de problema.

Na prática

Uma empresa publica seu atendimento no 0800 e a URA atende no PABX. O que quem liga ouve, e o que isso costuma significar:

O que quem liga ouve	Resposta SIP típica	Situação
Saudação da empresa	200 OK	URA funcionando
“Não foi possível completar a ligação”	183 Session Progress, sem 200	Mensagem da operadora, a URA nem foi alcançada
Sinal de ocupado	486 Busy Here	Canais esgotados ou URA travada
Toca até cair	480 Temporarily Unavailable	URA não atendeu
Silêncio depois de atender	200 OK sem áudio	Falha no áudio (RTP)

Por exemplo, se a URA trava por 30 minutos em um horário com 2.000 chamadas por hora, cerca de 1.000 clientes ficam sem atendimento antes de alguém perceber pela queda no volume da fila.

Como o Monitor usa isso

Um circuito de URA passa quando a chamada é atendida e a saudação escolhida é ouvida. Se quem fala é a operadora, com uma mensagem de erro no lugar da saudação, o teste não passa. Ocupado ou sem resposta também conta como falha, porque uma URA atende toda chamada. Veja como funciona o monitoramento de 0800 e URA.

Perguntas frequentes

Como saber se a URA está fora do ar?

Ligando para ela como um cliente faria e ouvindo o que toca. Uma URA saudável atende e reproduz a saudação certa. Ocupado, toque sem resposta, silêncio depois de atender ou uma mensagem da operadora no lugar da saudação indicam falha. Olhar só o servidor da URA não basta, porque o problema pode estar no número, no tronco ou no roteamento da operadora.

URA e IVR são a mesma coisa?

Sim. URA é o nome usado no Brasil e IVR (Interactive Voice Response) é o termo em inglês. Os dois descrevem o sistema que atende a ligação, toca mensagens gravadas e direciona quem liga por meio de teclas ou reconhecimento de voz. Em documentação de fornecedores e de contact center, os dois nomes aparecem misturados.

GLOSSÁRIO

ViSQOL: definição e exemplo na prática

Por Equipe 2N5 Atualizado em 7 de outubro de 2026

> **Resposta curta:** ViSQOL (Virtual Speech Quality Objective Listener) é um algoritmo de código aberto do Google Research que compara um áudio recebido com sua referência e devolve uma nota MOS-LQO de 1 a 5.

Em inglês: ViSQOL (Virtual Speech Quality Objective Listener)

O que é ViSQOL?

ViSQOL (Virtual Speech Quality Objective Listener) é um algoritmo que dá uma nota de qualidade a um áudio comparando-o com o original. Ele foi criado pelo Google Research, é de código aberto e está publicado em github.com/google/visqol. A versão atual é descrita no artigo “ViSQOL v3”, de Chinen e outros, apresentado na conferência QoMEX em 2020.

O ViSQOL é um algoritmo de referência completa (full reference): precisa de dois arquivos, o áudio de referência e o áudio degradado. Ele alinha os dois no tempo, compara seus espectrogramas trecho a trecho e mede a semelhança espectro-temporal entre eles. Essa semelhança é convertida numa nota MOS-LQO, na mesma escala de 1 a 5 da MOS.

O algoritmo tem dois modos. O modo de fala (speech mode) trabalha com áudio em 16 kHz e devolve MOS-LQO de 1 a 5, com escala ajustada para chegar a 5,0. O modo de áudio (audio mode) foi pensado para música e áudio geral, e sua nota máxima fica perto de 4,75. As duas escalas não se misturam: uma nota 4,5 no modo de áudio não equivale a 4,5 no modo de fala.

Na prática

Modo	Uso	Taxa de amostragem	Nota máxima
Fala (speech)	Voz, telefonia	16 kHz	5,0
Áudio (audio)	Música, áudio geral	48 kHz	cerca de 4,75

Numa ligação com codec G.711, o áudio tem 8 kHz de amostragem. Para usar o modo de fala, referência e áudio recebido são levados a 16 kHz antes da comparação. A referência precisa ser o mesmo conteúdo que deveria chegar: se o destino toca uma saudação, a referência é essa saudação gravada. Se o áudio recebido for outro, como uma mensagem da operadora, a semelhança cai e a nota acompanha.

Para comparar notas

Notas de modelos diferentes não se misturam: cada algoritmo tem seu mapeamento e seu teto. Ao ler um relatório de MOS-LQO, confira qual modelo e qual modo geraram a nota. Veja qualidade de voz com MOS-LQO.

Perguntas frequentes

O ViSQOL é gratuito?

Sim. O ViSQOL é publicado pelo Google Research como código aberto, no repositório github.com/google/visqol. Qualquer pessoa pode baixar, compilar e rodar o algoritmo sobre seus próprios arquivos de áudio para conferir uma nota. Isso o diferencia do POLQA, a norma ITU-T P.863, que é distribuída sob licença comercial.

Qual modo do ViSQOL usar para chamadas telefônicas?

O modo de fala (speech mode), que trabalha com áudio em 16 kHz e devolve MOS-LQO numa escala de 1 a 5, com teto em 5,0. O modo de áudio foi feito para música e áudio geral em 48 kHz, e sua nota máxima fica perto de 4,75. Para voz em telefonia, o modo de fala é o adequado.

Guias

GUIA

Seu 0800 parou e ninguém avisou: como monitorar 0800 e URA

Um 0800 pode passar a noite fora do ar com todos os painéis verdes, porque a falha acontece antes de a chamada chegar ao seu equipamento. Este guia mostra por que isso acontece, como testar o 0800 e a URA de fora, o que as regras do SAC pedem e o que fazer quando o número não completa.

Por Equipe 2N5 Publicado em 7 de outubro de 2026 Atualizado em 20 de outubro de 2026

Resumo

- Um 0800 pode falhar antes de chegar ao seu PABX, na rota da operadora, na portabilidade ou na plataforma da URA, e nesse caso nenhum equipamento seu registra nada.
- Só uma chamada feita de fora, como um cliente faz, mostra se o 0800 completa e se a URA atende com a mensagem certa.
- Um 0800 que toca a mensagem da operadora, ou uma URA trocada sem aviso, está fora do ar para quem liga, mesmo com a chamada completando.
- O Decreto 11.034/2022 vale até 1º de novembro de 2026 e exige acesso ao SAC 24 horas por dia, 7 dias por semana, por pelo menos um canal (não necessariamente o telefone), e atendimento por telefone obrigatório, com no mínimo 8 horas diárias de atendimento humano. A partir de 2 de novembro de 2026 vale o Decreto 13.135/2026, que o revoga e exige telefone com atendimento humano das 8h às 20h e um canal eletrônico 24 horas.
- Para as prestadoras de telecomunicações, o RGC da Anatel (Resolução 765/2023) pede atendimento telefônico gratuito e disponível 24 horas.

Como um 0800 passa a noite fora do ar sem ninguém perceber?

Um 0800 passa a noite fora do ar sem alarme quando a falha acontece antes de a chamada chegar ao seu equipamento. O PABX não recebe nada, então não tem do que reclamar; o tronco SIP continua registrado; e, de madrugada, poucas chamadas é o normal. Só quem liga percebe, e quem liga desiste.

Uma noite, hora a hora

A linha do tempo abaixo é uma ilustração, montada para mostrar o mecanismo, e não um caso real. Os horários e a causa são hipotéticos; o padrão é o que importa.

Horário	O que acontece	O que os painéis mostram	O que quem liga ouve
01:50	Uma mudança na operadora quebra a rota do 0800 até o seu tronco	Tudo verde	Nada ainda
02:00	Primeira ligação depois da mudança	Nenhuma chamada no PABX; tronco SIP registrado	Silêncio, e a ligação cai

Horário	O que acontece	O que os painéis mostram	O que quem liga ouve
02:00 às 07:59	Clientes tentam e desistem	Volume baixo, o normal da madrugada	Silêncio
08:00	O atendimento humano começa	Filas vazias, atendentes livres	Silêncio
09:00	Um supervisor estranha a fila vazia e liga do próprio celular	Nada mudou	O supervisor ouve o silêncio
09:30	O chamado é aberto na operadora, sem horário de início nem código de erro	Nada mudou	Silêncio

O cliente que ligou às 2h não deixou rastro em nenhum equipamento da empresa. A queda começou às 01:50 e foi notada às 09:00: 7 horas e 10 minutos. E o chamado aberto às 9h30 começa fraco, porque ninguém sabe dizer quando a falha começou nem o que a rota respondia.

Na mesma noite, com uma chamada de teste a cada 15 minutos no ritmo padrão do Monitor, o teste das 02:00 falharia, as novas tentativas das 02:02, 02:04 e 02:06 também, e às 02:06 um incidente seria aberto com o código SIP de cada chamada, avisando a primeira camada da escada por e-mail. A diferença é de 6 horas e 54 minutos, das 02:06 às 09:00.

Por que os painéis ficaram verdes

Cada painel respondia a uma pergunta diferente da que importava:

- **o PABX** dizia que estava ligado, e estava; ele não tem como saber das chamadas que a operadora parou de entregar;
- **o tronco SIP** aparecia registrado, e estava; o registro diz à operadora para onde entregar as chamadas, mas a tradução do 0800 acontece em outro ponto da rede dela;
- **o gráfico de volume** mostrava poucas chamadas, o que de madrugada é normal.

Nenhuma dessas medidas está errada. Elas só não ligam para o 0800. O guia monitoramento de circuitos de voz compara o que cada método enxerga.

0800 fora do ar, 0800 não funciona, 0800 não completa: é a mesma coisa?

Para quem liga, é: o cliente não fala com a empresa. Para quem investiga, são sintomas diferentes. “Fora do ar” e “não funciona” descrevem o que o cliente percebe: o número não toca, cai, dá ocupado ou atende a mensagem errada. “Não completa” descreve o que a sinalização mostra: a chamada foi recusada ou não chegou ao destino. Um 0800 também “não funciona” quando completa e toca a mensagem da operadora ou uma URA trocada.

“Não funciona do celular” é um caso à parte: o número atende de algumas origens e de outras não. As causas estão em por que um 0800 não completa do celular. Em todos os casos o primeiro passo é o mesmo: ligar de fora, de mais de uma origem, e anotar o horário, o que se ouviu e o código SIP.

Por que um 0800 para de completar?

Um 0800 para de completar por falhas em qualquer ponto entre quem liga e quem atende: a rota da operadora, a portabilidade do número, a plataforma da URA, o tronco SIP por trás dela ou a própria mensagem, trocada sem aviso. Quase todos esses pontos ficam fora do seu PABX e não geram nenhum alarme nele.

A rota da operadora

Um 0800 não é um número geográfico. Ele é gratuito para quem liga, como define a Resolução 749/2022 da Anatel no art. 18, e a operadora o traduz para um destino: o seu tronco, um DDR ou a plataforma que hospeda a URA. Essa tradução é uma configuração na rede da operadora. Uma mudança de destino mal feita, um erro numa manutenção ou um problema de interconexão entre redes quebra a rota sem que nada mude do seu lado.

A rota também pode variar com a origem. Uma chamada de celular e uma de fixo, ou de operadoras diferentes, podem seguir caminhos diferentes até o mesmo 0800, e uma falha pode valer só para uma delas. O guia por que o 0800 não completa do celular trata desse caso.

A portabilidade do número

Quando o 0800 ou o número de destino muda de operadora, cada rede precisa passar a encaminhar as chamadas para a nova. Enquanto isso não acontece em todas, o número funciona de algumas origens e falha de outras. É uma falha parcial e traiçoeira: quem testa do próprio telefone pode estar justamente numa origem que já foi atualizada, e conclui que está tudo bem.

A plataforma da URA

A URA pode rodar no PABX, numa plataforma de contact center ou na nuvem. Quando essa plataforma cai, fica sem canais ou recebe um fluxo publicado com erro, a chamada toca sem ninguém atender, é recusada ou atende e cai. Se a plataforma é de terceiros, o seu PABX não participa da chamada e não vê a falha.

O tronco SIP por trás do 0800

Atrás da URA ou do destino do 0800 existe um tronco SIP, e ele tem os seus próprios pontos de falha: canais esgotados, que costumam aparecer como SIP 503 com a causa Q.850 34 (nenhum circuito ou canal disponível); o registro SIP perdido; um SBC com problema; ou um NAT e um SIP ALG que deixam a sinalização passar e barram o áudio, o que produz a ligação muda. O guia ligação muda e áudio de um lado só detalha esse último caso.

A saudação trocada sem aviso

Uma nova versão do fluxo da URA, a gravação de feriado que ficou ligada, uma mensagem de teste esquecida, ou uma mudança de rota que manda o 0800 para a URA de outro cliente da plataforma. A chamada completa e, para a sinalização, tudo funcionou. Quem liga, porém, ouve a mensagem errada, e para ele o 0800 está fora do ar.

Early media: a mensagem gravada no lugar do toque

Antes de atender, uma rota pode enviar áudio: é o early media, descrito no RFC 3960, que costuma chegar junto com a resposta 183 Session Progress. Ele serve para tocar o sinal de chamada, mas também para as mensagens da operadora, como “este número não existe” ou “este número está temporariamente indisponível”.

Para quem liga, a experiência parece uma chamada que andou: ouviu-se uma voz. Mas a sua empresa nunca atendeu, e o seu PABX nunca viu essa chamada. Um monitoramento que só confere se houve áudio passaria nesse teste. Por isso o teste de um 0800 precisa comparar o que ouviu com a saudação esperada, e não apenas detectar som.

Como testar o 0800 e a URA de fora?

Teste o 0800 de fora ligando como um cliente liga: de outra operadora, de celular e de fixo, e nos horários em que ninguém da equipe está olhando. Para a URA, confira se a saudação que atende é a esperada. Um teste feito de dentro da própria rede não passa pela rota da operadora e não vê a falha dela.

O teste manual

Um teste manual bem feito segue sempre os mesmos passos, para que o resultado sirva de evidência:

1. **Ligue de pelo menos duas origens:** um celular e um fixo, de preferência de operadoras diferentes da que atende o 0800.
2. **Anote o horário com segundos** e o número de origem de cada tentativa.
3. **Ouça o que acontece antes do atendimento:** silêncio, sinal de chamada, sinal de ocupado ou uma mensagem da operadora.
4. **Confira a saudação:** é a da sua empresa, a versão atual, com o primeiro menu certo?
5. **Faça o teste da URA telefônica:** digite uma opção do primeiro menu e veja se a URA reconhece o tom. O DTMF costuma viajar dentro do RTP, como descreve o RFC 4733, e uma falha de negociação faz a URA não reconhecer as teclas, mesmo com a voz passando.
6. **Repita fora do horário comercial** pelo menos uma vez, porque a URA pode mudar de fluxo à noite.

O teste manual tem um limite óbvio: ninguém liga às 3h de domingo, a cada 15 minutos. Ele serve para investigar e para conferir depois de uma mudança, não para vigiar.

O teste automático

O teste automático é uma chamada de teste agendada, feita de uma plataforma fora da sua rede, que liga para o número e julga o resultado sozinha. No Monitor, as chamadas partem da plataforma da 2N5 para os números de atendimento, 0800, 0300, 4004 e números fixos, e cada número tem a sua agenda, em intervalos ou em horários fixos, inclusive à noite e nos fins de semana.

Na implantação, a 2N5 grava a saudação de referência de cada número. Cada chamada de teste compara o que ouviu com essa gravação: uma mensagem diferente, como a de uma operadora dizendo que o número não existe, não passa. Para uma URA, ocupado, sem atendimento ou tocar até o fim também é falha, porque ela deveria atender toda chamada sozinha. A mesma comparação mede a qualidade de voz, o MOS-LQO, uma nota de 1 a 5 na terminologia da ITU-T P.800.1.

Duas regras protegem as pessoas. O áudio de uma chamada de teste só é guardado quando quem atende é a gravação ou a URA informada, criptografado e guardado pelo prazo que a 2N5 definir; a voz de uma pessoa nunca é guardada. E se o circuito puder ser atendido por uma pessoa, ela ouve uma mensagem avisando que é um teste automático, e a chamada termina.

Sobre o custo: as chamadas de teste fazem parte do serviço. Para um 0800, como para qualquer ligação recebida, a tarifa de entrada segue o seu contrato com a operadora. Veja monitoramento de 0800 e URA.

O que uma chamada de teste não vê

Uma chamada que ouve a saudação e desliga não navega pelo menu. Ela não confere se cada opção leva à fila certa, se o DTMF é reconhecido ou se há atendentes humanos disponíveis no horário. Esses pontos pedem o teste manual depois de cada mudança no fluxo.

E um teste que parte sempre da mesma origem não vê uma falha que vale só para outra, como o 0800 que não completa de um celular de determinada operadora. O teste automático vigia o caminho todo, a toda hora; o teste manual de outras origens completa o quadro.

O que o decreto do SAC e a Anatel exigem do 0800?

Até 1º de novembro de 2026, o Decreto 11.034/2022 exige que o SAC fique acessível 24 horas por dia, 7 dias por semana, por pelo menos um canal (não necessariamente o telefone), e torna obrigatório o atendimento por telefone, com no mínimo 8 horas diárias de atendimento humano. A partir de 2 de novembro de 2026, o Decreto 13.135/2026 revoga o 11.034 e mantém o telefone obrigatório, com atendimento humano das 8h às 20h todos os dias (art. 14), e exige ao menos um canal eletrônico 24 horas (art. 12). Nenhum dos dois decretos diz que o 0800 precisa funcionar 24 horas. Para as prestadoras de telecomunicações, o RGC da Anatel pede atendimento telefônico gratuito e disponível 24 horas. Medir a disponibilidade do 0800 é a forma de mostrar que essas regras foram cumpridas.

Regra	O que pede
Decreto 11.034/2022 (até 1º/11/2026), art. 4º	Acesso ao SAC 24 horas por dia, 7 dias por semana, por pelo menos um canal
Decreto 11.034/2022 (até 1º/11/2026), art. 4º, § 2º	Atendimento por telefone obrigatório
Decreto 11.034/2022 (até 1º/11/2026), art. 5º, I	Atendimento humano por telefone de no mínimo 8 horas por dia
Decreto 11.034/2022 (até 1º/11/2026), art. 5º, II	Opções de reclamação e de cancelamento no primeiro menu
Decreto 11.034/2022 (até 1º/11/2026), art. 12, § 3º	Gravações das chamadas guardadas por no mínimo 90 dias
Decreto 13.135/2026 (a partir de 2/11/2026), art. 14	Atendimento por telefone obrigatório; atendimento humano das 8h às 20h, todos os dias
Decreto 13.135/2026 (a partir de 2/11/2026), art. 12	Pelo menos um canal eletrônico 24 horas por dia, 7 dias por semana
Decreto 13.135/2026 (a partir de 2/11/2026), art. 15, I	Espera de até 20 segundos para 80% das demandas e 300 segundos para as demais, salvo regra do regulador
Decreto 13.135/2026 (a partir de 2/11/2026), art. 19	Gravações das chamadas guardadas por no mínimo 90 dias
Anatel, RGC (Res. 765/2023), art. 15	Atendimento telefônico gratuito e disponível 24 horas; atendente humano 24 horas para demandas urgentes e das 6h às 22h para as demais
Anatel, RGC (Res. 765/2023), art. 18	Primeiro menu com cancelamento automático, reclamação e atendimento humano
Anatel, Res. 749/2022, art. 18	0800 gratuito para quem liga; 0300 e 0303 com custo compartilhado

O Decreto 11.034 vale para os SACs dos setores regulados desde 3 de outubro de 2022 até 1º de novembro de 2026, e o Decreto 13.135 vale a partir de 2 de novembro de 2026. O RGC vale para as prestadoras de telecomunicações desde 1º de setembro de 2025.

As regras dizem o que precisa estar disponível; mostrar que esteve é trabalho de quem opera o 0800. Uma chamada de teste a cada 15 minutos, com o resultado de cada uma guardado, é um registro hora a hora de que o número completava e a URA atendia com a saudação esperada. Os relatórios de SLA do Monitor mostram a disponibilidade de cada número no ano e no mês, com cada falha e o momento em que alguém assumiu. O conteúdo do primeiro menu, por sua vez, é conferido por quem ouve a URA a cada mudança.

O que quem liga ouve em cada falha do 0800, e o que o teste registra?

Cada falha de um 0800 soa de um jeito para quem liga e deixa um rastro diferente numa chamada de teste real. A tabela abaixo liga a causa provável, o que o cliente ouve e o que o teste registra, para que a primeira mensagem para a operadora já diga em que ponto procurar.

Falha	O que quem liga ouve	O que uma chamada de teste real registra
A operadora não encontra o destino do 0800	Silêncio e queda, ou a mensagem de número inexistente	SIP 404, ou early media com a mensagem da operadora, que não bate com a referência
A rota recusa a chamada	Silêncio, um sinal de erro ou uma mensagem	SIP 403 ou SIP 603, com a causa Q.850 quando vier
O tronco por trás do 0800 sem canais	Sinal de ocupado ou mensagem de congestionamento	SIP 503, por exemplo com a causa Q.850 34
A plataforma da URA fora do ar	Toca sem atender, ou cai	SIP 480 ou SIP 408; tocar até o fim é falha para uma URA
A URA ocupada	Sinal de ocupado	SIP 486: falha para uma URA
Codecs incompatíveis na rota	A chamada não completa	SIP 488
A saudação trocada sem aviso	Outra mensagem, de feriado, antiga ou de outra empresa	Chamada atendida, mas a saudação não bate com a gravação de referência: falha
Ligação muda	Atende e fica em silêncio	Chamada atendida sem a saudação esperada: falha
Áudio de um lado só	Quem liga ouve, mas não é ouvido	Num circuito com tom de teste ou eco, os tons enviados não voltam: falha
Voz picotada	A saudação com cortes e ruído	MOS-LQO abaixo de 3,0: a chamada conta como degradada
A URA não reconhece as teclas	A URA repete o menu ou diz que a opção é inválida	Não aparece numa chamada que só ouve a saudação: pede o teste manual

Duas leituras valem para qualquer linha. Um 0800 que toca sem atender e uma rota que cancela a chamada aparecem para quem testa como falta de atendimento, às vezes com SIP 487 quando o próprio teste desistiu de esperar; um SIP 180 seguido de nada não é sucesso. E a mesma resposta SIP pode vir com causas Q.850 diferentes, que a operadora usa para achar o ponto da rede. A lista de causas Q.850 e a consulta de código SIP ajudam a ler cada uma.

O que fazer quando o 0800 para?

Quando o 0800 para, confirme a falha de outra origem, descubra se as chamadas chegam ao seu equipamento, junte as evidências e abra o chamado na operadora com elas. Enquanto a operadora trabalha, avise a equipe de atendimento e reforce os outros canais do SAC. Depois, registre o início e o fim da queda do 0800.

1. **Confirme de fora.** Ligue de um celular e de um fixo, de operadoras diferentes. Se uma origem completa e outra não, anote quais: isso aponta para a rota ou para a portabilidade.
2. **Veja se as chamadas chegam até você.** No SBC ou no PABX, procure os INVITEs das tentativas no horário em que elas foram feitas. Se nenhum chegou, a falha está antes de você, na operadora ou na plataforma da URA. Se chegaram e foram recusadas, a falha está do seu lado.
3. **Junte as evidências.** O número chamado, as origens, o horário de cada tentativa com segundos e fuso, o código SIP, a causa Q.850 quando vier, o Call-ID e a gravação da mensagem que tocou, se tocou alguma. Guarde também a última chamada que funcionou.
4. **Abra o chamado com tudo na primeira mensagem.** Peça o número de protocolo e pergunte em que ponto da rota a chamada para. Um chamado com horário e código de erro é mais difícil de encerrar com “nenhum defeito encontrado”.
5. **Proteja o atendimento.** Avise a equipe do SAC e os supervisores, e reforce os outros canais de atendimento enquanto o 0800 estiver fora. Se o contrato com a operadora prevê um destino alternativo para o 0800, peça o desvio.
6. **Feche com números.** Registre o início e o fim da queda, porque é isso que entra no SLA do mês e do ano. O guia SLA de telefonia: cálculo anual e mensal mostra a conta. E pergunte por que a sua equipe soube pelo cliente, e não por um alerta.

No Monitor, os passos 1 e 3 acontecem sozinhos. Quatro falhas seguidas, por padrão (a primeira e três novas tentativas), abrem um incidente com um bloco pronto para colar no chamado: o circuito, a operadora, o primeiro sintoma, o código SIP e a causa Q.850 de cada chamada e a última chamada saudável. A escada de escalonamento avisa a primeira camada por e-mail e sobe até alguém assumir com um toque no link do e-mail. Quando duas chamadas boas seguidas confirmam a volta, o incidente fecha e os contatos do cliente são avisados. Veja alertas e escalonamento.

Uma ressalva vale para qualquer monitoramento: se o problema estiver do lado de quem testa, o teste não diz nada sobre o 0800. No Monitor, um teste que não pôde ser feito por um problema do lado da 2N5 fica sem visibilidade, não conta contra o número, não entra no SLA e não acorda a sua equipe.

Com que frequência testar o 0800?

Teste o 0800 com a frequência que a meta de disponibilidade exige e nos horários em que ninguém olha. Com uma chamada a cada 15 minutos e novas tentativas a cada 2 minutos, uma queda de madrugada no 0800 vira incidente em até 21 minutos; com uma chamada por hora, pode passar uma hora inteira antes do primeiro sinal.

A conta do pior caso: uma queda que começa logo depois de um teste bom leva até 15 minutos para ser vista, mais 6 minutos para as três novas tentativas confirmarem, ou 15 + 6 = 21 minutos até o incidente. No ritmo de 15 minutos, cada número recebe 24 × 4 = 96 chamadas de teste por dia, cada uma ocupando um canal por poucos segundos, dentro de um limite de chamadas que nunca disputa canal com os clientes.

Três cuidados ajudam a escolher a agenda:

- **A madrugada e o fim de semana contam mais.** É quando o 0800 fica sozinho. Um 0800 de atendimento 24 horas precisa de teste 24 horas.
- **Horários fixos completam o intervalo.** Um teste num horário marcado, por exemplo pouco antes da abertura do atendimento humano, confirma o número no momento em que mais clientes vão ligar.

- **Cada número de atendimento é um circuito.** Se a empresa tem um 0800 para clientes, um 4004 e um número de cobrança, cada um tem a sua rota e a sua URA, e cada um precisa do seu teste. O guia monitoramento de circuitos de voz mostra como escolher o que monitorar.

O objetivo é simples de dizer: na próxima vez que o 0800 parar às 2h, a primeira pessoa a saber deve ser alguém da sua equipe, às 2h04, com o código SIP na mão, e não um cliente, às 9h.

Perguntas frequentes

Por que o meu 0800 não completa?

A falha pode estar fora do seu PABX: a operadora deixou de rotear o 0800 até o seu destino, uma portabilidade não foi atualizada em todas as redes, a plataforma da URA caiu ou o tronco SIP por trás dela ficou sem canais. O código SIP e a causa Q.850 de uma chamada de teste mostram em que ponto a chamada parou.

Como testar um 0800 de madrugada sem ninguém precisar ligar?

Com chamadas de teste agendadas, feitas de fora da sua rede, que ligam para o 0800 como um cliente e conferem o que atendeu. No Monitor, cada número tem a sua agenda, em intervalos ou em horários fixos, inclusive à noite e nos fins de semana, e cada chamada compara a saudação ouvida com a gravação de referência.

O 0800 completou, mas toca a mensagem da operadora. Está fora do ar?

Para quem liga, sim: o cliente não fala com a sua empresa. Essa mensagem costuma chegar como early media, antes de qualquer atendimento, ou numa chamada atendida pela própria operadora. Um monitoramento que só confere se houve áudio deixa isso passar; é preciso comparar o que foi ouvido com a saudação esperada da URA.

O que o decreto do SAC exige do 0800?

Até 1º de novembro de 2026, o Decreto 11.034/2022 exige acesso ao SAC 24 horas por pelo menos um canal, atendimento por telefone obrigatório, atendimento humano de no mínimo 8 horas diárias e reclamação e cancelamento no primeiro menu. A partir de 2 de novembro, o Decreto 13.135/2026 o revoga e exige telefone com atendimento humano das 8h às 20h e um canal eletrônico 24 horas. Nenhum dos dois cita o 0800.

O que fazer primeiro quando o 0800 para?

Confirme de outra origem, ligando de um celular e de um fixo de operadoras diferentes. Depois veja se as chamadas chegam ao seu SBC ou PABX: se nenhuma chega, a falha está antes de você. Junte o horário, o código SIP, a causa Q.850 e o Call-ID de cada tentativa e abra o chamado na operadora com essas evidências.

Meu 0800 está fora do ar ou só não funciona do celular?

Teste de um fixo e de celulares de pelo menos duas operadoras, no mesmo horário. Se todos falham, o número está fora do ar para quem liga, e o problema costuma estar na rota da operadora, na portabilidade, na URA ou no tronco. Se só os celulares falham, o suspeito é uma restrição de origem ou uma rota móvel; o guia por que o 0800 não completa do celular lista as causas.

Fontes

1. Decreto nº 11.034/2022: regras do SAC, incluindo acesso 24 horas e atendimento telefônico (vale até 1º de novembro de 2026)
2. Decreto nº 13.135/2026, arts. 12, 14, 15 e 19: novo decreto do SAC, que revoga o 11.034 e vale a partir de 2 de novembro de 2026
3. Anatel, Resolução nº 765/2023 (RGC), arts. 15 e 18: atendimento telefônico e primeiro menu
4. Anatel, Resolução nº 749/2022, art. 18: 0800 gratuito para quem liga, 0300 e 0303 com custo compartilhado
5. RFC 3261: SIP e os códigos de resposta
6. RFC 3960: early media, o áudio antes do atendimento
7. RFC 4733: DTMF transportado no RTP
8. RFC 6432: causas Q.850 no cabeçalho Reason das respostas SIP
9. ITU-T P.800.1: terminologia MOS, incluindo MOS-LQO

GUIA

Alerta de queda de linha sem falso alarme

Um alerta de queda de linha só serve se for verdadeiro: quem é acordado às 2h por um falso alarme logo para de olhar. No Monitor da 2N5, uma chamada que falha é refeita antes de qualquer aviso, só quatro falhas seguidas abrem um incidente, e o aviso chega por e-mail, subindo de camada em camada até alguém confirmar.

Por Equipe 2N5 Publicado em 14 de outubro de 2026 Atualizado em 20 de outubro de 2026

Resumo

- Falso alarme é alerta de uma falha que não existia, e é o maior motivo para a equipe deixar de confiar no monitoramento.
- A defesa é o reteste: a chamada que falha é repetida, e um incidente só abre depois de quatro falhas seguidas, a primeira e três novas tentativas.
- O alerta chega por e-mail, com as evidências e um link; um toque no link confirma que alguém assumiu.
- Se ninguém confirma no tempo combinado, o alerta sobe para a camada seguinte, e depois para os administradores da empresa.
- O e-mail traz o horário, o código SIP e a causa Q.850 de cada chamada, para a equipe agir sem abrir o sistema.

Como receber alerta de queda de linha sem falso alarme?

Com três defesas em sequência: refazer a chamada que falhou, exigir falhas seguidas antes de abrir o incidente e só então avisar, por camadas, até alguém confirmar. Cada defesa corta um tipo de falso alarme, e juntas fazem com que um aviso no celular às 2h signifique que o circuito caiu de verdade.

O que é um falso alarme na telefonia?

Falso alarme é o aviso de uma falha que não existiu, ou que já tinha passado quando o aviso chegou. Na telefonia, as causas mais comuns são:

- **uma chamada de teste que falhou uma vez** por um solavanco na rota e voltou a funcionar na seguinte;
- **um problema do lado do próprio monitoramento**, que não consegue testar mas acusa o circuito;
- **uma manutenção programada** que ninguém avisou ao monitoramento;
- **um limite curto demais** para a oscilação normal da rede.

O custo é a confiança. Quando muitos alertas são falsos, a equipe passa a ignorar todos, e o alerta verdadeiro se perde no meio.

Por que testar de novo antes de alertar?

Porque uma única falha quase nunca diz o suficiente. O Monitor da 2N5 liga para cada circuito, por padrão, a cada 15 minutos. Quando uma chamada falha, ela é repetida três vezes, a cada 2 minutos. O incidente abre com quatro falhas seguidas, a primeira e três novas tentativas; duas chamadas boas seguidas confirmam a volta.

Momento	O que acontece
A chamada de teste falha	Nada é avisado; o teste é repetido em 2 minutos
Segunda e terceira falhas	Ainda nada é avisado
Quarta falha seguida	O incidente abre, com as evidências de cada chamada: horário, código SIP e causa Q.850
Uma chamada boa no meio	A contagem recomeça; a oscilação não vira alerta
Duas chamadas boas seguidas	O circuito volta, e o incidente fecha

A conta da espera: uma queda que começa logo depois de um teste bom é vista, no máximo, 15 minutos depois, e a quarta falha chega 6 minutos mais tarde (2 + 2 + 2). Em troca desses minutos, o alerta passa a ser confiável. Quando a falha é do lado da 2N5, o teste fica sem visibilidade, não conta contra o circuito e nunca acorda a sua equipe.

Por onde o alerta chega?

Por e-mail, com as evidências, os códigos e os números do incidente, e com um link que confirma que a pessoa assumiu o incidente, sem precisar entrar no sistema.

Cada pessoa pode ter mais de um endereço de e-mail dentro da camada; se um não está disponível, a mensagem segue pelo próximo, sem esperar.

Como funciona o escalonamento?

O alerta sobe em camadas, até alguém assumir. A camada 1 é avisada quando o incidente abre. Se ninguém confirma no tempo definido para a camada, avisa-se a camada 2, depois a 3. Uma única confirmação, com um toque no link da mensagem, para a subida, e o incidente passa a mostrar quem assumiu e quando.

Quem	Quando é avisado
Camada 1	Quando o incidente abre
Camadas seguintes	Quando a anterior não confirma no tempo definido
Administradores da empresa	Quando nenhuma camada confirma
Contatos do cliente	Quando um serviço tem problema e quando é resolvido; não fazem parte da subida

O tempo até a primeira confirmação alimenta o relatório de SLA como resposta média, o que mostra o quanto a equipe demora para assumir. O glossário explica MTTR e MTTA.

Como evitar alerta durante uma manutenção?

Com uma janela de manutenção: os circuitos escolhidos, num horário marcado, deixam de abrir incidente. A janela precisa existir antes do início; uma manutenção declarada depois da queda é só uma queda. O que passar do horário combinado volta a contar.

O que mais reduz o falso alarme?

- **Medir a chamada, não o equipamento.** Um tronco registrado não prova que a chamada completa; o falso verde é o outro lado do falso alarme.

- **Comparar a URA com a gravação de referência**, para que a mensagem da operadora não passe por atendimento.
- **Ter alguém por camada**, e não uma pessoa só: uma escada com uma camada só vira falso silêncio quando essa pessoa está sem sinal.
- **Registrar as manutenções antes.**

Para saber mais sobre o caminho completo, veja alertas e escalonamento e como funciona. Quando o incidente abre, o guia Chamadas falhando: diagnóstico ajuda a ler os códigos, e o Como cobrar o SLA da operadora com provas mostra o que fazer com o registro.

Perguntas frequentes

Como receber alerta quando a linha cair?

Cadastre o e-mail da pessoa como contato do Monitor da 2N5. Quando um incidente é confirmado, a mensagem chega com as evidências e um link, e um toque nele confirma que você assumiu.

O que é reteste antes de alertar?

É repetir a chamada que falhou, depois de um intervalo curto, antes de avisar alguém. Uma oscilação de um minuto, uma rota que falhou uma vez ou uma chamada perdida não chegam a ser alerta. No Monitor da 2N5, a chamada é repetida três vezes, a cada 2 minutos, e só quatro falhas seguidas abrem o incidente.

Quanto tempo passa entre a queda e o alerta?

Com o ritmo padrão, uma queda é vista na próxima chamada de teste, em até 15 minutos, e as três novas tentativas somam mais 6 minutos até a quarta falha. O aviso sai logo depois de o incidente abrir. O intervalo entre testes e o número de tentativas existem para trocar alguns minutos por um alerta confiável.

E se ninguém responder ao alerta?

O alerta sobe: se a primeira camada não confirma no tempo definido, avisa a segunda, depois a terceira. Quando nenhuma camada confirma, os administradores da empresa são avisados. Uma única confirmação, com um toque no link, para a subida e registra quem assumiu e quando.

Posso silenciar os alertas durante uma manutenção?

Sim. Uma janela de manutenção cobre os circuitos escolhidos num horário marcado, e as falhas desses circuitos durante a janela não abrem incidente. A janela precisa ser registrada antes de começar; o que passar do horário combinado volta a contar como queda.

Fontes

1. RFC 3261: SIP, os códigos de resposta que a chamada de teste registra
2. ITU-T E.800: definições de qualidade de serviço, incluindo disponibilidade
3. RFC 6432: causas Q.850 no cabeçalho Reason das respostas SIP

GUIA

Chamadas falhando: como diagnosticar pelo código SIP e pela causa Q.850

Quando as chamadas de um tronco SIP ou de um 0800 começam a falhar, o código SIP e a causa Q.850 da primeira chamada que falhou dizem em que ponto ela parou e de quem é o próximo passo. Este guia reúne os códigos que mais aparecem, 503, 486, 480, 487 e 603, e as causas 16, 34 e 127, com a pergunta certa a fazer para cada um.

Por Equipe 2N5 Publicado em 14 de outubro de 2026 Atualizado em 14 de outubro de 2026

Resumo

- O código SIP diz o que o servidor decidiu fazer com a chamada; a causa Q.850 diz o motivo, no cabeçalho Reason, e quase sempre é o que a operadora usa para localizar a falha.
- SIP 503 com causa 34 é falta de canal ou de rota, e SIP 486 com causa 17 costuma ser o limite de canais simultâneos esgotado.
- SIP 480 é destino sem registro ou indisponível, SIP 487 é uma chamada cancelada antes de atender e SIP 603 é uma recusa explícita.
- Causa 16 é encerramento normal e não é erro; causa 127 é um motivo que a rede não informou.
- Para abrir chamado na operadora, junte o horário com fuso, o número chamado, o código SIP, a causa Q.850 e o Call-ID de cada tentativa.

Por onde começar quando as chamadas falham?

Pelo código da primeira chamada que falhou, não pela reclamação. Cada chamada recusada devolve um código SIP, e muitas devolvem também uma causa Q.850 no cabeçalho Reason (RFC 6432). Os dois juntos dizem em que ponto a chamada parou e quem pode resolver.

Um caminho curto, na ordem:

1. **Reúna as tentativas**: horário com fuso, número de origem, número chamado, código SIP, causa Q.850 e Call-ID de cada uma.
2. **Veja se a chamada chegou ao seu SBC ou PABX.** Se nenhuma chegou, a falha está antes, na rota da operadora.
3. **Leia o código na tabela abaixo** e siga a página dele para o detalhe.
4. **Repita de outras origens**: um fixo e celulares de operadoras diferentes mostram se a falha vale para todas.

Uma chamada de teste agendada ajuda muito aqui: ela já traz o horário, o código e a causa de cada tentativa, inclusive das que ninguém viu. Veja o que é monitoramento sintético de chamadas.

Que código SIP significa o quê?

Código	O que significa	Causa mais comum num tronco ou 0800	Próximo passo
503 Service Unavailable	O servidor está temporariamente incapaz de processar a chamada	Falta de canal ou de rota na operadora, ou um SBC fora do ar	Ler o Retry-After e a causa Q.850; abrir chamado com o Call-ID se persistir
486 Busy Here	O destino foi alcançado, mas não pode aceitar outra chamada	Limite de canais simultâneos esgotado	Comparar as chamadas ativas no momento com o limite contratado
480 Temporarily Unavailable	O destino foi localizado, mas não está disponível agora	Destino sem registro, em Não Perturbe ou sem atender	Verificar o registro do destino e o Retry-After
487 Request Terminated	O pedido foi encerrado por um CANCEL antes do atendimento	Quem ligou desligou tocando, ou o PABX desistiu por tempo esgotado	Não é falha do destino; investigar só quando for excessivo
603 Decline	O destino foi contatado e recusou a chamada de forma explícita	A pessoa rejeitou, ou um bloqueio de chamadas	Ver se a recusa veio do destino, do PABX ou da operadora

Para os outros códigos, o índice de códigos SIP tem uma página para cada um, e a consulta de código SIP abre o código digitado.

E as causas Q.850?

A causa Q.850 é o motivo que a rede informa para encerrar a chamada, vinda da telefonia tradicional e carregada pelo SIP no cabeçalho Reason. As três que mais geram dúvida:

Causa	O que indica	Quando investigar
16, Normal call clearing	Encerramento normal: uma das pontas desligou depois de a chamada ser estabelecida	Só quando muitas chamadas terminam com 16 em poucos segundos, sem áudio ou logo após a URA atender
34, No circuit/channel available	Não havia circuito ou canal livre para completar a chamada	Sempre: costuma ser limite de canais esgotado, seu ou da operadora
127, Interworking, unspecified	A chamada passou por uma interconexão que não informa o motivo	Descobrir em que trecho a chamada falhou e qual resposta veio dali

O índice de causas Q.850 lista as demais.

Como ligar o código SIP à causa Q.850?

Os dois se encaixam. O SIP 503 aparece muito com a causa 34 (falta de canal), mas também com outras, como a 38, a 41 e a 88. O SIP 486 costuma vir com a causa 17, destino ocupado. O SIP 603 combina com a 21, chamada rejeitada. O SIP 480 vem com as causas 19, 20 e 31, e o SIP 487 não tem causa associada, porque é um cancelamento. O mapeamento entre as duas famílias está na RFC 3398.

Quais padrões de falha merecem atenção?

- **Muitos 503 com causa 34 num horário de pico**: capacidade do tronco esgotada. Compare o pico de chamadas simultâneas com os canais contratados.
- **486 e causa 17 numa URA ou 0800**: costuma ser o mesmo limite de canais, aparecendo como “ocupado”.

- **480 num ramal ou numa URA que deveria atender**: destino sem registro. Confira o registro SIP.
- **Muitos 487 seguidos**: o PABX está desistindo antes de a chamada ser atendida, ou quem liga desiste tocando. Veja depois de quantos segundos veio o CANCEL.
- **Causa 16 em chamadas muito curtas**: o encerramento é normal, mas o problema pode estar antes. Veja quem mandou o BYE e se houve áudio nos dois sentidos.
- **Causa 127 em chamadas que passam por um gateway**: o motivo se perdeu na conversão entre redes. Peça à operadora o código de origem.

O que levar para a operadora?

Uma tabela, uma linha por tentativa: horário com fuso, número de origem, número chamado, código SIP, causa Q.850, Call-ID e o que se ouviu. É o que a operadora consegue localizar nos próprios registros. O guia Como cobrar o SLA da operadora com provas mostra como transformar esses registros em uma cobrança.

Como o Monitor da 2N5 usa esses códigos?

Cada chamada de teste do Monitor da 2N5 registra o código SIP e a causa Q.850 devolvidos, e as quatro falhas seguidas que abrem um incidente chegam ao alerta com essas evidências. Veja o monitoramento de troncos SIP e o monitoramento de 0800 e URA.

Perguntas frequentes

Por que as minhas chamadas estão falhando no tronco SIP?

Olhe o código SIP da primeira falha e a causa Q.850 do cabeçalho Reason. Um 503 com causa 34 aponta falta de canal ou de rota; um 486, o limite de canais; um 480, destino sem registro; um 603, recusa explícita. Sem o código, qualquer diagnóstico é palpite. Registre o horário, o número chamado e o Call-ID de cada tentativa.

O que significa SIP 503 Service Unavailable e quando preocupa?

SIP 503 Service Unavailable significa que o servidor está temporariamente incapaz de processar a chamada, por sobrecarga ou manutenção. Em troncos, o mais comum é falta de canal ou de rota na operadora, ou um SBC fora do ar. Preocupa quando se repete: leia o Retry-After e a causa Q.850 e abra chamado com o Call-ID.

Causa Q.850 16 é erro?

Não. A causa 16, Normal call clearing, é o encerramento normal: uma das pontas desligou depois de a chamada ser estabelecida. É o valor mais comum nos registros de chamadas. Só merece investigação quando muitas chamadas terminam com 16 em poucos segundos, sem áudio ou logo depois de a URA atender, porque aí o desligamento pode ser consequência de outro problema.

Qual a diferença entre o código SIP e a causa Q.850?

O código SIP é a resposta do protocolo, como 503 ou 486, e tem classes: 4xx é falha do pedido, 5xx é falha do servidor e 6xx é falha global. A causa Q.850 vem da telefonia tradicional e dá o motivo com mais precisão, como a 34 de falta de canal. A RFC 6432 define como a causa viaja no cabeçalho Reason.

Como saber se o problema é da operadora ou da minha rede?

Veja se a chamada chega ao seu SBC ou PABX. Se nenhuma chegar, a falha está antes de você, na rota da operadora, e o código e o horário de cada chamada de teste são a prova para o chamado. Se chegar e for recusada pela sua regra de entrada, o problema está na sua configuração.

O que significa erro SIP 503 / 486 / 480 / 408?

O 503 é serviço indisponível: em troncos, falta de canal ou de rota na operadora, ou um SBC fora do ar. O 486 é ocupado, normalmente o limite de canais. O 480 é destino temporariamente indisponível, como um número sem registro. O 408 é tempo esgotado: a chamada não teve resposta, por rota ou firewall. Leia o código sempre junto com a causa Q.850 e o horário de cada chamada.

O que é a causa Q.850 16 / 34 / 127?

A causa Q.850 é o motivo da desconexão, definido pela telefonia tradicional, que viaja no cabeçalho Reason da resposta SIP. A 16 é encerramento normal da chamada, e não um erro. A 34 é falta de circuito ou canal disponível. A 127 é interfuncionamento sem causa especificada: a chamada passou por uma rede que não informa o motivo, e o defeito pode estar em qualquer trecho.

Fontes

1. RFC 3261: SIP, as classes de respostas e os códigos 4xx, 5xx e 6xx
2. RFC 6432: causas Q.850 no cabeçalho Reason das respostas SIP
3. RFC 3398: o mapeamento entre causas Q.850 e códigos de resposta SIP
4. ITU-T Q.850: as causas de encerramento de chamada

GUIA

Como cobrar o SLA da operadora com provas

Para cobrar o SLA de uma operadora, a empresa precisa mostrar, queda por queda, o que aconteceu e quando: o horário, o número chamado, o código SIP, a causa Q.850 e o tempo fora do ar, já com as manutenções descontadas. Uma queda que o cliente percebeu é difícil de contestar; uma que o teste registrou, não.

Por Equipe 2N5 Publicado em 14 de outubro de 2026 Atualizado em 20 de outubro de 2026

Resumo

- A cobrança começa no contrato: o período de medição, o que conta como indisponibilidade, a janela de manutenção e quem mede.
- A prova é um registro feito no momento, de fora da rede, com horário, número chamado, código SIP e causa Q.850 de cada chamada de teste.
- A disponibilidade é (período − manutenção − tempo fora do ar) ÷ (período − manutenção) × 100; a calculadora de SLA faz a conta para qualquer meta.
- Em 99,9%, o limite é de 8 h 45 min 36 s fora do ar por ano de 365 dias, ou 43 min 12 s por mês de 30 dias.
- O tempo em que o próprio monitoramento ficou sem visibilidade não é queda do circuito e deve ficar fora da conta.

Como cobrar o SLA da operadora?

Em três partes: o que o contrato promete, o que foi medido e a conta entre os dois. Sem a primeira, não se sabe o que cobrar; sem a segunda, não há o que mostrar; sem a terceira, a cobrança é uma opinião. Um SLA só é cobrável quando alguém mediu.

O que o contrato precisa dizer?

Antes de aceitar uma meta, combine por escrito:

1. **o período de medição** (ano ou mês) e o fuso horário;
2. **o que conta como indisponibilidade**: só a chamada que não completa, ou também a chamada muda e a qualidade abaixo do limite;
3. **como a manutenção é avisada** e qual a janela máxima;
4. **quem mede, e como**: a medição da operadora, a sua, ou uma independente;
5. **qual evidência vale** para abrir uma contestação, e o prazo para pedir o crédito.

Se o contrato já existe e não diz isso, a primeira cobrança serve também para combinar o critério. O guia SLA de telefonia: cálculo anual e mensal detalha cada ponto.

Que provas levar?

Uma prova boa é um registro feito na hora, de fora da sua rede, que a operadora consegue conferir. Para cada queda:

Campo	Para que serve
Horário de início e de fim, com fuso	Mede a duração e localiza a falha nos registros da operadora
Número chamado e número de origem	Diz qual circuito e qual rota falharam
Código SIP de cada chamada de teste	Mostra como a rota recusou, por exemplo SIP 503
Causa Q.850	Dá o motivo, como a causa 34
Call-ID	Permite à operadora achar a chamada exata
O que se ouviu	Distingue silêncio, ocupado e mensagem da operadora
Duração e resultado das chamadas seguintes	Mostra quando o circuito voltou

Os códigos e as causas estão explicados em Chamadas falhando: diagnóstico. Uma queda registrada com esses campos é difícil de contestar; a percebida por um cliente que reclamou, não.

Como calcular a disponibilidade?

Disponibilidade = (período – manutenção programada – tempo fora do ar) ÷ (período – manutenção programada) × 100. A calculadora de SLA do site faz essa conta para qualquer meta e já considera as janelas de manutenção: use a Calculadora de SLA.

Duas referências para a conversa com a operadora, em 99,9%:

Período	Tempo fora do ar permitido
Ano de 365 dias	8 h 45 min 36 s
Mês de 30 dias	43 min 12 s

Cada queda entra na conta pelo tempo medido, e o tempo medido depende da frequência do teste: com uma chamada a cada 15 minutos e novas tentativas a cada 2 minutos depois de uma falha, o início e o fim de cada queda ficam marcados com poucos minutos de margem.

O que fica fora da conta?

- **Manutenção programada**, avisada e dentro da janela combinada.
- **Falhas causadas pelo próprio cliente**, como um PABX desligado na filial, quando o contrato é com a operadora e o defeito não está nela.
- **O tempo em que o monitoramento ficou sem visibilidade** por um problema dele mesmo. Um teste que não pôde ser feito não diz nada sobre o circuito.

Colocar essas exceções no relatório, e não escondê-las, é o que torna o número defensável: a operadora percebe que a conta é honesta.

Como montar a cobrança, passo a passo?

1. **Junte o relatório do período** (ano ou mês, conforme o contrato) com as quedas e a disponibilidade.
2. **Liste as quedas** em uma tabela, uma por linha, com os campos acima.
3. **Desconte as manutenções** que foram avisadas dentro da janela.
4. **Compare com a meta** e calcule a diferença em minutos.
5. **Abra o chamado** com a tabela e o relatório, e peça que a operadora confira as rotas nos horários indicados.

6. **Guarde os relatórios** mês a mês. O número dos últimos 12 meses é o que fecha o ano.

O crédito, a multa ou a rescisão são o que o contrato prever; a forma de pedir e o prazo também. Isso é assunto para o seu jurídico, e este guia não é parecer jurídico.

O que o Monitor da 2N5 entrega?

O Monitor da 2N5 liga do Brasil para cada circuito de voz, em agenda própria, e guarda o resultado de cada chamada de teste. Todo mês envia por e-mail um relatório de SLA com a disponibilidade do mês e dos últimos 12 meses, cada incidente com a duração, o tempo total fora do ar e a disponibilidade por circuito e por operadora. Um período em que o teste não pôde ser feito por um problema do lado da 2N5 fica fora da conta e aparece separado. Para uma obrigação do atendimento ao consumidor, veja também Decreto do SAC e RGC.

Perguntas frequentes

Como cobrar o SLA da operadora?

Abra o chamado com um relatório de disponibilidade e a lista de quedas: horário e fuso de cada falha, número chamado, código SIP, causa Q.850 e duração. Some o tempo fora do ar, desconte as manutenções avisadas e compare com a meta do contrato. Confira antes se o contrato define a forma de contestação e o prazo para pedir o crédito.

Que provas valem na contestação com a operadora?

Vale o que a operadora consegue localizar nos próprios registros: horário com fuso, número de origem e destino, código SIP, causa Q.850 e Call-ID de cada tentativa. Um registro feito no momento, por chamadas de teste de fora da rede, é mais difícil de contestar do que a lembrança de que o número ficou fora do ar.

99,9% de disponibilidade é quanto tempo fora do ar?

Em um ano de 365 dias, 8 horas, 45 minutos e 36 segundos. Em um mês de 30 dias, 43 minutos e 12 segundos. Em uma semana, 10 minutos e 5 segundos. Em um dia, 1 minuto e 26 segundos. A calculadora de SLA do site mostra o valor para outras metas e inclui as janelas de manutenção.

A manutenção programada conta como queda?

Normalmente não, se foi avisada com a antecedência que o contrato pede e ficou dentro da janela combinada: ela sai do período antes da conta. O que passa da janela conta como queda a partir do momento em que a janela terminou. Por isso a janela precisa estar registrada antes de começar.

O que fazer se a operadora contesta a medição?

Mostre a sequência de chamadas de teste do período, com o resultado de cada uma, e peça que ela confira as rotas nos horários indicados. Se o contrato diz quem mede, use essa medição como referência e a sua como evidência de apoio. Dúvidas de interpretação do contrato são para o seu jurídico.

Fontes

1. ITU-T E.800: definições de qualidade de serviço, incluindo disponibilidade

2. RFC 3261: SIP, os códigos de resposta que ficam no registro de cada chamada
3. RFC 6432: causas Q.850 no cabeçalho Reason das respostas SIP
4. Anatel, Resolução nº 765/2023 (RGC), art. 15: atendimento telefônico disponível 24 horas

GUIA

Decreto do SAC e RGC da Anatel: como provar que o 0800 e a URA estavam no ar

Os decretos do SAC (o 11.034/2022, que vale até 1º de novembro de 2026, e o 13.135/2026, que o revoga e vale a partir de 2 de novembro de 2026) e o Regulamento Geral de Direitos do Consumidor da Anatel dizem o que o atendimento por telefone precisa oferecer, mas não dizem como provar que ele estava disponível. Este guia resume os artigos que tratam do canal telefônico e mostra como chamadas de teste e um relatório de disponibilidade documentam o ano inteiro.

Por Equipe 2N5 Publicado em 7 de outubro de 2026 Atualizado em 14 de outubro de 2026

Resumo

- Até 1º de novembro de 2026 vale o Decreto 11.034/2022 (em vigor desde 3 de outubro de 2022, art. 18): acesso ao SAC 24 horas por dia, 7 dias por semana, por pelo menos um canal, e atendimento por telefone obrigatório (art. 4º), com no mínimo 8 horas diárias de atendimento humano (art. 5º, I).
- A partir de 2 de novembro de 2026 vale o Decreto 13.135/2026, que revoga o 11.034 (art. 24) e entra em vigor vinte dias depois da publicação de 13 de outubro de 2026 (art. 25). Ele mantém o telefone obrigatório (art. 14), com atendimento humano das 8h às 20h todos os dias, e exige ao menos um canal eletrônico 24 horas (art. 12).
- O 11.034 não fixa o tempo máximo de espera: manda os órgãos reguladores definirem esse tempo (art. 5º, III). O 13.135 fixa até 20 segundos para pelo menos 80% das demandas e até 300 segundos para as demais, salvo regra específica do regulador (art. 15, I e § 1º).
- Para as prestadoras de telecomunicações, o RGC da Anatel (Resolução 765/2023), em vigor desde 1º de setembro de 2025, exige atendimento telefônico gratuito e disponível 24 horas (art. 15).
- Nenhum dos dois decretos menciona o 0800, e nenhuma das normas diz como provar a disponibilidade; um registro de chamadas de teste feitas de fora, com horário e resultado de cada uma, é uma forma de documentá-la.
- Este guia não é parecer jurídico: como cada norma se aplica à sua empresa deve ser confirmado com o seu jurídico.

O que é o decreto do SAC?

O decreto do SAC é o Decreto nº 11.034, de 5 de abril de 2022, que vale até 1º de novembro de 2026. A partir de 2 de novembro de 2026, o decreto do SAC é o Decreto nº 13.135, de 9 de outubro de 2026, que revoga o 11.034. Os dois regulamentam o Código de Defesa do Consumidor para fixar as regras do Serviço de Atendimento ao Consumidor. O 11.034 vale para os fornecedores de serviços regulados pelo Poder Executivo federal, e cada órgão regulador aplica essas regras ao seu setor, considerando o porte do fornecedor.

O art. 1º do Decreto 11.034 define o alcance: o decreto vale “no âmbito dos fornecedores dos serviços regulados pelo Poder Executivo federal”, e o parágrafo único manda os órgãos reguladores considerarem “o porte do fornecedor do serviço regulado”. O art. 2º define o SAC como o atendimento

feito por diversos canais integrados para tratar demandas como informação, dúvida, reclamação, contestação, suspensão ou cancelamento de contratos e serviços. A oferta e a contratação de produtos ficam de fora.

Um detalhe que muda a leitura: **o Decreto 11.034 não lista setores pelo nome**. Quem define como ele se aplica a cada setor é o regulador desse setor (arts. 5º, 13 e 14). Por isso, "o decreto vale para a minha empresa?" tem duas partes: se o seu serviço é regulado pelo Executivo federal e o que a norma do seu regulador diz. O Decreto 13.135 também deixa ao regulador competente definir os critérios de aplicação (art. 1º, parágrafo único, I) e acrescenta um grupo nomeado: os fornecedores que, por plataformas ou outros meios digitais, ofertem ou prestem serviços financeiros, de pagamento, de crédito ou outros de natureza financeira ao consumidor e estejam sujeitos à regulação ou à supervisão do Banco Central do Brasil (art. 1º, parágrafo único, II).

Quando o Decreto 11.034 entrou em vigor?

O Decreto 11.034 entrou em vigor em 3 de outubro de 2022. O art. 18 diz que ele vale "cento e oitenta dias após a data de sua publicação", e a publicação no Diário Oficial da União foi em 6 de abril de 2022. O mesmo decreto revogou o Decreto nº 6.523/2008, a regra anterior do SAC.

A revogação está no art. 17. Quem ainda cita as regras de 2008 em contratos, manuais ou roteiros de URA está citando um texto que não vale mais. O texto do Planalto traz o aviso de que não substitui o publicado no Diário Oficial; para uso formal, a referência é a publicação oficial. O Decreto 11.034 deixa de valer quando o Decreto 13.135 entra em vigor, em 2 de novembro de 2026, como descreve a próxima seção.

O que muda com o Decreto 13.135, e a partir de quando?

O Decreto nº 13.135, de 9 de outubro de 2026, publicado no Diário Oficial da União de 13 de outubro de 2026, regulamenta de novo o SAC e, no art. 24, revoga o Decreto 11.034. O art. 25 o faz entrar em vigor vinte dias depois da publicação, o que, pela contagem do prazo, é 2 de novembro de 2026. Assim, **o Decreto 11.034 vale até 1º de novembro de 2026, e a partir de 2 de novembro de 2026 vale o Decreto 13.135**. Confirme a data no texto publicado no Diário Oficial.

O que o Decreto 13.135 diz sobre o telefone e o canal 24 horas, com os artigos:

- o atendimento por canais telefônicos é obrigatório (art. 14, caput);
- o atendimento telefônico por pessoa humana vai das 8h às 20h, sem interrupção, sete dias por semana, e pode ser precedido de menu eletrônico (art. 14, § 1º); nas demandas urgentes, é imediato e a qualquer tempo (art. 14, § 2º, e art. 17);
- se o atendimento humano por telefone for interrompido antes de terminar, o fornecedor deve retornar a chamada em até trezentos segundos (art. 14, § 3º);
- o tempo máximo de espera pelo atendente é de até vinte segundos para pelo menos 80% das demandas atendidas e de até trezentos segundos para as demais, salvo regra específica do regulador (art. 15, I e § 1º);
- a opção de falar com uma pessoa deve existir em todos os níveis do atendimento telefônico (art. 15), e o cancelamento imediato e o atendimento humano devem estar disponíveis inclusive no primeiro nível (art. 16, § 2º);
- ao menos um canal eletrônico de comunicação deve funcionar 24 horas por dia, sete dias por semana, com atendimento em tempo real por pessoa humana das 8h às 20h (art. 12 e § 1º); a chamada telefônica, definida no art. 3º, § 1º, é um canal à parte;

- o acesso é gratuito em todos os canais (art. 8º);
- as gravações das chamadas ficam guardadas por no mínimo noventa dias (art. 19), e o histórico de cada demanda por no mínimo seis meses depois da resolução (art. 18, § 4º, II).

O novo texto não fala em 0800 e não exige que o telefone funcione 24 horas: o que funciona 24 horas é um canal eletrônico, e só as demandas urgentes têm atendimento humano por telefone a qualquer tempo. Nada nele exige um 0800 24 horas. O RGC é uma norma da Anatel, com a sua própria exigência de 24 horas para as prestadoras de telecomunicações, descrita adiante; este guia não verificou se a Anatel vai atualizar o RGC por causa do novo decreto.

Ponto	Decreto 11.034 (até 1º de novembro de 2026)	Decreto 13.135 (a partir de 2 de novembro de 2026)
Telefone	Obrigatório (art. 4º, § 2º)	Obrigatório (art. 14)
Atendimento humano por telefone	No mínimo 8 horas diárias (art. 5º, I)	Das 8h às 20h, todos os dias (art. 14, § 1º)
Acesso 24 horas	Pelo menos um dos canais integrados (art. 4º)	Pelo menos um canal eletrônico (art. 12)
Tempo máximo de espera	Fixado pelos reguladores (art. 5º, III)	20 segundos para 80% das demandas e 300 segundos para as demais, salvo regra do regulador (art. 15, I e § 1º)
Gratuidade	Art. 3º	Art. 8º
Gravações das chamadas	No mínimo 90 dias (art. 12, § 3º)	No mínimo 90 dias (art. 19)
Registro do atendimento	No mínimo dois anos (art. 12, § 5º)	Histórico por no mínimo seis meses após a resolução (art. 18, § 4º, II)
Quem alcança	Serviços regulados pelo Poder Executivo federal	Os mesmos critérios e, também, serviços financeiros sob regulação ou supervisão do Banco Central (art. 1º, parágrafo único)

Fonte: os textos do Decreto 11.034/2022 e do Decreto 13.135/2026 no Planalto. O restante deste guia descreve o Decreto 11.034, que vale até 1º de novembro de 2026, e o RGC da Anatel. A análise de como o novo decreto muda a sua obrigação é para o seu jurídico.

O que o Decreto 11.034 exige do atendimento por telefone, até 1º de novembro de 2026?

Até 1º de novembro de 2026, o Decreto 11.034 exige que o acesso ao SAC seja gratuito (art. 3º), disponível 24 horas por dia, 7 dias por semana, por pelo menos um canal (art. 4º), e que o atendimento por telefone exista (art. 4º, § 2º), com no mínimo 8 horas diárias de atendimento humano e reclamação e cancelamento no primeiro menu (art. 5º). A partir de 2 de novembro, valem as regras do Decreto 13.135, na seção anterior.

Artigo (Decreto 11.034)	O que diz	O que significa para o 0800 e a URA
Art. 3º	O acesso ao SAC é gratuito e o atendimento não gera ônus para o consumidor	O número de atendimento não pode cobrar de quem liga
Art. 4º, caput e § 1º	Acesso ininterrupto, 24 horas por dia, 7 dias por semana, por no mínimo um dos canais integrados	O canal 24 horas pode ser outro; o telefone não é obrigado a ser esse canal pelo decreto

Artigo (Decreto 11.034)	O que diz	O que significa para o 0800 e a URA
Art. 4º, § 2º	O acesso por atendimento telefônico é obrigatório, nos termos do art. 5º	O telefone tem de existir e funcionar nos horários do art. 5º
Art. 4º, § 4º	O acesso inicial ao atendente não pode depender de o consumidor informar dados antes	A URA não pode exigir CPF ou contrato para deixar falar com alguém
Art. 5º, I	Horário de atendimento não inferior a 8 horas diárias, com atendimento por humano	Atendente disponível pelo menos 8 horas por dia
Art. 5º, II	O primeiro menu tem obrigatoriamente as opções de reclamação e de cancelamento	A saudação e o primeiro menu da URA precisam oferecer essas opções
Art. 5º, III	Tempo máximo de espera para falar com o atendente e para a transferência, fixado pelos reguladores	O número vem da norma do setor, não do decreto

Fonte de todas as linhas: o texto do Decreto 11.034/2022 no Planalto.

Gratuidade (art. 3º)

O art. 3º do Decreto 11.034 diz que “o acesso ao SAC será gratuito e o atendimento das demandas não acarretará ônus para o consumidor”. Na numeração brasileira, o código que cumpre isso pelo próprio desenho é o 0800: pelo art. 18 da Resolução 749/2022 da Anatel, no 0800 a instituição assinante se responsabiliza pelo pagamento, “caracterizando uma chamada sem ônus para o usuário originador”. Os códigos 0300 e 0303, pela mesma resolução, são de custo compartilhado entre quem liga e o assinante. O guia Por que um 0800 não completa do celular? trata das restrições de origem que costumam aparecer nesse modelo de cobrança. O art. 8º do Decreto 13.135 também fixa o acesso gratuito em todos os canais.

24 horas por pelo menos um canal (art. 4º)

O caput do art. 4º do Decreto 11.034 pede acesso “ininterruptamente, durante vinte e quatro horas por dia, sete dias por semana”, e o § 1º diz que isso será garantido por “no mínimo, um dos canais de atendimento integrados”. Na leitura literal, o canal 24 horas pode ser um aplicativo ou um site, e o telefone, obrigatório pelo § 2º, segue as horas do art. 5º. O § 3º admite interromper o SAC quando o serviço não estiver disponível para uso ou contratação, observada a regra do setor. Os §§ 5º e 6º proíbem publicidade durante a espera sem consentimento prévio e permitem mensagens informativas. No Decreto 13.135, o funcionamento 24 horas passa a ser exigido de um canal eletrônico (art. 12), distinto da chamada telefônica (art. 3º, §§ 1º e 2º).

O mínimo do atendimento telefônico (art. 5º)

O art. 5º do Decreto 11.034 lista o que os reguladores devem observar no telefone: pelo menos 8 horas diárias com atendimento humano (inciso I), reclamação e cancelamento no primeiro menu (inciso II) e um tempo máximo de espera (inciso III). O parágrafo único permite aos reguladores exigir mais de 8 horas de atendimento humano. O art. 15, § 5º, dá a mesma possibilidade à Secretaria Nacional do Consumidor para fornecedores com SAC de baixa efetividade.

O que o Decreto 11.034 não fixa?

O Decreto 11.034 não fixa o tempo máximo de espera, o prazo de resolução por setor nem o prazo do processamento técnico de um cancelamento. Em todos esses pontos, ele manda o órgão regulador decidir. Também não fixa um horário de atendimento humano acima de 8 horas: só permite que o regulador o exija.

Os pontos em que o decreto delega ao regulador:

- **Tempo máximo de espera** (art. 5º, III): para o contato direto com o atendente e para a transferência ao setor competente. O decreto exige que exista um tempo máximo, mas não diz qual.
- **Mais horas de atendimento humano** (art. 5º, parágrafo único).
- **Prazo de resolução das demandas** (art. 13, § 4º). O decreto fixa só o prazo de resposta: sete dias corridos a partir do registro (art. 13, caput).
- **Prazo do processamento técnico do cancelamento** (art. 14, parágrafo único). Pelo art. 14, o cancelamento tem efeito imediato, salvo quando for necessário esse processamento.
- **O porte do fornecedor** (art. 1º, parágrafo único).

Na prática, quem procura “qual o tempo máximo de espera do SAC” precisa da norma do seu setor. Para telecomunicações, o RGC da Anatel deixa esse tempo e o conceito de “primeiro menu” para o Grupo de Implantação (art. 18, § 3º, da Resolução 765/2023). A partir de 2 de novembro de 2026, o Decreto 13.135 fixa o tempo (até vinte segundos para pelo menos 80% das demandas e até trezentos segundos para as demais, art. 15, I), mas não se aplica onde houver regra específica do regulador (art. 15, § 1º).

Que registros o decreto do SAC já obriga a guardar?

O decreto do SAC obriga a manter a gravação das chamadas ao SAC por no mínimo 90 dias e a dar um número de protocolo a cada demanda. Pelo Decreto 11.034, o registro de cada atendimento fica guardado por no mínimo dois anos após a resolução (art. 12); pelo Decreto 13.135, o histórico fica por no mínimo seis meses após a resolução (art. 18, § 4º, II). Nenhum desses registros mostra se o 0800 estava no ar quando ninguém conseguiu ligar.

O art. 12 do Decreto 11.034 garante ao consumidor acompanhar a demanda “por meio de registro numérico ou outro tipo de procedimento eletrônico”. O § 3º torna obrigatória “a manutenção da gravação da chamada efetuada para o SAC” por no mínimo noventa dias, e o § 4º permite ao consumidor pedir acesso a ela nesse prazo. O § 5º manda guardar o registro do atendimento por no mínimo dois anos. No Decreto 13.135, o consumidor acompanha a demanda por protocolo (art. 18), e as gravações das chamadas e o conteúdo das mensagens ficam guardados por no mínimo noventa dias (art. 19).

Todos esses registros nascem de uma chamada que chegou. Quando o 0800 não completa, não há chamada, não há gravação e não há protocolo. A ausência de registros num período pode ser falta de demanda ou falta de canal, e os registros do SAC sozinhos não distinguem uma coisa da outra.

O que é o RGC da Anatel?

O RGC é o Regulamento Geral de Direitos do Consumidor de Serviços de Telecomunicações, aprovado pela Resolução nº 765/2023 da Anatel. Ele vale para telefonia fixa, telefonia móvel, banda larga fixa e TV por assinatura, e está em vigor desde 1º de setembro de 2025. É a norma do setor de telecomunicações

que aplica o decreto do SAC.

A ligação com o decreto está no próprio texto: o art. 3º, V, do Anexo define o Atendimento Telefônico “nos termos previstos neste Regulamento e no Decreto nº 11.034, de 5 de abril de 2022”. Essa referência é do texto do RGC publicado; este guia não verificou se a Anatel vai atualizá-la depois da revogação do 11.034. O art. 1º do Anexo cobre o STFC, o SMP, o SCM e os serviços de TV por assinatura; o art. 2º exclui os acessos exclusivamente de IoT.

A vigência tem uma nota na página da Resolução 765 na Anatel: pelo Acórdão nº 228, de 28 de agosto de 2024, a maior parte do regulamento passou a valer em 1º de setembro de 2025, e o RGC anterior (Resolução 632/2014) foi revogado na mesma data.

Art. 15: o atendimento telefônico 24 horas

O art. 15 diz que o Atendimento Telefônico deverá: “I - ser gratuito; II - receber chamadas originadas do STFC e do SMP; III - estar disponível ininterruptamente, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e, IV - dispor de atendente humano durante 24 (vinte e quatro) horas para demandas urgentes e, para as demais, de 6 (seis) às 22 (vinte e duas) horas, ininterruptamente, 7 (sete) dias por semana.”

Aqui a diferença para o decreto é direta: para as prestadoras de telecomunicações, o **telefone** precisa estar disponível 24 horas, e não só algum canal. O inciso II também pesa: o número tem de receber chamadas de telefones fixos (STFC) e de celulares (SMP). O § 1º permite à Anatel alterar as horas de atendimento humano, e o § 2º deixa para o Manual Operacional a definição de “demandas urgentes”.

Art. 18: o primeiro menu

O art. 18 diz que no primeiro menu do Atendimento Telefônico deverão estar disponíveis, no mínimo, as opções de “I - rescisão do contrato de forma automatizada, sem intervenção de atendente; II - registro de reclamação; e, III - atendimento por humano”. O § 1º exige a opção de falar com o atendente em todos os submenus, e o § 3º deixa para o Grupo de Implantação o tempo máximo de espera e o conceito de primeiro menu.

Art. 91: prestadoras de pequeno porte

O art. 91 trata das Prestadoras de Pequeno Porte: o atendimento telefônico delas deve funcionar “no mínimo, pelo período de 8 (oito) horas, ininterruptamente, nos dias úteis”. O art. 90 lista os artigos que se aplicam a elas, e do art. 15 entram os incisos I e II (gratuidade e chamadas de fixos e celulares), mas não os incisos III e IV (24 horas e as horas de atendimento humano).

Ponto	Decreto 11.034/2022 (até 1º de novembro de 2026)	RGC, Resolução 765/2023
Quem cobre	Fornecedores de serviços regulados pelo Executivo federal, conforme o regulador de cada setor	Prestadoras de telefonia fixa e móvel, banda larga e TV por assinatura
Em vigor desde	3 de outubro de 2022	1º de setembro de 2025
Gratuidade	Art. 3º	Art. 15, I
Disponível 24 horas	O acesso ao SAC, por pelo menos um canal (art. 4º)	O próprio atendimento telefônico (art. 15, III)
Atendimento humano	No mínimo 8 horas por dia (art. 5º, I)	24 horas para urgências, 6h às 22h para o resto (art. 15, IV)
Primeiro menu	Reclamação e cancelamento (art. 5º, II)	Cancelamento automatizado, reclamação e humano (art. 18)

Ponto	Decreto 11.034/2022 (até 1º de novembro de 2026)	RGC, Resolução 765/2023
Tempo máximo de espera	Fixado pelos reguladores (art. 5º, III)	Definido pelo Grupo de Implantação (art. 18, § 3º)
Pequeno porte	O regulador considera o porte (art. 1º)	8 horas nos dias úteis (art. 91)

A partir de 2 de novembro de 2026, a coluna do decreto passa a ser a do Decreto 13.135, na tabela da seção sobre o novo decreto.

Como provar que o 0800 estava no ar?

Para provar que o 0800 estava no ar, é preciso um registro feito no momento, de fora da empresa, que mostre para cada horário se a chamada completou e se a URA atendeu com a mensagem certa. Nem o decreto nem o RGC dizem como provar a disponibilidade; chamadas de teste agendadas são uma forma de produzir esse registro.

Os sistemas da própria empresa contam a história de dentro. Um PABX ligado e um tronco registrado mostram que o equipamento funcionava, não que um cliente de fora completava a chamada. Quando o problema está na rota da operadora ou numa URA trocada, o painel continua verde.

O que uma chamada de teste registra

O Monitor, serviço gerenciado da 2N5, faz chamadas de teste reais para cada número de atendimento: 0800, 0300, 4004 e números fixos. Cada número monitorado é um **circuito de voz**, com a sua agenda e as pessoas que devem saber quando ele falha. A chamada parte da plataforma da 2N5, ouve o que atende e desliga. Para cada chamada fica registrado:

- o horário e o número chamado;
- se a chamada completou ou foi recusada, com o código SIP que a rota devolveu, como um SIP 503, e a causa Q.850 quando a rede a informa;
- se quem atendeu foi o esperado: na implantação, a 2N5 grava a saudação de referência da URA, e cada chamada compara o que ouviu com essa gravação. A mensagem de uma operadora dizendo que o número não existe não passa;
- se o áudio passou e a qualidade de voz medida no áudio, o MOS-LQO.

Os códigos SIP seguem a RFC 3261, e as causas Q.850 chegam no cabeçalho Reason definido pela RFC 6432. É o tipo de dado que a operadora consegue localizar nos registros dela.

Um cuidado com dados pessoais: o áudio de uma chamada de teste só é guardado quando quem atende é a gravação ou a URA informada, criptografado e pelo prazo que a 2N5 definir. A voz de uma pessoa nunca é guardada; se o número puder ser atendido por alguém, essa pessoa ouve antes que é um teste automático.

Por que o intervalo entre chamadas importa

Um registro só mostra o que mediu. Se o teste acontece uma vez por hora, uma queda de 40 minutos pode passar entre duas chamadas boas, e o período sai como disponível. No ritmo padrão do Monitor, cada número recebe uma chamada a cada 15 minutos. Quando uma chamada falha, ela é repetida três vezes, a cada 2 minutos; quatro falhas seguidas abrem um incidente, e duas chamadas boas seguidas confirmam a volta.

A conta da margem: uma queda que começa logo depois de uma chamada boa é vista, no máximo, 15 minutos depois, na chamada seguinte. Com as novas tentativas a cada 2 minutos, a quarta falha seguida chega 6 minutos depois da primeira (2 + 2 + 2). Uma oscilação isolada, que falha uma vez e volta, não abre incidente e não entra na conta.

Horários fixos, noites e fins de semana

A obrigação do art. 15, III, do RGC é de 24 horas, 7 dias por semana. Cada número monitorado tem a sua agenda, em intervalos ou em horários fixos, inclusive à noite e nos fins de semana. Só uma agenda que cobre o horário inteiro de obrigação permite dizer “testado durante todo o período”.

O relatório que documenta o ano

Todo mês, o Monitor envia por e-mail um relatório de serviço às pessoas que a empresa escolheu, em português ou em inglês. Ele traz a disponibilidade de cada circuito no mês e nos **últimos 12 meses**, que é o número que fecha o ano. Os 12 relatórios mensais, cada um com o seu número de 12 meses, cobrem o ano inteiro de obrigação.

Bloco do relatório	O que documenta
Disponibilidade de voz	O mês e os últimos 12 meses, contra a meta
Incidentes	Cada incidente, com a gravidade e a duração
Tempo fora do ar	O total no período, por circuito
Resposta média	O tempo até alguém assumir cada incidente
O período, dia a dia	Quais dias tiveram falha confirmada
Por circuito e por operadora	A disponibilidade de cada número e de cada operadora

Dois cuidados deixam o número defensável. O primeiro: um período em que a 2N5 não conseguiu testar por um problema do lado da 2N5 fica fora da conta e aparece separado; a falta de visibilidade do monitoramento nunca vira indisponibilidade do circuito. O segundo: uma manutenção programada precisa estar registrada antes, numa janela de manutenção com início e fim. O guia SLA de telefonia: cálculo anual e mensal mostra a conta, e a calculadora de SLA faz a conta para qualquer meta.

Exemplo com dados de demonstração: disponibilidade de 99,89% no mês e 99,91% nos últimos 12 meses, meta de 99,90% atingida, 4 incidentes e 3 h 55 min fora do ar no mês.

O que a chamada de teste não prova?

A chamada de teste prova que o número completava a partir da origem de onde ela liga e que a URA atendia com a mensagem esperada. Ela não prova o tempo de espera até o atendente, as horas de atendimento humano, o conteúdo de cada opção do menu nem que o número completava de todas as operadoras.

Exigência	Artigo	A chamada de teste mostra?
Canal telefônico disponível e atendendo	Decreto 11.034 art. 4º, § 2º; Decreto 13.135 art. 14; RGC art. 15, III	Sim, para cada horário testado, a partir da origem da 2N5
A URA certa atendendo	Nenhum artigo específico; é o que quem liga ouve	Sim, a saudação é comparada com a gravação de referência
Gratuidade para quem liga	Decreto 11.034 art. 3º; Decreto 13.135 art. 8º; RGC art. 15, I	Não; depende do código contratado, como o 0800

Exigência	Artigo	A chamada de teste mostra?
Chamadas de fixos e de celulares	RGC art. 15, II	Só da origem de onde o teste liga
Atendimento humano nas horas exigidas	Decreto 11.034 art. 5º, I; Decreto 13.135 art. 14, § 1º; RGC art. 15, IV	Não; a chamada ouve a saudação e desliga
Tempo máximo de espera	Decreto 11.034 art. 5º, III; Decreto 13.135 art. 15, I; RGC art. 18, § 3º	Não
Opções do primeiro menu	Decreto 11.034 art. 5º, II; Decreto 13.135 art. 16, § 2º; RGC art. 18	Só o que estiver na saudação comparada
Gravações e protocolos	Decreto 11.034 art. 12; Decreto 13.135 arts. 18 e 19	Não; são registros do próprio SAC

Cada origem segue a sua própria rota até o 0800, e uma rota pode falhar enquanto as outras funcionam. O teste da 2N5 não substitui um teste de cada operadora de celular quando a suspeita é uma restrição de origem.

Como montar o registro de disponibilidade do SAC?

O registro de disponibilidade do SAC se monta com quatro peças: a lista de números que o consumidor pode discar, o que deve atender cada um, uma agenda de testes que cubra todo o horário de obrigação e um relatório guardado mês a mês. Com isso, a empresa responde com dados quando alguém afirma que o telefone não atendia.

1. **Liste todos os números divulgados.** O art. 7º do Decreto 11.034 (e o art. 9º do Decreto 13.135) exige que os canais de acesso ao SAC constem dos documentos e canais do fornecedor; cada número divulgado, 0800, 0300 ou 4004, é um número que alguém vai discar.
2. **Defina o que deve atender cada número.** A gravação de referência distingue “atendeu a URA certa” de “atendeu a mensagem da operadora”.
3. **Cubra o horário inteiro de obrigação.** Para uma prestadora de telecomunicações, 24 horas por dia, 7 dias por semana (art. 15, III, do RGC). Para os outros setores, o horário que a norma do regulador fixar, com o atendimento humano por telefone das 8h às 20h todos os dias a partir de 2 de novembro de 2026 (art. 14, § 1º, do Decreto 13.135).
4. **Registre as manutenções antes.** Uma janela de manutenção com início e fim, marcada antes de começar. O que passar da janela é queda.
5. **Guarde os relatórios mensais.** O número de 12 meses de cada relatório é o que fecha o ano.
6. **Leve a evidência à operadora.** O horário, o número chamado, o código SIP e a causa Q.850 de cada chamada de teste localizam a falha na rota. A página Monitoramento de 0800 e URA mostra como o Monitor trata cada caso, e Relatórios de SLA mostra o relatório.

O que este guia não é

Este guia não é parecer jurídico. Ele resume o texto dos Decretos 11.034/2022 e 13.135/2026 e da Resolução 765/2023 da Anatel, nas versões publicadas nos sites oficiais, conferidas em 14 e 15 de outubro de 2026, quando o Decreto 13.135/2026 já estava publicado e ainda não em vigor (vigência a partir de 2 de novembro de 2026), e mostra uma forma técnica de documentar a disponibilidade do canal telefônico.

Três perguntas ficam para o seu jurídico: se o serviço da sua empresa está sujeito ao decreto; o que a norma do seu regulador diz sobre o atendimento telefônico, o tempo de espera e o atendimento humano; e que valor um registro de chamadas de teste tem num processo administrativo ou judicial. O texto que vale é o publicado no Diário Oficial da União.

Perguntas frequentes

O decreto do SAC obriga o 0800 a funcionar 24 horas?

Não. Pelo Decreto 11.034/2022 (até 1º de novembro de 2026), o SAC funciona 24 horas por pelo menos um canal, que não precisa ser o telefone, e o atendimento humano por telefone tem no mínimo 8 horas diárias (arts. 4º e 5º). Pelo Decreto 13.135/2026 (a partir de 2 de novembro), o canal 24 horas é eletrônico (art. 12), e o telefone tem atendimento humano das 8h às 20h (art. 14). Para telecomunicações, o RGC exige o telefone 24 horas.

Qual é o tempo máximo de espera no SAC, pelos Decretos 11.034 e 13.135?

O Decreto 11.034 não fixa um número: o art. 5º, III, manda os órgãos reguladores definirem o tempo máximo de espera. O Decreto 13.135 fixa, a partir de 2 de novembro de 2026, até vinte segundos para pelo menos 80% das demandas atendidas e até trezentos segundos para as demais (art. 15, I), salvo regra específica do regulador (art. 15, § 1º). Para telecomunicações, o RGC deixa o tempo para o Grupo de Implantação (art. 18, § 3º).

O que mudou com o RGC da Resolução 765/2023?

Desde 1º de setembro de 2025, o atendimento telefônico das prestadoras de telefonia, internet e TV por assinatura deve ser gratuito, receber chamadas de fixos e celulares e estar disponível 24 horas, com atendente humano 24 horas para demandas urgentes e das 6h às 22h para as demais (art. 15). O primeiro menu deve ter cancelamento automatizado, reclamação e atendimento humano (art. 18).

Como provar que o SAC estava disponível de madrugada?

Com registros feitos na hora, de fora da empresa. Uma chamada de teste para o 0800 em intervalos curtos, inclusive de madrugada, deixa para cada horário o resultado da chamada, o código SIP devolvido e se a URA atendeu com a mensagem esperada. Somados, esses registros dão a disponibilidade do período.

Este guia substitui a análise do jurídico?

Não. Ele resume o texto oficial dos decretos e do RGC e mostra uma forma de documentar a disponibilidade do canal telefônico. Se a sua empresa está sujeita a cada norma, e como a norma do seu regulador aplica o decreto ao seu setor, são perguntas para o seu jurídico.

O Decreto 11.034 foi revogado?

Foi revogado pelo Decreto 13.135, de 9 de outubro de 2026 (art. 24), publicado no Diário Oficial de 13 de outubro e em vigor vinte dias depois (art. 25), ou seja, a partir de 2 de novembro de 2026. O 11.034 vale até 1º de novembro de 2026; a partir de 2 de novembro vale o 13.135, que mantém o telefone obrigatório e o atendimento humano das 8h às 20h (art. 14).

Fontes

1. Decreto nº 11.034/2022: diretrizes e normas sobre o SAC (arts. 1º a 18)
2. Decreto nº 13.135/2026: novo decreto do SAC, que revoga o 11.034 (arts. 1º, 8º, 12, 14 a 16, 18, 19, 24 e 25)
3. Anatel, Resolução nº 765/2023 (RGC): atendimento telefônico, arts. 15, 18 e 91, e notas de vigência
4. Anatel, Resolução nº 749/2022 (Regulamento de Numeração), art. 18: código 0800 sem ônus para quem liga
5. RFC 3261: SIP e as classes de códigos de resposta
6. RFC 6432: causas Q.850 no cabeçalho Reason das respostas SIP

GUIA

Ligação muda e áudio de um lado só no VoIP: causas e como corrigir

A chamada completa, o cronômetro corre e um dos lados não ouve nada. Quase sempre a sinalização SIP funcionou e o áudio RTP se perdeu no caminho, num NAT, num firewall ou num endereço errado no SDP. Este guia mostra cada causa, onde conferir no Asterisk e no firewall, e como provar que o áudio voltou a passar nos dois sentidos.

Por Equipe 2N5 Publicado em 7 de outubro de 2026 Atualizado em 20 de outubro de 2026

Resumo

- Ligação muda (sem áudio nos dois sentidos) e áudio unidirecional são falhas do RTP, não do SIP: a chamada completa e o áudio não chega.
- A causa mais frequente é um endereço IP privado no SDP, anunciado por um PABX atrás de NAT sem o endereço externo configurado.
- O SIP ALG de roteadores e firewalls reescreve o SDP e costuma piorar o problema; a recomendação usual é desligá-lo e tratar o NAT no PABX.
- A faixa de portas UDP do RTP precisa estar aberta e encaminhada para o PABX; no Asterisk ela fica no rtp.conf, de 10000 a 20000 no exemplo padrão.
- Uma chamada que cai perto de 32 segundos indica ACK perdido: o 200 OK é retransmitido por 64 × T1, com T1 de 500 ms, e a sessão é encerrada.
- Um teste com serviço de eco ou tons prova os dois sentidos; os contadores de RTP enviados e recebidos mostram de que lado o áudio parou.

O que é ligação muda e o que é áudio de um lado só?

Ligação muda é a chamada VoIP que completa sem áudio em nenhum dos dois sentidos: ninguém ouve ninguém. Áudio de um lado só, ou áudio unidirecional, é a chamada em que um lado ouve e o outro não. Nos dois casos a sinalização SIP funcionou; o que falhou foi o caminho do áudio, o fluxo RTP.

Em inglês, os termos são *no-way audio* e *one-way audio*. Áudio de um lado só indica que um dos sentidos encontrou o caminho e o outro não, o que aponta quase sempre para endereço, NAT ou firewall de um lado específico. Ligação muda costuma apontar para algo que afeta o fluxo inteiro: codec, criptografia, uma faixa de portas fechada nos dois sentidos ou uma mídia marcada como inativa.

Num 0800 ou numa URA, uma chamada que completa e fica em silêncio é pior que uma recusa: ela aparece como atendida e nenhum alarme de completamento dispara.

Por que a chamada completa e o áudio não passa?

A chamada completa e o áudio não passa porque a chamada VoIP usa dois caminhos separados. O SIP (RFC 3261) negocia a chamada; o áudio viaja em RTP (RFC 3550), em portas UDP escolhidas na hora. O 200 OK prova que o SIP passou, mas não prova que o RTP encontra o endereço e a porta anunciados.

O endereço do áudio vai dentro da própria mensagem SIP, no corpo SDP. Pelo modelo de oferta e resposta da RFC 3264, quem liga oferece um endereço, uma porta e uma lista de codecs; quem atende responde com os seus. Cada lado envia o áudio para o endereço que o outro anunciou. Um exemplo de oferta feita por um PABX atrás de NAT:

```
v=0
o=- 4021 4021 IN IP4 192.168.1.20
s=-
c=IN IP4 192.168.1.20
t=0 0
m=audio 14562 RTP/AVP 8 0
a=rtpmap:8 PCMA/8000
a=rtpmap:0 PCMU/8000
a=sendrecv
```

A linha `c=` diz para onde enviar o áudio, e a linha `m=` diz em que porta e com quais codecs. Nesse exemplo, o PABX anunciou 192.168.1.20, um endereço privado. A operadora, do lado de fora, envia o áudio para esse endereço, que não existe na internet, e o áudio some. O PABX, por sua vez, envia o seu áudio para o endereço público que a operadora anunciou, e esse sentido funciona. Resultado: a operadora ouve o ramal, e o ramal não ouve a operadora.

A linha `a=sendrecv` também conta. Os atributos `sendonly`, `recvonly` e `inactive` limitam o sentido do áudio de propósito, por exemplo numa chamada em espera. Um `inactive` que sobra de uma espera ou de uma transferência mal concluída pode deixar a chamada muda com a rede inteira funcionando.

Quais são as causas mais comuns de ligação muda e áudio unidirecional?

As causas mais comuns de ligação muda e áudio unidirecional no VoIP são oito: NAT sem tratamento, SIP ALG reescrevendo o SDP, faixa RTP bloqueada, IP externo errado no SDP, falta de RTP simétrico, codec incompatível, SRTP de um lado só e early media mal tratada. A tabela resume o sintoma de cada uma.

Causa	Sintoma típico	Onde conferir
NAT sem tratamento	Áudio de um lado só, quase sempre de fora para dentro	Endereço na linha `c=` do SDP enviado pelo PABX
SIP ALG no roteador ou firewall	Sintoma que muda de chamada para chamada, registro que cai, chamadas que caem perto de 32 s	Opções de SIP ou VoIP do roteador ou firewall
Faixa RTP bloqueada ou sem encaminhamento	Ligação muda ou de um lado só, só nas chamadas pelo tronco	Regras de entrada e encaminhamento de portas UDP
IP externo errado no SDP	Áudio de entrada some, às vezes só depois de uma troca de IP ou de link	`external_media_address` no PJSIP, `externaddr` no chan_sip
Falta de RTP simétrico	Áudio de um lado só com telefones remotos ou com a outra ponta atrás de NAT	`rtp_symmetric` e `force_rport` no endpoint
Codec incompatível	Recusa com SIP 488, ou chamada completa com silêncio ou ruído	Linhas `m=` e `a=rtpmap` da oferta e da resposta
SRTP de um lado só	Ligação muda nos dois sentidos, ou recusa com SIP 488	Perfil `RTP/SAVP` no SDP e criptografia de mídia no endpoint
Early media	Silêncio antes do atendimento: não se ouve o toque nem a mensagem da operadora	183 Session Progress com SDP

NAT sem tratamento

O NAT troca o endereço privado do PABX pelo endereço público do link nos cabeçalhos IP, mas não mexe no conteúdo da mensagem SIP. O SDP continua dizendo 192.168.1.20, e a outra ponta acredita nele. A RFC 4787 descreve como os NATs tratam UDP, com comportamentos de mapeamento diferentes conforme o destino, e a RFC 6314 reúne as práticas de travessia de NAT para SIP: anunciar o endereço público, responder para a porta de onde a mensagem veio, manter o mapeamento vivo com mensagens periódicas e usar RTP simétrico. Telefones e adaptadores atrás de NAT também podem descobrir o próprio endereço público com STUN (RFC 8489).

SIP ALG reescrevendo o SDP

O SIP ALG é uma função de muitos roteadores e firewalls que lê as mensagens SIP, troca os endereços privados por públicos dentro do SIP e do SDP e abre portas RTP sob demanda. Quando o PABX já anuncia o endereço externo, as duas correções se somam; quando o ALG reescreve só uma parte, por exemplo o cabeçalho Contact e não a linha `c=`, o resultado é um SDP incoerente. O ALG também não lê SIP sobre TLS, porque a mensagem vai criptografada. Por isso a recomendação usual é desligá-lo e tratar o NAT num lugar só.

Faixa de portas RTP bloqueada ou sem encaminhamento

Cada fluxo RTP usa uma porta UDP, e pela RFC 3550 o RTCP correspondente usa a porta seguinte. O PABX escolhe as portas dentro de uma faixa configurada, e o firewall precisa deixar essa faixa inteira chegar até ele. Um encaminhamento parcial produz um defeito intermitente: as chamadas que caem numa porta dentro da parte encaminhada funcionam, e as outras ficam mudas.

IP externo errado no SDP

Configurar o endereço externo resolve o NAT até o endereço mudar. Links com IP dinâmico, um segundo link que assume quando o principal cai, ou uma rota de saída por um link diferente do anunciado fazem o PABX anunciar um endereço que não é o de onde o tráfego sai. O mesmo vale para a lista de redes locais: o Asterisk só troca o endereço privado pelo público para destinos fora das redes listadas como locais. Uma rede interna que falta na lista, como a VPN de uma filial, recebe o IP público e passa a ter áudio de um lado só.

RTP simétrico

RTP simétrico quer dizer enviar e receber o áudio pela mesma porta e, do outro lado, devolver o áudio para o endereço e a porta de onde ele de fato chegou, ignorando o que o SDP disse. É a forma mais robusta de atravessar um NAT que não se conhece, e é uma das práticas da RFC 6314. Quando a outra ponta, um telefone remoto ou uma operadora atrás de NAT, anuncia um endereço que não funciona, só o RTP simétrico do seu lado faz o áudio chegar até ela.

Codec incompatível

Se a oferta e a resposta não têm nenhum codec de voz em comum, a chamada costuma ser recusada com SIP 488 Not Acceptable Here. O caso mais difícil é a chamada que completa: um lado aceita um codec que não sabe tratar, uma conversão de codec falha no PABX, ou a lista de codecs muda num reenvio do SDP. A chamada aparece atendida e fica muda ou com ruído.

SRTP de um lado só

Com SRTP, o áudio vai criptografado, e o SDP anuncia o perfil `RTP/SAVP` em vez de `RTP/AVP`. Se um lado exige criptografia e o outro envia áudio aberto, ou se as chaves não foram combinadas, os pacotes chegam e são descartados. A chamada fica muda nos dois sentidos com os contadores de pacotes normais. Pela RFC 3264, um fluxo de mídia recusado volta na resposta com a porta 0, e esse detalhe no SDP costuma ser a pista.

Early media

Early media é o áudio que chega antes do atendimento: o toque de chamada gerado pela rede ou a mensagem da operadora dizendo que o número não existe. Ele vem com um SIP 183 Session Progress que traz SDP, e a RFC 3960 descreve como esse áudio antecipado é tratado. Se o PABX, o firewall ou o telefone não deixam esse áudio passar, quem liga ouve silêncio até o atendimento, e uma chamada que falha com uma mensagem gravada parece muda. Um SDP no 183 diferente do SDP no 200 OK também pode deixar o áudio apontado para o lugar errado depois do atendimento.

Como o sintoma aponta para a causa?

O sintoma de uma ligação muda ou de um áudio unidirecional aponta para a causa quando se observa em que sentido o áudio falha, em que momento da chamada e em quais chamadas. Um defeito em toda chamada de entrada é diferente de um que aparece em uma de cada três.

Sintoma	Causa provável	Primeira verificação
O ramal não ouve quem está fora; quem está fora ouve o ramal	IP privado no SDP, SIP ALG, faixa RTP de entrada fechada	SDP enviado pelo PABX e encaminhamento de portas
Quem está fora não ouve o ramal	Saída UDP restrita, ou SDP da outra ponta com endereço inalcançável	Regras de saída do firewall e SDP recebido
Ninguém ouve ninguém	Codec, SRTP, mídia `inactive` ou recusada com porta 0	Oferta e resposta lado a lado
O áudio para depois de uma espera ou transferência	Novo SDP num reenvio de INVITE, mídia direta entre as pontas	`direct_media` e o SDP do reenvio
O áudio para depois de alguns minutos de silêncio	Tempo de sessão UDP curto no firewall	Tempos de sessão UDP e mensagens de manutenção
A chamada cai perto de 32 segundos	ACK perdido por Contact com endereço privado	Cabeçalho Contact do 200 OK
Falha em algumas chamadas e não em outras	Faixa RTP encaminhada pela metade, dois links de saída	Porta RTP das chamadas que falharam
Silêncio só antes do atendimento	Early media bloqueada	183 com SDP e o que o PABX faz com ele

Por que a chamada cai depois de 32 segundos?

Porque o ACK não chegou. Pela RFC 3261, quem atende uma chamada retransmite o 200 OK até receber o ACK. Se passar 64 × T1 sem ACK, a sessão deve ser encerrada. Com o T1 padrão de 500 ms, são 64 × 0,5 = 32 segundos. O ACK é enviado para o endereço do cabeçalho Contact do 200 OK; se o PABX atrás de NAT pôs ali o seu endereço privado, o ACK se perde, o PABX continua retransmitindo e derruba a chamada no fim da conta. Não é um problema de áudio, mas aparece junto com ele, porque nasce do mesmo NAT mal tratado.

Como corrigir a ligação muda no Asterisk, no Issabel e no FreePBX?

No Asterisk, no Issabel e no FreePBX, a correção da ligação muda passa por quatro ajustes: informar o endereço externo e as redes locais no transporte, desligar a mídia direta e ligar o RTP simétrico nos endpoints do tronco, alinhar a faixa RTP do rtp.conf com o firewall e conferir os codecs e a criptografia de mídia dos dois lados.

PJSIP: o transporte

No PJSIP, o endereço externo e as redes locais ficam no transporte. Com documentação de exemplo, 203.0.113.10 como IP público e duas redes internas:

```
[transport-udp-nat]
type=transport
protocol=udp
bind=0.0.0.0:5060
external_media_address=203.0.113.10
external_signaling_address=203.0.113.10
local_net=192.168.1.0/24
local_net=10.20.0.0/16
```

`external_media_address` é o endereço que vai na linha `c=` do SDP; `external_signaling_address` é o que vai nos cabeçalhos SIP, como Contact e Via. `local_net` lista as redes para as quais o Asterisk mantém o endereço privado. Liste todas as redes internas, inclusive as de VPN das filiais.

PJSIP: o endpoint do tronco

No endpoint do tronco e dos telefones remotos:

```
[tronco-operadora]
type=endpoint
transport=transport-udp-nat
direct_media=no
rtp_symmetric=yes
force_rport=yes
rewrite_contact=yes
disallow=all
allow=alaw,ulaw
```

Com `direct_media=yes`, o Asterisk tenta tirar a si mesmo do caminho do áudio depois do atendimento, com um novo INVITE para que as duas pontas troquem RTP direto. Atravessando NAT, isso costuma falhar e o áudio some logo depois do atendimento ou de uma transferência; `direct_media=no` mantém o áudio passando pelo Asterisk. `rtp_symmetric=yes` liga o RTP simétrico, `force_rport=yes` responde para a porta de onde a mensagem veio, e `rewrite_contact=yes` grava o endereço de onde o registro chegou, e não o que o aparelho disse. As linhas `disallow` e `allow` definem os codecs aceitos, na ordem de preferência; elas precisam ter interseção com o que a operadora aceita. O comando `pjsip show endpoint tronco-operadora` mostra os valores em vigor.

Se a operadora exige SRTP, a opção `media_encryption` do endpoint precisa combinar com ela. Se ela não usa, a opção precisa estar desligada.

chan_sip, em instalações antigas

No chan_sip, que as versões recentes do Asterisk já não trazem, os equivalentes ficam no `sip.conf`: `externaddr` (antes `externip`) para o endereço público, `localnet` para as redes locais, `nat=force_rport,comedia` para o RTP simétrico e `directmedia=no` para manter o áudio no Asterisk.

rtp.conf: a faixa de portas

A faixa de portas RTP do Asterisk fica no `rtp.conf`:

```
[general]
rtpstart=10000
rtpend=20000
```

Esses são os valores do arquivo de exemplo do Asterisk e o padrão do FreePBX. A faixa do firewall precisa ser exatamente a mesma, ou maior. Se for preciso estreitar a faixa, faça a conta: cada ponta de chamada que passa pelo Asterisk usa um par de portas (RTP e RTCP), e uma chamada entre um telefone e o tronco tem duas pontas, ou seja, quatro portas. Uma faixa de 10.000 portas comporta, em conta aproximada, 10.000 ÷ 4 = 2.500 chamadas simultâneas.

No mesmo arquivo, a opção `strictrtp`, ligada por padrão nas versões atuais, faz o Asterisk aceitar o RTP só da origem que ele aprendeu no início da chamada. Uma operadora que troca a origem do áudio no meio da chamada, por exemplo depois de uma mensagem gravada, pode ter o áudio descartado. Desligá-la é um teste de diagnóstico, não a correção definitiva.

FreePBX e Issabel

No FreePBX, os campos equivalentes ficam em **Settings** → **Asterisk SIP Settings**, na aba **General SIP Settings**: **External Address**, **Local Networks** e **RTP Port Ranges**. Prefira a interface aos arquivos: o FreePBX regrava os arquivos que gera ao aplicar a configuração, e os ajustes feitos à mão ficam nos arquivos terminados em `_custom.conf`. O Issabel traz o Asterisk com uma interface derivada do FreePBX, e os mesmos três itens, endereço externo, redes locais e faixa RTP, aparecem nas suas configurações SIP. Em centrais Issabel antigas com chan_sip, vale a seção anterior.

Para um primeiro teste interno, o FreePBX tem um teste de eco no código `*43`, e no Asterisk puro o aplicativo `Echo()` do plano de discagem faz o mesmo. Esse teste só prova o trecho entre o telefone e o PABX; o tronco, o NAT e o firewall ficam de fora.

Como ajustar o firewall e o roteador para o áudio VoIP?

Para o áudio VoIP atravessar o firewall e o roteador, três ajustes resolvem a maior parte dos casos: desligar o SIP ALG quando o PABX já trata o NAT, encaminhar para o PABX a mesma faixa UDP de RTP que ele usa e dar às sessões UDP um tempo de vida maior que o intervalo entre as mensagens.

Desligue o SIP ALG

O nome e o lugar mudam de fabricante para fabricante, e vale sempre conferir a documentação da versão instalada:

- **FortiGate**: o tratamento de SIP pode vir de um *session helper* de SIP ou da ALG de SIP aplicada pelo perfil de VoIP das políticas. Confira os dois antes de concluir que o SIP passa sem alteração.
- **MikroTik**: o *helper* fica em **IP** → **Firewall** → **Service Ports**, na entrada **sip**. Desabilite essa entrada.

- **pfSense**: o ponto mais citado para VoIP é o NAT de saída trocar a porta de origem das conexões. Uma regra de NAT de saída com porta estática para o endereço do PABX evita a troca.
- **Roteadores de banda larga**: muitos trazem a opção como “SIP ALG” ou “SIP Passthrough” nas configurações avançadas de NAT.

Depois de desligar, limpe as sessões ativas para que as entradas antigas saiam da tabela de conexões.

Abra e encaminhe a faixa RTP

Encaminhe a faixa UDP inteira, 10000 a 20000 no exemplo, para o endereço interno do PABX, e libere essa mesma faixa nas regras de entrada. Por segurança, limite a origem aos endereços da operadora sempre que ela informar quais são, e faça o mesmo com a porta SIP.

Ajuste os tempos de sessão UDP

O firewall esquece um mapeamento UDP que fica sem tráfego. A RFC 4787 pede que esse temporizador não expire em menos de 2 minutos e recomenda um padrão de 5 minutos ou mais. Equipamentos com tempos menores derrubam o mapeamento do registro SIP entre duas renovações, e o tronco passa a receber chamadas que não chegam ao PABX. Duas saídas: aumentar o tempo de sessão UDP no firewall para as portas de voz, ou fazer o PABX enviar mensagens com mais frequência, com uma renovação de registro mais curta e o `qualify_frequency` do AOR no PJSIP, que envia um OPTIONS periódico.

E se houver um SBC?

Um SBC na borda assume o NAT e ancora o áudio entre o PABX e a operadora; o PABX conversa só com ele, numa rede conhecida. O cuidado é não tratar o NAT duas vezes: SBC, ALG e PABX corrigindo o mesmo endereço geram um SDP incoerente.

Como saber se o 0800 ou o tronco SIP está com ligação muda?

A forma de saber se um 0800, uma URA ou um tronco SIP está com ligação muda é ligar de fora e verificar o áudio nos dois sentidos, numa chamada real, de forma repetida. Um painel de PABX não vê o problema: o tronco aparece registrado, a chamada é atendida, e só quem está na linha percebe o silêncio.

O teste que prova os dois sentidos é uma chamada para um serviço de eco ou de tons. O que a chamada envia precisa voltar: se o eco devolve o áudio, ele chegou até lá e voltou. Uma chamada interna, um teste de eco no próprio PABX ou o toque de chamada antes do atendimento não provam isso, porque deixam de fora o tronco, o NAT ou o próprio caminho do áudio depois do atendimento. Por causa dos defeitos intermitentes, como uma faixa RTP encaminhada pela metade, um teste isolado também não basta: o defeito pode aparecer só numa parte das chamadas.

É isso que o Monitor faz para cada **circuito de voz**, que é cada tronco SIP, 0800 ou número de atendimento monitorado. A 2N5 faz chamadas de teste reais da própria plataforma, no ritmo combinado, sem instalar nada no PABX e sem integração com ele. Quando o número é atendido por um tom de teste ou por um serviço de eco, a chamada passa quando é atendida e os tons enviados voltam. Áudio em um só sentido ou ausente conta como falha, mesmo com a chamada completa. Veja o que cada chamada verifica em monitoramento de troncos SIP.

Uma falha é repetida antes de qualquer alerta. No ritmo padrão, cada circuito recebe uma chamada a cada 15 minutos; depois de uma falha, a chamada é repetida três vezes, a cada 2 minutos, quatro falhas seguidas abrem um incidente e duas chamadas boas seguidas confirmam a volta. O incidente avisa a escada de escalonamento por e-mail, até alguém assumir; veja alertas e escalonamento. Se o problema estiver do lado da 2N5, o teste fica sem visibilidade e não conta contra o circuito.

Como os contadores de RTP mostram de que lado o áudio parou?

Os contadores de RTP enviados e recebidos mostram de que lado o áudio parou porque cada sentido tem o seu fluxo. Numa chamada normal, os dois contadores sobem juntos. Quando um deles fica parado em zero enquanto o outro sobe, o áudio unidirecional está provado, e o sentido parado indica em que trecho procurar.

A conta de referência é simples. Com áudio empacotado a cada 20 ms, cada sentido envia 1.000 ÷ 20 = 50 pacotes por segundo. Uma chamada de 60 segundos tem cerca de 3.000 pacotes em cada sentido. Um contador de recebidos em zero ao lado de 3.000 enviados não deixa dúvida.

No Asterisk, três comandos dão essa visão:

- `pjsip show channelstats` mostra, para cada canal ativo, os pacotes recebidos e transmitidos, a perda, o jitter e o tempo de ida e volta;
- `rtp set debug on` mostra cada pacote com o endereço de origem e de destino, e revela na hora um áudio sendo enviado para um endereço privado; `rtp set debug ip` filtra por endereço;
- no chan_sip, `sip show channelstats` faz o papel do primeiro.

Fora do Asterisk, uma captura de pacotes no PABX ou no firewall, aberta no Wireshark em **Telephony → RTP → RTP Streams**, lista cada fluxo com origem, destino e quantidade de pacotes. Capturar dos dois lados do firewall mostra se o pacote para na borda. O RTCP ajuda também: pela RFC 3550, o relatório de quem envia traz a contagem de pacotes e de bytes enviados, e o relatório de quem recebe traz a fração perdida, o total perdido e o jitter. Uma ponta que nunca recebe RTCP da outra tem o mesmo problema no caminho de volta.

Enviados pelo PABX	Recebidos pelo PABX	Leitura
Normais	Zero	O áudio de fora não chega: IP privado no SDP, SIP ALG ou faixa RTP de entrada fechada
Zero	Normais	O PABX não envia: mídia `recvonly` ou `inactive`, falha de conversão de codec, mídia direta
Normais	Normais, com silêncio mesmo assim	O áudio chega e não é usado: SRTP sem chave, codec errado, trecho entre PABX e telefone
Zero	Zero	Nenhum fluxo: mídia recusada com porta 0, `inactive`, canal sem ponte
Sobem e depois param	Sobem e depois param	Novo SDP num reenvio de INVITE, tempo de sessão UDP vencido, troca de origem com `strictrtp`

O que levar para a operadora?

Leve à operadora o horário de cada chamada que falhou, o número chamado, o Call-ID, a captura do SIP com o SDP da oferta e da resposta, e os contadores de RTP dos dois sentidos. Se o seu PABX envia áudio ao endereço anunciado e nada volta, o problema está do lado dela ou entre vocês.

Uma ligação muda não tem código de erro: a chamada completou com 200 OK. No Monitor, cada incidente traz o circuito, a operadora, o primeiro sintoma, o código SIP e a causa Q.850 de cada chamada, e a última chamada saudável, num bloco pronto para colar no chamado. A consulta de código SIP ajuda a ler os códigos das chamadas que foram recusadas no caminho.

Lista de verificação

1. Confirme o sentido que falha e em quais chamadas: todas, só as de entrada, só algumas.
2. Capture o SIP e leia o SDP: o endereço da linha `c=` é o público?
3. Desligue o SIP ALG do roteador ou firewall, e reinicie as sessões ativas.
4. Configure `external_media_address`, `external_signaling_address` e todas as redes em `local_net`.
5. Use `direct_media=no`, `rtp_symmetric=yes`, `force_rport=yes` e `rewrite_contact=yes` no tronco e nos telefones remotos.
6. Alinhe a faixa do `rtp.conf` com o encaminhamento UDP do firewall, inteira.
7. Ajuste os tempos de sessão UDP ou encurte a renovação do registro.
8. Compare codecs e criptografia da oferta e da resposta.
9. Confira o que acontece com o 183 e o early media.
10. Prove o resultado com chamadas reais de fora para um eco ou tom, de forma repetida, olhando os contadores de RTP dos dois sentidos.

Perguntas frequentes

Por que a ligação VoIP completa e fica muda?

Porque o SIP, que completa a chamada, e o RTP, que leva o áudio, seguem caminhos diferentes. O 200 OK prova que o SIP passou. O áudio depende do endereço e da porta anunciados no SDP; se esse endereço é privado, se a porta está fechada no firewall ou se os dois lados não combinam codec ou criptografia, a chamada fica muda.

O que é áudio unidirecional?

É a chamada em que um lado ouve e o outro não. O sentido que falha indica onde procurar: quando quem está dentro não ouve quem está fora, o áudio de entrada não chega, quase sempre por IP privado no SDP, SIP ALG ou faixa RTP sem encaminhamento. Quando é o contrário, olhe a saída do PABX e o SDP da outra ponta.

Desligar o SIP ALG resolve sempre?

Não sempre, mas é o primeiro passo recomendado quando o PABX já trata o NAT. O SIP ALG reescreve endereços dentro do SIP e do SDP, e a correção dupla gera endereços trocados. Depois de desligá-lo, o PABX precisa anunciar o endereço externo certo e a faixa RTP precisa estar encaminhada, senão o problema continua.

Por que a chamada cai depois de uns 30 segundos?

Quase sempre porque o ACK não chegou. Pela RFC 3261, quem atende retransmite o 200 OK até receber o ACK e, depois de 64 × T1, 32 segundos com T1 de 500 ms, encerra a sessão. O ACK vai para o endereço do cabeçalho Contact; se esse endereço é privado, ele se perde no NAT.

Como testar se o áudio passa nos dois sentidos?

Com uma chamada real, vinda de fora pelo tronco, para um serviço de eco ou de tons: o que sai precisa voltar. Uma chamada interna só prova o trecho entre telefone e PABX. Enquanto isso, os contadores de RTP do PABX mostram se os pacotes estão saindo e chegando nos dois sentidos.

O que causa ligação muda ou áudio de um lado só no VoIP?

Quase sempre o SIP completa a chamada, mas o RTP, que leva o áudio, não chega. As causas mais comuns são um IP privado anunciado no SDP, o SIP ALG reescrevendo endereços, uma porta ou faixa RTP bloqueada no firewall e um codec ou uma criptografia sem acordo entre as pontas. O sentido que falha indica onde procurar, e uma chamada real de fora confirma a correção.

O que é SIP ALG e por que derruba ligações?

SIP ALG é uma função de roteadores e firewalls que inspeciona e reescreve o tráfego SIP para ajudar na passagem pelo NAT. Ele derruba ligações quando reescreve errado os endereços do SIP e do SDP, sobretudo se o PABX também trata o NAT: a chamada completa, mas fica muda. Desligá-lo é o primeiro passo recomendado quando o PABX já trata o NAT, embora nem sempre resolva.

Fontes

1. RFC 3261: SIP, incluindo a retransmissão do 200 OK até o ACK (64 × T1)
2. RFC 3264: modelo de oferta e resposta com SDP
3. RFC 3550: RTP e RTCP, contadores de pacotes e jitter
4. RFC 3960: early media e geração de toque de chamada no SIP
5. RFC 6314: práticas de travessia de NAT para aplicações SIP
6. RFC 4787: comportamento de NAT para UDP, incluindo tempos de mapeamento
7. RFC 8489: STUN

GUIA

Monitoramento de circuitos de voz: troncos SIP, 0800 e URA

Um tronco SIP registrado e um PABX sem alarmes não provam que uma chamada completa com áudio. Este guia compara as formas de monitorar um circuito de voz, mostra como confirmar uma queda sem alarme falso e diz que evidência guardar para cobrar a operadora.

Por Equipe 2N5 Publicado em 7 de outubro de 2026 Atualizado em 20 de outubro de 2026

Resumo

- Ping e SIP OPTIONS mostram que um equipamento responde; só uma chamada de teste real mostra que a chamada de um cliente completa, com áudio nos dois sentidos.
- A captura passiva no PABX só vê as chamadas que chegam até ele: quando a falha está antes, na operadora ou na rota do 0800, ela não registra nada.
- No ritmo padrão do Monitor, cada circuito recebe uma chamada de teste a cada 15 minutos; depois de uma falha, três novas tentativas a cada 2 minutos, e quatro falhas seguidas abrem um incidente.
- Duas chamadas boas seguidas confirmam a volta do circuito; uma falha isolada nunca vira incidente.
- Quando a falha é do próprio monitoramento, o teste fica sem visibilidade: não conta contra o circuito e não entra no SLA.
- A evidência de cada falha é o código SIP, a causa Q.850, o Call-ID e o horário exato de cada chamada de teste.

O que é monitoramento de circuitos de voz?

Monitoramento de circuitos de voz é a verificação contínua de que cada tronco SIP, número 0800, DDR de filial e URA completa chamadas com áudio nos dois sentidos e com a mensagem certa. Um circuito de voz, aqui, é qualquer número ou rota por onde um cliente chega até a sua empresa por telefone.

A definição importa porque muda o que se mede. A maior parte das ferramentas de um ambiente de telefonia olha para os equipamentos: se o SBC está ligado, se o tronco está registrado, se o processador do PABX está folgado. Essas perguntas são necessárias, mas respondem a outra coisa. Um equipamento pode estar perfeito enquanto a chamada de um cliente não chega até ele.

Este guia trata da pergunta que o cliente faz: se eu ligar agora, alguém atende? Os guias sobre 0800 e URA, ligação muda, qualidade de voz e SLA aprofundam cada parte.

Por que o painel fica verde enquanto o cliente ouve silêncio?

O painel fica verde porque mede o equipamento, e não a chamada. O PABX está ligado, o tronco SIP aparece registrado e o link responde, enquanto a falha está na rota da operadora, na tradução do 0800 ou no caminho do áudio. Nenhum desses pontos manda alarme para o painel da sua equipe.

Três situações comuns mostram o problema:

- **A chamada nunca chega.** A operadora deixou de rotear o seu 0800 ou um DDR até o seu tronco. O PABX não recebe nada, então não tem o que reclamar.

- **A chamada chega, mas o áudio não.** A sinalização SIP passa e a chamada é atendida, mas o RTP, que leva a voz, para em um NAT, num firewall ou num SIP ALG. O resultado é a ligação muda ou o áudio de um lado só, e o PABX registra uma chamada completada.
- **A mensagem errada atende.** A URA foi trocada, a gravação de feriado ficou ligada ou a operadora toca a mensagem de número inexistente. Para a sinalização, tudo funcionou.

Há um agravante: de madrugada e no fim de semana, poucas chamadas é o normal. O cliente que liga às 2h e ouve silêncio desiste, e a falha só aparece quando o atendimento abre e as filas estão estranhamente vazias.

Ping, SIP OPTIONS, captura passiva ou chamada de teste: o que cada um vê?

Cada método de monitoramento de um tronco SIP responde a uma pergunta diferente. O ping diz se um endereço responde; o SIP OPTIONS e o registro, se a pilha SIP responde; a captura passiva, como foram as chamadas que chegaram. Só a chamada de teste real diz se a chamada de um cliente completa agora, com áudio.

Método	O que vê	O que não vê	Para que serve
Ping	Que o endereço do SBC ou do PABX responde na rede	O serviço SIP, a rota da operadora, o áudio, a mensagem; muitos SBCs nem respondem a ping	Saber se o equipamento sumiu da rede
SIP OPTIONS e registro (keep-alive)	Que a pilha SIP do outro lado responde e que o registro do tronco está válido	Se um INVITE para o seu número é roteado até você, se o áudio passa, quem atende	Manter o tronco e o NAT ativos e notar a perda do registro
Monitoramento passivo (captura de pacotes, estatísticas RTCP no PABX)	Códigos SIP, perda e jitter das chamadas reais que chegaram ao PABX	As chamadas que nunca chegaram; nada, quando não há tráfego	Diagnosticar qualidade e investigar uma chamada específica
Chamada de teste real	Se a chamada completa, o código SIP e a causa Q.850, quem atendeu, o áudio nos dois sentidos e a qualidade medida	Origens e números que ela não disca; o que acontece entre dois testes	Saber se o cliente consegue falar com você, a qualquer hora

Os métodos se completam: a chamada de teste diz **se** está funcionando; os outros ajudam a descobrir **por que** não está.

Ping

O ping é o teste mais barato e o mais limitado. Ele confirma que um endereço IP responde, o que ajuda a saber se um SBC ou um link sumiu. Mas um equipamento que responde ao ping pode estar com o serviço SIP parado, e muitos SBCs descartam o ping de propósito, por segurança.

SIP OPTIONS e registro

O método OPTIONS, definido no RFC 3261, pergunta a um elemento SIP o que ele suporta. Na prática, SBCs e operadoras enviam OPTIONS em intervalos para saber se o outro lado está vivo e, junto com outras técnicas descritas no RFC 6314, para manter abertos os mapeamentos de NAT. O REGISTER, também do RFC 3261, é como o tronco diz à operadora para onde entregar as chamadas. Veja registro SIP.

Um tronco registrado e respondendo a OPTIONS prova que a sinalização entre os dois equipamentos funciona. Não prova três coisas: que a operadora roteia um número específico até esse tronco (a tradução de um 0800 acontece em outro lugar da rede dela); que o áudio passa, já que o RTP viaja em outras portas e pode ser barrado enquanto o OPTIONS passa; e que quem atende é a URA certa.

Monitoramento passivo no PABX

A captura de pacotes no PABX ou no SBC registra a sinalização e o áudio das chamadas reais. Os relatórios RTCP do RFC 3550 trazem a perda de pacotes e o jitter de cada sentido, e muitos equipamentos calculam a partir deles uma nota MOS estimada pelo modelo E da ITU-T G.107, que a ITU-T P.800.1 chama de MOS-CQE. É a ferramenta certa para investigar por que uma chamada específica soou mal.

O limite é estrutural: o monitoramento passivo só vê o que chega. Se a operadora parou de entregar as chamadas do 0800, não há pacote para capturar, e de madrugada, sem tráfego, não há dado nenhum. Uma queda no volume de chamadas não serve de sinal às 3h de domingo, quando zero chamadas é o esperado.

Chamada de teste real

A chamada de teste disca o número de fora, como um cliente faz, e julga o resultado. Ela atravessa a operadora, a tradução do 0800, o tronco, o SBC, o PABX e a URA, e por isso vê o que o cliente veria. É o único método que funciona igual às 3h e às 15h, porque não depende de alguém ligar.

Ela também tem limites. Testa a partir da sua origem e só os números que disca; uma falha que afeta apenas chamadas vindas de celular, por exemplo, pode não aparecer (veja por que o 0800 não completa do celular). Não vê o que acontece entre um teste e o próximo. E ocupa um canal por alguns segundos, como uma chamada de cliente.

O que uma chamada de teste precisa verificar?

Uma chamada de teste precisa verificar quatro coisas, em ordem: se a chamada completou, se atendeu quem deveria atender, se o áudio passou nos dois sentidos e se a voz chegou com qualidade. Um teste que confere só a primeira deixa passar o 0800 mudo, a URA trocada e a mensagem da operadora.

A chamada completou?

A resposta da rota a um INVITE diz o que aconteceu. As respostas 1xx indicam andamento, 200 OK indica atendimento, e as respostas 4xx, 5xx e 6xx indicam falha. As que um teste mais encontra:

Resposta SIP	O que costuma significar	Para o monitoramento
180 Ringing	O destino está tocando	Andamento, ainda não é atendimento
183 Session Progress	Andamento com áudio antes do atendimento, o early media (RFC 3960)	Pode ser o toque ou uma mensagem da operadora; não é atendimento
403 Forbidden	A rota recusou a chamada	Falha
404 Not Found	O número não existe para essa rota	Falha
408 Request Timeout	Nenhuma resposta final a tempo	Falha
480 Temporarily Unavailable	O destino está indisponível no momento	Falha

Resposta SIP	O que costuma significar	Para o monitoramento
486 Busy Here	Ocupado	Falha para uma URA, que deveria atender toda chamada
487 Request Terminated	A chamada foi cancelada antes do atendimento	Quando o teste desistiu de esperar, é falha de atendimento
488 Not Acceptable Here	A oferta de mídia, como os codecs, não foi aceita (RFC 3264)	Falha
503 Service Unavailable	O serviço do outro lado não está disponível	Falha
603 Decline	O destino recusou a chamada	Falha

Junto com o código SIP, muitas rotas enviam a causa Q.850 da rede de telefonia no cabeçalho Reason, como descreve o RFC 6432. A lista de códigos SIP, a lista de causas Q.850 e a consulta de código SIP explicam cada uma.

Atendeu quem deveria atender?

“Atendeu” não basta. Um 0800 pode completar e tocar a gravação da operadora dizendo que o número não existe; uma URA pode ser trocada sem aviso. Por isso cada circuito precisa de uma definição do que deve atender, e o teste precisa conferir.

No Monitor, essa escolha é feita na implantação e decide o que conta como funcionando:

- **Uma saudação ou mensagem gravada, a URA:** passa quando a chamada é atendida e a saudação esperada é ouvida. A 2N5 grava a saudação de referência de cada número, e cada chamada compara o que ouviu com ela. A mensagem de erro de uma operadora não passa.
- **Um tom de teste ou serviço de eco:** passa quando a chamada é atendida e os tons enviados voltam.
- **Outro:** pode tocar até o fim ou ser atendido com áudio, conforme o combinado. Se uma pessoa atender, ela ouve uma mensagem avisando que é um teste automático.

Para uma URA, ocupado, sem atendimento ou tocar até o fim é falha: ela atende toda chamada sozinha.

O áudio passou nos dois sentidos?

Uma chamada pode ser atendida e ficar muda, ou levar a voz para um lado só. A sinalização SIP e o áudio seguem caminhos diferentes: o SIP combina os endereços e as portas, e o RTP leva a voz. Um NAT que reescreve só um dos dois, um SIP ALG que altera a mensagem ou um firewall que barra as portas de mídia produzem a ligação muda, enquanto o PABX registra uma chamada completada. Num circuito com tom de teste ou eco, o teste confere que os tons enviados voltam. O guia ligação muda e áudio de um lado só detalha as causas.

A voz chegou com qualidade?

Uma chamada pode completar e soar picotada. O Monitor mede a qualidade de escuta a partir do áudio que a chamada recebeu, comparado com a gravação de referência, com um modelo perceptual de qualidade de escuta com referência, e dá uma nota de 1 a 5: o MOS-LQO, na terminologia da ITU-T P.800.1. É diferente do MOS-CQE que um PABX estima com números da rede pelo modelo E da G.107: um mede o que chegou, o outro calcula o que deveria ter chegado.

Por padrão, o circuito está saudável com MOS-LQO a partir de 3,8, e uma nota abaixo de 3,0 marca a chamada como degradada. Uma chamada degradada passa pelas mesmas novas tentativas de qualquer falha. Veja qualidade de voz medida e o guia MOS e MOS-LQO na prática.

Como confirmar uma queda sem alarme falso?

Uma queda de circuito de voz se confirma repetindo a chamada antes de avisar alguém. Uma falha isolada pode ser uma rota que oscilou uma vez; quatro falhas seguidas, com poucos minutos entre elas, são uma queda. A mesma lógica vale para a volta: uma chamada boa não basta, duas seguidas confirmam.

No ritmo padrão do Monitor, cada circuito recebe uma chamada de teste a cada 15 minutos. Quando uma falha, a chamada é repetida três vezes, a cada 2 minutos; quatro falhas seguidas abrem um incidente, e duas chamadas boas seguidas confirmam a volta. Em forma de linha do tempo, com T sendo o horário do teste que falhou primeiro:

Momento	Chamada	Resultado	O que acontece
T − 15 min	Teste agendado	Completa, a URA atende	Circuito saudável
T	Teste agendado	SIP 503	Primeira falha; nova tentativa em 2 minutos; ninguém é avisado
T + 2 min	Nova tentativa	SIP 503	Segunda falha seguida; nova tentativa em 2 minutos
T + 4 min	Nova tentativa	SIP 503	Terceira falha seguida; nova tentativa em 2 minutos
T + 6 min	Nova tentativa	SIP 503	Quarta falha seguida: incidente aberto, com as evidências; a camada 1 é avisada por e-mail
Depois	Chamadas seguintes	Falham	O incidente segue aberto; se ninguém confirmar a tempo, o alerta sobe para a camada seguinte
Na volta	Chamada	Completa, a URA atende	Primeira chamada boa; o incidente ainda não fecha
Logo depois	Chamada seguinte	Completa, a URA atende	Segunda boa seguida: volta confirmada, incidente fechado, contatos avisados

Se a chamada de T + 2 min completar, a sequência para ali: houve uma falha isolada, ninguém foi acordado e nada entra no SLA. É esse filtro que permite confiar num alerta às 2h.

Quanto tempo leva para uma queda virar alerta?

Depende de quando a queda começa em relação ao teste. No pior caso, ela começa logo depois de um teste bom: leva até 15 minutos para o próximo teste ver a falha e mais 6 minutos para as três novas tentativas confirmarem, ou seja, 15 + 6 = 21 minutos até o incidente. No melhor caso, começa logo antes de um teste e vira incidente em cerca de 6 minutos.

Testar com mais frequência reduz esse tempo, mas cada teste ocupa um canal por alguns segundos. A conta da frequência padrão: 24 horas × 4 testes por hora = 96 chamadas de teste por dia, por circuito, sem contar as novas tentativas.

Por que quatro falhas e duas boas?

Quatro falhas seguidas, em 6 minutos, separam uma oscilação de uma queda sem atrasar demais o alerta. Duas chamadas boas seguidas evitam o vai e volta de um circuito instável, que de outro modo fecharia e reabriria o incidente a cada teste. Esses são os valores padrão do Monitor.

Quando o próprio monitoramento fica cego?

O monitoramento fica cego quando o teste não pode ser feito por um problema do lado de quem testa: a plataforma de chamadas sem resposta, a conta de origem fora do ar, a rede do próprio monitoramento caída. Nesse caso o teste não diz nada sobre o circuito de voz, e não pode contar como queda dele.

Contar a cegueira como queda causa três estragos. A equipe é acordada às 2h por um problema que não é dela. O SLA do circuito sai pior do que foi. E a contestação com a operadora enfraquece, porque basta a operadora mostrar que o lado dela estava normal naquela hora para pôr em dúvida as outras quedas registradas. A cegueira também não pode contar como tempo no ar: se ninguém conseguiu testar, ninguém sabe como o circuito estava.

No Monitor, quando a falha está do lado da 2N5, por exemplo um problema do lado da 2N5, como a nossa plataforma de chamadas sem resposta, o teste fica **sem visibilidade**:

- não conta contra o circuito e não abre incidente para o cliente;
- não entra no SLA: o período sai da conta e aparece separado no relatório;
- não acorda a equipe do cliente; a 2N5 é avisada se durar mais de 30 minutos;
- um sinal periódico avisa a 2N5 também se o monitoramento parar de rodar.

Quem monta o próprio monitoramento precisa da mesma separação. Uma forma prática é ter um destino de controle, um número que sempre deveria completar, testado da mesma origem. Se o circuito e o controle falham juntos, o problema provavelmente está na origem do teste, e não no circuito.

Que evidência guardar de cada falha?

Para cada chamada de teste que falhou, guarde o código SIP da resposta, a causa Q.850 quando ela vier, o Call-ID, o horário exato com fuso, o número chamado e a origem. Com isso a operadora consegue achar a chamada nos próprios registros, e o “nenhum defeito encontrado” fica difícil de sustentar.

Evidência	De onde vem	Por que importa
Código SIP	A linha de status da resposta (RFC 3261), por exemplo 503	Diz em que ponto e como a chamada foi recusada
Causa Q.850	O cabeçalho Reason, quando a rota envia (RFC 6432), por exemplo `Reason: Q.850;cause=34`	Traz a causa da rede de telefonia por trás do SIP
Call-ID	O cabeçalho Call-ID da chamada (RFC 3261)	Identifica a chamada nos registros da operadora
Horário	O relógio de quem testou, com segundos e fuso	Cruza com os registros da operadora e marca o início e o fim da queda
Número chamado e origem	O próprio teste	Uma falha pode valer só para uma origem ou um número
Última chamada saudável	O histórico de testes	Delimita quando a queda começou
O que foi ouvido	A gravação da chamada, quando a URA ou a gravação atendeu	Prova a mensagem errada ou a mensagem da operadora

Guarde o código SIP e a causa Q.850 juntos, chamada por chamada: a mesma resposta 503 pode vir com causas diferentes, e cada uma aponta para um lugar.

No Monitor, cada incidente traz um bloco pronto para colar no chamado da operadora: o circuito, a operadora, o primeiro sintoma, o código SIP e a causa Q.850 de cada chamada, e a última chamada saudável. Exemplo, com dados de demonstração: *SIP 503 Service Unavailable, Q.850 causa 34 (nenhum circuito ou canal disponível), confirmado após 4 chamadas com falha*. O áudio só é guardado quando quem atende é a gravação ou a URA informada, criptografado e guardado pelo prazo que a 2N5 definir; a voz de uma pessoa nunca é guardada.

O que monitorar: troncos SIP, 0800, DDRs de filial ou URA?

Monitore primeiro o que o cliente disca, depois cada caminho por onde essas chamadas passam. Em geral, isso significa os números de atendimento, como 0800 e 4004, a URA que os atende, um DDR por tronco SIP e por operadora, e um DDR em cada filial. Cada um vira um circuito de voz com agenda própria.

O que	O que discar	O que deve atender	O que o teste mostra
Número de atendimento (0800, 0300, 4004)	O próprio número, como o cliente disca	A saudação da URA	A rota da operadora, a portabilidade, a plataforma da URA
URA telefônica	O número que cai nela	A saudação gravada como referência	A mensagem trocada, a plataforma fora do ar, a qualidade
Tronco SIP	Um DDR que entra por esse tronco	Um tom de teste, um eco ou uma saudação	Recusa da operadora, canais lotados, áudio de um lado só
DDR de filial	Um número da filial	Tom, eco, saudação, ou um ramal que pode tocar	O tronco, o link e o PABX daquela filial
Fila de atendimento	O número da fila	A saudação, ou pode tocar	Se a fila recebe chamadas

Um tronco, um DDR

Se você tem dois troncos SIP de operadoras diferentes por redundância, teste cada um com um DDR que entra só por ele. Testar apenas o número principal esconde a queda do primeiro tronco enquanto o segundo segura as chamadas, e você só descobre quando os dois caem juntos. A redundância só vale se cada caminho for testado.

Números de atendimento e URA

O número de atendimento é o que mais pesa, porque é o que o cliente conhece. Teste o próprio 0800, e não só o DDR para onde ele é traduzido: a tradução fica na operadora, e é ali que muitas falhas acontecem. O guia Seu 0800 parou e ninguém avisou trata desse caso em detalhe, e a página monitoramento de 0800 e URA mostra como o Monitor julga cada número. Para as filiais, um DDR por filial, com um ramal ou um tom de teste atrás, cobre o tronco, o link e o PABX de cada uma; veja monitoramento de troncos SIP.

Com que frequência testar um circuito de voz?

A frequência do teste define a resolução do SLA de um circuito de voz. Com uma chamada a cada 15 minutos e novas tentativas a cada 2 minutos depois de uma falha, o início e o fim de cada queda ficam marcados com poucos minutos de margem. Testar de hora em hora pode deixar passar quedas inteiras de 40 minutos.

A conta parte da meta. Uma meta de 99,9% num mês de 30 dias permite 43.200 minutos × 0,001 = 43,2 minutos fora do ar. Se o teste acontece a cada 60 minutos, uma queda de 40 minutos pode começar e terminar entre dois testes e nunca entrar no relatório: o SLA sai melhor do que foi. Para a meta valer alguma coisa, o intervalo entre testes precisa ser bem menor do que o tempo que ela permite. A calculadora de SLA faz a conta para qualquer meta e período.

Duas outras decisões pesam tanto quanto o intervalo:

- **Os horários sem ninguém olhando.** Um 0800 de atendimento 24 horas precisa de teste de madrugada e no fim de semana, porque é quando ninguém da equipe vai perceber sozinho. No Monitor, cada número tem a sua agenda, em intervalos ou em horários fixos, inclusive à noite e nos fins de semana.
- **O limite de chamadas.** Cada teste ocupa um canal por alguns segundos. Com muitos circuitos atrás do mesmo tronco, o teste precisa caber num limite de chamadas para nunca disputar canal com os clientes.

E o link de internet por onde a voz passa?

O link de internet é o circuito de dados por onde a voz quase sempre passa, e uma queda nele derruba todos os circuitos de voz do local de uma vez. Medir o link ao lado das chamadas de teste responde à primeira pergunta de toda queda de voz: foi a linha ou foi a conexão?

No Monitor, um agente que a 2N5 instala no local mede latência, perda de pacotes, jitter, tempo de DNS e velocidade. Cada circuito de voz pode ser ligado ao link do seu local; com a opção de esperar pelo link, a equipe recebe um alerta sobre o link, e não um por circuito de voz que passa por ele. Veja circuitos de dados.

Quem deve ser avisado quando um circuito de voz cai?

Quando um circuito de voz cai de verdade, quem precisa saber é quem consegue agir naquela hora, e não uma caixa de e-mail que ninguém abre de madrugada. Uma escada com camadas, que sobe até alguém assumir, garante que o alerta de um incidente confirmado não fique sem resposta.

No Monitor, o incidente avisa a camada 1 por e-mail. Se ninguém confirmar no tempo definido, o alerta sobe para a camada seguinte; uma única confirmação, um toque no link do e-mail, para a subida e registra quem assumiu. Se nenhuma camada confirmar, os administradores da empresa são avisados. Os contatos do cliente recebem o aviso do problema e o da solução, fora da escada. Janelas de manutenção silenciam os circuitos escolhidos durante o horário marcado. Veja alertas e escalonamento.

O tempo até a primeira confirmação entra nos relatórios de SLA ao lado da disponibilidade. Medir a chamada, confirmar a queda, separar a cegueira, guardar a evidência e avisar a pessoa certa: é isso que transforma um monitoramento em resposta.

Perguntas frequentes

Ping ou SIP OPTIONS bastam para monitorar um tronco SIP?

Não. O ping diz que o endereço do SBC ou do PABX responde na rede, e o SIP OPTIONS diz que a pilha SIP do outro lado responde. Nenhum dos dois faz uma chamada: não mostram se a operadora roteia o seu número até você, se o áudio passa nos dois sentidos ou se a URA certa atende. Para isso é preciso uma chamada de teste real.

De quanto em quanto tempo testar um circuito de voz?

Num intervalo bem menor do que o tempo fora do ar que a meta permite. Uma meta de 99,9% num mês de 30 dias tolera 43 minutos; testar de hora em hora pode deixar passar uma queda inteira. No ritmo padrão do Monitor, a chamada de teste acontece a cada 15 minutos, com novas tentativas a cada 2 minutos depois de uma falha.

Por que não alertar já na primeira chamada que falha?

Porque uma falha isolada pode ser uma rota que oscilou uma vez, e um alerta falso às 2h ensina a equipe a ignorar os próximos. Repetir a chamada separa a oscilação da queda: no Monitor, quatro falhas seguidas, por padrão (a primeira e três novas tentativas), abrem um incidente, e só um incidente confirmado avisa alguém por e-mail.

O que é um teste sem visibilidade?

É um teste que não pôde ser feito por um problema do lado de quem testa, por exemplo a plataforma de chamadas do monitoramento sem resposta. Ele não diz nada sobre o circuito. No Monitor, esse período não conta contra o circuito, não entra no SLA e não acorda a equipe do cliente; quem é avisada é a 2N5.

O que mandar para a operadora quando um tronco SIP cai?

O número chamado, a origem, o horário de cada chamada com segundos e fuso, o código SIP da resposta, a causa Q.850 quando ela veio e o Call-ID. Com esses dados a operadora encontra cada chamada nos próprios registros. Inclua também a última chamada que funcionou, para marcar quando a queda começou.

Fontes

1. RFC 3261: SIP, incluindo os métodos OPTIONS e REGISTER, os códigos de resposta e o Call-ID
2. RFC 3264: o modelo de oferta e resposta da negociação de mídia no SIP
3. RFC 3550: RTP e RTCP, incluindo os relatórios de perda e jitter
4. RFC 3960: early media, o áudio antes do atendimento
5. RFC 6432: causas Q.850 no cabeçalho Reason das respostas SIP
6. RFC 6314: práticas de travessia de NAT para SIP, incluindo keep-alive
7. ITU-T P.800.1: terminologia MOS, incluindo MOS-LQO e MOS-CQE
8. ITU-T G.107: o modelo E e o fator R

GUIA

Monitoramento passivo ou chamadas de teste ativas: qual escolher para a telefonia

O monitoramento passivo analisa as chamadas reais que passam pela sua rede; as chamadas de teste ativas ligam por conta própria, de fora, e conferem o resultado. O passivo explica o que aconteceu com quem ligou; o ativo avisa quando ninguém consegue ligar, inclusive quando ninguém tentou. Quase sempre vale ter os dois, e este guia mostra em que ordem.

Por Equipe 2N5 Publicado em 14 de outubro de 2026 Atualizado em 14 de outubro de 2026

Resumo

- Monitoramento passivo captura ou lê o tráfego SIP e RTP das chamadas reais e calcula indicadores como MOS estimado, jitter e perda de pacotes.
- Chamadas de teste ativas partem de fora da rede, em horário marcado, e verificam se o número completa, quem atende e como está o áudio.
- O passivo não vê o que não passou pela sua rede: uma falha na rota da operadora que impede a chamada de chegar não deixa nenhum registro para analisar.
- O ativo não vê o motivo dentro da sua rede: ele mostra que a chamada falhou e com que código, mas não substitui a captura para investigar a causa.
- Para um 0800 ou uma URA, comece pelo teste ativo; para um tronco com muito tráfego e queixas de qualidade, some o passivo.

Qual a diferença entre monitoramento passivo e chamadas de teste ativas?

No monitoramento passivo, a ferramenta fica de fora do caminho e olha as chamadas que os clientes fizeram; nas chamadas de teste ativas, a ferramenta liga. A diferença muda o que cada uma consegue ver. O passivo vê tudo o que passou pela sua rede e nada do que não passou; o ativo vê o resultado de uma chamada de cliente simulada, a qualquer hora, mas só nas chamadas que ele faz.

	Monitoramento passivo	**Chamadas de teste ativas**
O que faz	Captura ou lê o tráfego das chamadas reais	Liga para os números, em horário marcado
Exemplos de ferramentas	VoIPmonitor (captura de SIP e RTP); PRTG e Zabbix medem a rede e o PABX por sensores, sem chamadas de teste	Monitor da 2N5
Precisa de tráfego real?	Sim: sem chamada, não há o que analisar	Não: gera as próprias chamadas
Vê a falha na rota da operadora?	Só se alguma chamada chegar a ser registrada	Sim, vê a chamada que não completa
Vê a URA trocada ou a mensagem da operadora?	Não, a menos que alguém ouça	Sim, compara com a gravação de referência
Vê a causa dentro da sua rede?	Sim, com a captura da chamada	Só o código SIP e a causa Q.850 devolvidos
Instalação	Na sua rede (espelhamento de porta, espelhamento no SBC ou leitura do PABX)	Nenhuma: liga de fora

Sobre as ferramentas da tabela, os fatos vêm das páginas dos próprios fabricantes, listadas nas fontes: o VoIPmonitor faz captura passiva de SIP e RTP, com MOS, detecção de áudio de um lado só e regras de fraude, e não faz chamadas; o PRTG usa sensores de SIP OPTIONS, QoS e Cisco IP SLA, com MOS estimado a partir da rede; o Zabbix lê trunks, canais e filas do Asterisk. Nas páginas que consultamos, nenhum dos três liga para a rede pública para conferir um 0800 ou uma URA.

Quando o monitoramento passivo é a melhor escolha?

Quando você precisa entender chamadas que já aconteceram. Com a captura, é possível abrir uma chamada específica, ver a sinalização e o áudio, e descobrir se o atraso estava no seu SBC ou na operadora. O passivo é a ferramenta certa para:

- investigar a reclamação de um cliente sobre uma chamada específica;
- acompanhar indicadores de tráfego real, como a taxa de completamento (ASR e ACD) e o tempo de pós-discagem;
- detectar padrões de fraude e uso anormal do tronco;
- medir jitter e perda de pacotes das chamadas que de fato passaram.

Quando as chamadas de teste ativas são a melhor escolha?

Quando o risco é o número ficar fora do ar sem ninguém perceber. As chamadas ativas servem melhor a:

- **0800, 0300 e 4004**, cujo problema costuma estar antes da sua rede, na rota ou na portabilidade, onde nenhum equipamento seu enxerga;
- **URA**, para conferir que atende a mensagem certa e não a da operadora;
- **madrugada, fim de semana e números pouco discados**, em que o tráfego real é pouco ou nenhum;
- **medir o SLA da operadora** com um registro independente de cada horário;
- **troncos SIP** que precisam ser conferidos de fora, e não só pelo registro.

Um 0800 que deixou de completar às 2h da manhã não aparece no monitoramento passivo: não houve chamada para capturar. O guia Seu 0800 parou e ninguém avisou mostra esse caso.

Dá para usar os dois?

Dá, e é o arranjo mais comum em operações maiores: o ativo avisa que algo parou, com horário e código; o passivo ajuda a descobrir por que. As ferramentas não competem pelo mesmo trabalho. Uma sequência razoável:

1. **Comece pelo ativo** nos números que dão dinheiro ou que a regra obriga a atender (SAC, 0800 de vendas, URA de suporte).
2. **Some o passivo** quando houver volume de tráfego e dúvidas sobre qualidade que só a análise das chamadas reais resolve.
3. **Use os códigos** das chamadas de teste que falharam como ponto de partida. O guia Chamadas falhando: diagnóstico mostra o que cada um quer dizer.

O que o Monitor da 2N5 faz, e o que não faz?

O Monitor da 2N5 é de chamadas de teste ativas: liga do Brasil para 0800, URA e tronco SIP, em agenda própria para cada circuito, confere o que atendeu, mede a qualidade de voz no áudio recebido (MOS-LQO) e abre um incidente depois de quatro falhas seguidas, a primeira e três novas tentativas. Ele não captura o tráfego da sua rede e não substitui uma ferramenta de captura para achar a causa dentro dela. Veja as comparações com o VoIPmonitor, o PRTG e o Zabbix, e a definição em o que é monitoramento sintético de chamadas.

Perguntas frequentes

Qual a diferença entre monitoramento passivo e ativo de VoIP?

O passivo observa as chamadas que os clientes já fizeram, por captura de tráfego ou leitura de registros, e calcula indicadores sobre elas. O ativo faz as próprias chamadas de teste, em horários marcados, de fora da rede. O passivo explica o que ocorreu com chamadas existentes; o ativo detecta a falha mesmo sem nenhuma chamada real passando.

O VoIPmonitor faz chamadas de teste?

Não. Segundo o site do fabricante, o VoIPmonitor faz captura passiva de SIP e RTP e calcula MOS, detecta áudio de um lado só e aplica regras contra fraude; ele analisa o tráfego e não gera chamadas. É uma ferramenta muito boa para investigar chamadas reais, e outra categoria em relação a ligar para o 0800 e conferir a URA.

O PRTG faz chamadas de teste para o meu 0800?

Pelas páginas do fabricante, o PRTG mede com sensores: ping SIP OPTIONS, tempo de ida e volta de QoS e Cisco IP SLA, com MOS estimado a partir da rede. Não encontramos discagem para a rede pública, 0800 ou URA. Ele mostra a saúde da rede e do tronco; conferir o que atende no 0800 é outra tarefa.

Zabbix monitora tronco SIP e qualidade de chamada?

O Zabbix, que é de código aberto, tem um modelo para Asterisk que lê o estado de troncos e peers, de canais e de filas. Pelo que o fabricante publica, ele não faz chamadas de teste nem avalia o áudio. Serve para ver o PABX por dentro, e não para saber se uma chamada de fora completa.

Preciso dos dois tipos de monitoramento?

Depende do risco. Se o que importa é saber que o 0800, a URA ou o tronco atendem a qualquer hora, comece pelo ativo. Se há muito tráfego e reclamações de qualidade, o passivo mostra as chamadas problemáticas. Em operações maiores os dois convivem: o ativo avisa, o passivo ajuda a achar a causa.

O PRTG e o Zabbix fazem chamadas de teste?

Nas páginas dos fabricantes, não. O PRTG mede com sensores, como ping SIP OPTIONS, QoS de ida e volta e Cisco IP SLA, e o Zabbix lê o estado de troncos, canais e filas pelo modelo do Asterisk. Nenhum dos dois disca para a rede pública nem confere o que atende. Para isso é preciso uma chamada de teste ativa, que liga de fora e ouve o resultado.

Fontes

1. VoIPmonitor: captura passiva de SIP e RTP, MOS e detecção de áudio de um lado só
2. Paessler PRTG: monitoramento de VoIP por sensores (SIP OPTIONS, QoS, Cisco IP SLA)
3. Zabbix: integração com Asterisk (estado de troncos, canais e filas)
4. RFC 3261: SIP, o protocolo que as duas abordagens observam

GUIA

O que é monitoramento sintético de chamadas

Monitoramento sintético de chamadas é um robô que liga, em horários marcados, para o seu 0800, a sua URA ou o seu tronco SIP, como um cliente ligaria, e registra o que aconteceu: se a chamada completou, o que atendeu e como estava o áudio. Ele responde à pergunta que nenhum painel de equipamento responde: o cliente consegue falar com a empresa agora?

Por Equipe 2N5 Publicado em 14 de outubro de 2026 Atualizado em 20 de outubro de 2026

Resumo

- Chamada sintética é uma chamada de teste, feita por um sistema e não por uma pessoa, em horário marcado e sempre da mesma forma.
- Ela mede o que o cliente vive: a chamada completa, a URA certa atende, o áudio passa nos dois sentidos e a qualidade de voz é boa.
- O monitoramento passivo analisa as chamadas reais que já passaram; o sintético vê também a hora em que ninguém ligou.
- Para valer como medida, a chamada precisa ser real: um PABX ligado e um tronco registrado não provam que uma chamada completa.
- No Monitor da 2N5, cada circuito de voz recebe uma chamada de teste a cada 15 minutos por padrão, e só quatro falhas seguidas abrem um incidente.

O que é monitoramento sintético de chamadas?

Monitoramento sintético de chamadas é a prática de ligar de propósito, por um sistema e em horários marcados, para os números que o cliente disca, e registrar o resultado de cada ligação. A chamada é “sintética” porque quem liga é um robô, não um cliente; ela é real porque percorre a rede da operadora de verdade, do mesmo jeito que a de um cliente.

Cada chamada de teste segue um roteiro fixo: ligar para o número, esperar o atendimento, ouvir o que atendeu, comparar com o que deveria atender e desligar. O que fica registrado é o que importa para quem cuida da telefonia: se completou, em quanto tempo, com que código SIP, e como estava a voz.

Para que serve uma chamada de teste?

Ela responde, de hora em hora ou de quinze em quinze minutos, uma pergunta só: **um cliente conseguiria falar com a empresa agora?** Os painéis do PABX e do tronco respondem outra pergunta, se o equipamento está de pé, e as duas respostas podem ser diferentes.

O que aconteceu	O painel do PABX mostra	A chamada de teste mostra
A operadora parou de rotear o 0800 até o tronco	Tudo verde, nenhuma chamada	A chamada não completa, com o código SIP devolvido
A URA foi trocada ou a plataforma publicou um fluxo errado	Tudo verde, chamadas atendidas	A saudação ouvida não confere com a gravação de referência
A operadora atende com a mensagem “número inexistente”	Nenhuma chamada	A chamada completa, mas a mensagem não é a da URA

O que aconteceu	O painel do PABX mostra	A chamada de teste mostra
A chamada completa, mas o áudio vai só para um lado	Chamada normal	Áudio ausente ou fraco na medição
A qualidade da voz caiu na rota	Sem alarme	MOS-LQO abaixo do limite

Um 0800 que passa a noite fora do ar sem ninguém perceber é o caso clássico. O guia Seu 0800 parou e ninguém avisou mostra uma noite hora a hora.

Como funciona uma chamada sintética?

Em quatro passos, repetidos na agenda de cada circuito:

1. **Ligar.** O sistema disca o número monitorado (0800, 0300, 4004, número fixo ou o número de um tronco SIP) a partir de fora da rede do cliente.
2. **Ouvir.** Registra se a chamada completou, o código SIP e a causa Q.850 devolvidos, e o áudio recebido.
3. **Comparar.** Confere o que atendeu com a gravação de referência da URA e mede a qualidade de voz no áudio recebido, o MOS-LQO.
4. **Decidir.** Uma falha isolada é repetida; só falhas seguidas viram incidente e alerta.

O último passo é o que separa um monitoramento útil de um gerador de alarme falso. No ritmo padrão do Monitor da 2N5, cada circuito recebe uma chamada a cada 15 minutos. Quando uma falha, a chamada é repetida três vezes, a cada 2 minutos; quatro falhas seguidas, a primeira e três novas tentativas, abrem o incidente, e duas chamadas boas seguidas confirmam a volta. O guia Alerta de queda de linha, sem falso alarme descreve esse caminho.

Qual a diferença para o monitoramento passivo?

O monitoramento passivo observa as chamadas reais que passam pela rede, por captura de tráfego, e calcula indicadores sobre elas. O sintético liga por conta própria. A consequência prática é simples: o passivo só enxerga o que aconteceu quando havia chamada, e de madrugada, num fim de semana ou num número pouco discado, pode não haver nenhuma.

Os dois se completam, e nenhum substitui o outro. O guia Monitoramento passivo vs chamadas de teste ativas compara os dois e diz quando cada um serve.

O que a chamada sintética não vê?

Ela vê o que acontece a partir da origem de onde liga. Uma falha que só vale para os clientes de uma operadora de celular, ou de uma região, pode passar despercebida se a chamada de teste parte de outro caminho; o guia Por que um 0800 não completa do celular trata desse caso. Ela também não substitui a análise das chamadas reais para encontrar a causa dentro da sua rede.

Que termos aparecem junto com o assunto?

Quem pesquisa o tema encontra, em português, “chamada de teste”, “monitoramento ativo” e “teste de disponibilidade”; em inglês, “synthetic calls” e “synthetic voice monitoring”. São o mesmo conceito. O que muda de uma ferramenta para outra é o que ela liga (só o número, a URA inteira, o tronco SIP), de onde liga e o que faz com o resultado.

Como o Monitor da 2N5 faz isso?

O Monitor da 2N5 é um serviço gerenciado: a 2N5 cadastra cada circuito, grava a saudação de referência da URA, define a agenda e liga do Brasil para 0800, URA e tronco SIP. Cada ligação vira um registro com horário, número chamado, código SIP, causa Q.850 e MOS-LQO, e o conjunto vira o relatório de SLA do mês e dos últimos 12 meses. Veja como funciona e o monitoramento de 0800 e URA.

Perguntas frequentes

O que é uma chamada sintética?

É uma chamada de teste iniciada por um sistema, em horário agendado, que segue sempre o mesmo roteiro: ligar para um número, ouvir quem atende, às vezes apertar uma opção da URA e desligar. O resultado de cada chamada fica registrado com horário, código SIP, causa Q.850 e avaliação do áudio, e vira a base da disponibilidade medida.

Monitoramento sintético é o mesmo que monitoramento ativo?

Na telefonia, na prática, sim. Os dois termos descrevem testes que o próprio monitoramento inicia, em oposição ao monitoramento passivo, que só observa as chamadas que os clientes já fizeram. Sintético é o nome usado em monitoramento de sites e de redes, e ativo é o nome mais comum entre quem trabalha com VoIP.

Para que serve a chamada sintética se eu já monitoro o PABX?

O monitoramento do PABX mostra o equipamento por dentro. A chamada sintética mostra o caminho inteiro por fora, da operadora ao atendimento. Uma rota quebrada na operadora, uma portabilidade mal feita ou uma URA trocada deixam o PABX com tudo verde, porque nenhuma chamada chega a ele. Só uma chamada de fora enxerga isso.

A chamada sintética atrapalha os canais do meu tronco?

Quase nada. Cada chamada de teste ocupa um canal por poucos segundos, e o Monitor trabalha dentro de um limite de chamadas combinado para não disputar canal com os seus clientes. A frequência padrão é de uma chamada a cada 15 minutos por circuito, o que dá 96 chamadas curtas por dia.

Com que frequência a chamada sintética deve rodar?

Quanto menor o intervalo, menos tempo uma queda passa sem ser vista. A cada 15 minutos, uma queda é vista em até 15 minutos e confirmada em mais 6 pelas novas tentativas. Para uma meta de 99,9% ao mês, que tolera 43 minutos, um teste de hora em hora é pouco.

Fontes

1. RFC 3261: SIP, o protocolo das chamadas de teste e os códigos de resposta
2. RFC 6432: causas Q.850 no cabeçalho Reason das respostas SIP
3. ITU-T P.800.1: terminologia MOS, incluindo MOS-LQO
4. ITU-T E.800: definições de qualidade de serviço, incluindo disponibilidade

GUIA

Por que um 0800 não completa do celular, se funciona do fixo

Quando o 0800 da empresa atende do telefone fixo do escritório mas não completa de um celular, o problema quase nunca é o atendimento. Está em algum ponto entre a operadora de quem liga e a configuração do número. Este artigo lista as causas, na ordem em que vale a pena conferir.

Por Equipe 2N5 Publicado em 7 de outubro de 2026 Atualizado em 14 de outubro de 2026

Resumo

- O 0800 é gratuito para quem liga; quem paga é o assinante, e a chamada de celular costuma custar mais para ele.
- Muitos serviços 0800 permitem ao assinante escolher de que origens aceita chamadas; uma restrição esquecida derruba as chamadas de celular.
- Cada origem segue a sua própria rota até o 0800: uma rota pode falhar enquanto as outras funcionam.
- Teste de pelo menos dois celulares de operadoras diferentes e anote horário, número de origem e o que se ouviu.
- Para as prestadoras de telecomunicações, a Anatel exige que o atendimento telefônico receba chamadas de telefones fixos e celulares.

Por que o 0800 funciona do fixo e não do celular?

Porque a chamada de cada origem faz um caminho diferente até o 0800, e basta um desses caminhos falhar. A chamada de um celular passa pela operadora móvel de quem liga, que precisa encaminhá-la para a operadora dona do 0800, que traduz o 0800 para o número real de atendimento e só então entrega a chamada ao tronco e à URA da empresa. Uma restrição de origem, uma rota mal configurada ou uma tradução feita só para algumas origens derrubam as chamadas de celular sem afetar as do fixo.

“Não funciona do celular” e “não completa do celular” são o mesmo problema?

São, na prática. Quem diz que o 0800 “não funciona do celular” costuma descrever uma chamada que não completa: silêncio, ocupado, queda depois de alguns segundos ou uma mensagem da operadora. Se o 0800 inteiro está fora do ar, a falha vale também para o fixo; veja o guia Seu 0800 parou e ninguém avisou. Se só o celular falha, as causas abaixo são o ponto de partida.

Quais são as causas mais comuns?

Causa	O que quem liga do celular ouve	Onde verificar
Restrição de origem no serviço 0800	Mensagem da operadora dizendo que a chamada não pode ser completada, ou ocupado	Contrato e configuração do 0800 com a operadora dona do número
Tradução do 0800 configurada só para algumas origens ou áreas	Mensagem de número inexistente, ou silêncio	Operadora dona do 0800
Rota entre a operadora móvel e a operadora do 0800 com problema	Silêncio, ou queda depois de alguns segundos	Operadora móvel de quem liga e operadora do 0800

Causa	O que quem liga do celular ouve	Onde verificar
O tronco ou a URA recusa o formato do número de origem	Ocupado, ou mensagem de erro do próprio PABX	Regras de entrada do PABX ou do SBC (formato do número A)
Capacidade do tronco esgotada nos horários de pico	Ocupado em alguns horários	Canais simultâneos contratados e ocupação do tronco

Restrição de origem

O 0800 é gratuito para quem liga: pelo regulamento de numeração da Anatel, a instituição assinante paga a chamada. Como a chamada de celular costuma custar mais para o assinante, muitos serviços 0800 permitem escolher de que origens o número aceita chamadas. Uma restrição criada para economizar, ou herdada de um contrato antigo, faz o número funcionar do fixo e falhar do celular. É a primeira coisa a perguntar à operadora.

Tradução e rota

Por trás do 0800 existe um número real. A operadora dona do 0800 guarda essa tradução e pode configurá-la por origem ou por região, por exemplo para mandar as chamadas de cada estado a um atendimento diferente. Se a tradução para chamadas de celular, ou de uma região, estiver errada ou faltando, só essas chamadas falham. O mesmo acontece quando a rota entre a operadora móvel de quem liga e a operadora do 0800 tem um problema de interconexão.

O próprio PABX ou SBC

As chamadas chegam ao tronco da empresa com o número de quem liga, e esse número tem formatos diferentes conforme a origem: com ou sem o 0 e o código da operadora, com DDD, às vezes em formato internacional. Uma regra de entrada que só aceita um formato, ou que usa o número de origem para escolher o destino, pode recusar as chamadas de celular. No log do PABX elas aparecem como recusadas, por exemplo com SIP 403 ou SIP 484.

Como testar antes de abrir chamado?

Faça chamadas de teste de várias origens no mesmo horário e anote o resultado de cada uma.

1. **Ligue de um telefone fixo e de celulares de pelo menos duas operadoras diferentes**, no mesmo intervalo de 10 a 15 minutos.
2. **Anote para cada chamada** o número de origem, a operadora, o horário com fuso e o que se ouviu: atendimento normal, silêncio, ocupado, mensagem da operadora (copie o texto).
3. **Confira o log do PABX ou do SBC** para as chamadas que deveriam ter chegado. Se não há registro, a chamada não chegou ao seu tronco e o problema está antes, na operadora. Se há registro com recusa, o problema está na sua regra de entrada.
4. **Abra o chamado com a operadora dona do 0800**, com a tabela das chamadas. Peça que ela confira a restrição de origem e a tradução do número.

O que a regra exige do atendimento?

Para os SACs dos setores regulados, o Decreto nº 11.034/2022, até 1º de novembro de 2026, e o Decreto nº 13.135/2026, a partir de 2 de novembro de 2026, garantem o acesso gratuito ao SAC e tornam obrigatório o atendimento por telefone. Para as prestadoras de telecomunicações, o Regulamento Geral de Direitos do Consumidor da Anatel (Resolução nº 765/2023) é explícito: o

atendimento telefônico deve ser gratuito, ficar disponível 24 horas e receber chamadas originadas de telefones fixos e de celulares. Um 0800 que não completa do celular deixa de fora justamente o cliente que só tem celular.

E o monitoramento?

Um monitoramento por chamada real mostra se o 0800 completa e se a URA atende com a mensagem certa, a partir da origem de onde ele liga. O Monitor liga da plataforma da 2N5: ele avisa quando o número para de completar ou a URA muda, mas não testa cada operadora de celular. Para uma restrição que só afeta celulares, o teste manual acima continua sendo o caminho. Veja como o monitoramento de 0800 e URA funciona.

Perguntas frequentes

Ligar para 0800 do celular é de graça?

Sim. Pelo regulamento de numeração da Anatel, no código 0800 a instituição assinante se responsabiliza pelo pagamento, e a chamada é sem ônus para quem liga, de telefone fixo ou de celular. Por isso o custo da chamada de celular recai sobre a empresa dona do número.

Por que algumas empresas bloqueiam 0800 para celular?

Porque a chamada de celular para 0800 custa mais para quem paga, que é a empresa. Alguns contratos de 0800 permitem escolher as origens aceitas. Uma restrição criada para economizar, ou herdada de um contrato antigo, impede o cliente que só tem celular de ser atendido.

Como provar para a operadora que o 0800 não completa do celular?

Faça chamadas de teste de celulares de pelo menos duas operadoras e de um telefone fixo, no mesmo horário. Anote para cada uma o número de origem, o horário com fuso e o que se ouviu: silêncio, mensagem da operadora, ocupado. Com isso a operadora consegue localizar a rota que falhou.

Um monitoramento que liga para o 0800 pega esse problema?

Pega quando a falha atinge a origem de onde ele liga. O Monitor liga da plataforma da 2N5, então mostra se o 0800 completa e se a URA atende com a mensagem certa a partir dessa origem. Ele não substitui o teste de cada operadora de celular.

Meu 0800 não funciona do celular, mas funciona do fixo. O que isso quer dizer?

Quer dizer que a falha vale só para as chamadas que chegam pela rede móvel, e não que o número esteja fora do ar. As causas mais comuns são uma restrição de origem no serviço 0800, uma tradução configurada só para algumas origens, uma rota com problema entre a operadora móvel e a do 0800 ou uma regra de entrada do PABX que recusa o formato do número.

Por que o meu 0800 não completa ligações do celular?

Quase sempre porque a falha está na rota ou na regra do número, e não porque o 0800 está desligado. As causas mais comuns são uma restrição de origem no serviço 0800 que bloqueia a rede móvel, uma tradução configurada só para algumas origens, uma rota com problema entre a operadora móvel e a do 0800 ou uma regra de entrada do PABX. Teste de celulares de duas operadoras e de um fixo.

Fontes

1. Anatel, Resolução nº 749/2022 (Regulamento de Numeração), art. 18: código 0800 sem ônus para quem liga
2. Anatel, Resolução nº 765/2023 (RGC), art. 15: atendimento telefônico gratuito, 24 horas, recebendo chamadas do STFC e do SMP
3. Decreto nº 11.034/2022, arts. 3º e 4º: acesso gratuito ao SAC e atendimento telefônico obrigatório (vale até 1º de novembro de 2026)
4. Decreto nº 13.135/2026, arts. 8º e 14: acesso gratuito ao SAC e atendimento telefônico obrigatório (vale a partir de 2 de novembro de 2026)
5. RFC 3261: códigos de resposta SIP

GUIA

Qualidade de voz em VoIP: MOS e MOS-LQO na prática

Uma chamada pode completar, ter áudio nos dois sentidos e ainda soar picotada. A nota MOS é a forma padrão de dizer o quanto, mas existe mais de um MOS, e eles não medem a mesma coisa. Este guia explica a escala, as siglas da ITU-T, o que jitter, perda e atraso fazem com a voz e como agir quando a nota cai.

Por Equipe 2N5 Publicado em 7 de outubro de 2026 Atualizado em 7 de outubro de 2026

Resumo

- A escala MOS da ITU-T P.800 vai de 5 (excelente) a 1 (ruim) e nasceu de testes com ouvintes.
- Pela ITU-T P.800.1, MOS-LQO é a qualidade de escuta calculada por um modelo objetivo; a saída do modelo E da G.107 é MOS-CQE, uma estimativa.
- Um MOS medido compara o áudio recebido com uma gravação de referência, como faz a P.863 (POLQA); a P.862 (PESQ) foi retirada em 5 de janeiro de 2024.
- No modelo E, os valores padrão dão R ≈ 93,2; R 80 corresponde a MOS 4,03, R 60 a 3,10, e o MOS-CQE máximo é 4,5.
- A G.114 recomenda até 400 ms de atraso num sentido para planejamento; abaixo de 150 ms o atraso é praticamente transparente.
- No Monitor, o circuito está saudável com MOS-LQO a partir de 3,8 e degradado abaixo de 3,0, limites que a 2N5 ajusta por circuito.

O que é MOS em VoIP?

MOS em VoIP é a nota média de opinião, *Mean Opinion Score*, da qualidade de uma chamada, numa escala de 1 a 5. A nota nasceu de testes em que ouvintes davam notas a amostras de áudio, pelos métodos da ITU-T P.800. Hoje quase toda nota MOS é calculada por um modelo, que tenta prever o que esses ouvintes diriam.

Quem procura por “MOS score” encontra a mesma coisa: o S já é de *score*, e o termo é só a forma como a sigla circula em inglês. O que muda de uma ferramenta para outra é o que entra no cálculo. Um PABX pode mostrar 4,2 para uma chamada que um modelo de escuta avalia em 3,1, e os dois números podem estar certos, porque medem coisas diferentes: um estima a qualidade a partir da rede, o outro ouve o áudio que chegou. Antes de comparar duas notas, é preciso saber de que tipo cada uma é.

Como é a escala MOS da ITU-T P.800?

A escala MOS da ITU-T P.800 tem cinco categorias, de 5 (excelente) a 1 (ruim). No método de classificação por categoria absoluta, cada ouvinte escuta uma amostra e escolhe uma categoria; a média das notas de todos os ouvintes é o MOS daquela amostra. É uma média de opiniões, não uma medida física do sinal.

Nota	Categoria	Na P.800, em inglês
5	Excelente	Excellent
4	Boa	Good

Nota	Categoria	Na P.800, em inglês
3	Razoável	Fair
2	Pobre	Poor
1	Ruim	Bad

Duas consequências práticas. Primeiro, por ser uma média, a nota raramente chega aos extremos: basta parte dos ouvintes não dar 5 para a média ficar abaixo disso, mesmo com áudio sem defeito. Segundo, cada modelo que prevê o MOS tem a sua própria faixa útil. O MOS estimado pelo modelo E, por exemplo, para em 4,5. Por isso um “4,3” de uma ferramenta e um “4,3” de outra não são automaticamente a mesma qualidade.

O que significam MOS-LQO, MOS-CQE e as outras siglas?

As siglas MOS-LQO, MOS-CQE e as demais vêm da ITU-T P.800.1, que dá nome a cada tipo de MOS por duas perguntas: o que foi avaliado, a escuta ou a conversação, e como a nota foi obtida, com ouvintes, com um modelo sobre o sinal ou com um modelo sobre parâmetros da rede. Cada combinação tem a sua sigla.

	Subjetiva: ouvintes	Objetiva: modelo sobre o áudio	Estimada: modelo sobre parâmetros
Qualidade de escuta (LQ)	MOS-LQS	MOS-LQO	MOS-LQE
Qualidade de conversação (CQ)	MOS-CQS	MOS-CQO	MOS-CQE

A diferença entre escuta e conversação importa mais do que parece. A qualidade de escuta avalia o áudio num sentido: se a voz chegou clara. Ela não vê o atraso, porque um ouvinte que só escuta não percebe se a resposta demorou. A qualidade de conversação inclui o que atrapalha uma conversa de verdade, como atraso e eco. Um MOS-LQO alto com 500 ms de atraso é possível: a voz soa limpa e a conversa é ruim.

A saída do modelo E da ITU-T G.107 é um MOS-CQE: uma estimativa de qualidade de conversação, feita a partir de parâmetros. Uma medição como a da P.863 é um MOS-LQO: qualidade de escuta, calculada sobre o áudio. Chamar as duas só de “MOS” é a origem da maior parte das discussões sobre nota de voz.

Qual a diferença entre MOS medido e MOS estimado?

A diferença entre MOS medido e MOS estimado está no que entra no cálculo. O MOS medido, um MOS-LQO, vem do áudio que a chamada recebeu, comparado com a gravação esperada. O MOS estimado, um MOS-CQE, vem de números da rede, como perda de pacotes, jitter e atraso, aplicados a um modelo que nunca ouve a chamada.

MOS medido: o áudio contra a referência

Os modelos com referência recebem dois sinais, o de referência e o degradado, e calculam o quanto o segundo se afastou do primeiro de um jeito que um ouvinte notaria. Os mais citados:

- **P.863 (POLQA)**: a recomendação da ITU-T para qualidade de escuta objetiva, que devolve um MOS-LQO.

- **P.862 (PESQ)**: a recomendação anterior, retirada pela ITU-T em 5 de janeiro de 2024 e substituída pela P.863. Ainda aparece em equipamentos e relatórios antigos. Veja POLQA e PESQ.

Como ouvem o áudio, esses modelos veem o que a rede não informa: voz cortada na origem, ruído, conversão de codec malfeita, o efeito real da perda de pacotes depois que o telefone tentou disfarçá-la, e até uma mensagem errada no lugar da saudação, porque a comparação com a referência não passa.

MOS estimado: o modelo E e o fator R

O modelo E da ITU-T G.107 é uma ferramenta de planejamento de transmissão. Ele soma as degradações de uma rota num índice, o fator R:

R = Ro – Is – Id – Ie,eff + A

Ro é a relação sinal-ruído básica, Is as degradações simultâneas ao sinal de voz, Id as degradações causadas pelo atraso e pelo eco, Ie,eff a degradação do equipamento, que inclui o codec e a perda de pacotes, e A o fator de vantagem, a tolerância do usuário em troca de mobilidade, por exemplo. Com todos os valores padrão da G.107, R ≈ 93,2.

A G.107 converte R em MOS-CQE por uma fórmula, válida para R entre 0 e 100: **MOS = 1 + 0,035 × R + R × (R – 60) × (100 – R) × 7 × 10^{-6}**. Para R a partir de 100, o MOS-CQE é 4,5, o máximo. Para o R padrão: 1 + 0,035 × 93,2 + 93,2 × 33,2 × 6,8 × 7 × 10^{-6} = 1 + 3,262 + 0,147 ≈ 4,41.

Fator R	MOS-CQE
100 ou mais	4,50
93,2 (valores padrão)	4,41
90	4,34
80	4,03
70	3,60
60	3,10
50	2,58

Repare que a nota máxima de uma rota perfeita, pelo modelo E, fica em 4,41 com os valores padrão. Um equipamento que mostra um MOS de 4,4 para todas as chamadas de uma rede sem perda está mostrando o teto do modelo, não uma qualidade medida.

Quando usar cada um

	MOS-LQO medido	MOS-CQE estimado
Entrada	O áudio recebido e a gravação de referência	Perda, jitter, atraso e o codec da rota
Exige referência	Sim	Não
Vê o atraso	Não: é qualidade de escuta	Sim, pelo termo Id
Vê áudio cortado na origem ou mensagem errada	Sim	Não
Bom para	Saber se a voz chegou clara a quem ligou	Planejar uma rota e acompanhar a rede

As duas têm lugar. Uma estimativa de rede é barata e serve para olhar cada chamada da central. Uma chamada escutada diz se a voz chegou.

Que nota MOS é boa em VoIP?

Uma nota MOS boa em VoIP, num MOS-LQO medido, fica perto de 4: a voz soa clara e ninguém precisa se esforçar para entender. Abaixo de 3, as pessoas começam a reclamar. Os números valem para a qualidade de escuta medida; um MOS-CQE estimado usa outra conta e não deve ser comparado com eles diretamente.

A tabela descreve, de forma aproximada, o que se ouve em cada faixa de MOS-LQO, e como o Monitor lê cada faixa com os limites padrão:

MOS-LQO	O que se ouve	Leitura no Monitor
4,0 ou mais	Voz clara, sem esforço; as diferenças só aparecem lado a lado com a referência	Saudável
De 3,8 a 4,0	Clara, com alguma perda de nitidez perceptível para quem presta atenção	Saudável
De 3,0 a 3,8	Inteligível, com cortes curtos, chiado ou voz metálica; a conversa exige atenção	Em operação, com a nota marcada abaixo do ideal
De 2,0 a 3,0	Palavras perdidas e pedidos de repetição; é a faixa das reclamações	Degradado
Abaixo de 2,0	Conversa difícil ou impossível	Degradado

O limite certo depende do uso. Uma URA que só toca uma saudação tolera menos degradação do que parece, porque o cliente não pode pedir para repetir; um tronco interno entre filiais pode viver com uma nota um pouco menor. Por isso os limites do Monitor são ajustados por circuito.

Quanto jitter é aceitável?

O jitter aceitável é o que o buffer de jitter do telefone ou do PABX consegue absorver sem descartar pacotes e sem somar atraso demais. As recomendações citadas aqui não fixam um número único: o mesmo jitter que um buffer grande absorve sem perda vira picote num buffer pequeno, e o buffer grande cobra o preço em atraso.

Jitter é a variação do atraso entre um pacote e o seguinte. Os pacotes de voz saem em intervalos regulares, por exemplo um a cada 20 ms, e chegam em intervalos irregulares. O buffer de jitter segura os pacotes por alguns milissegundos e os entrega no ritmo certo. Um pacote que chega depois do tempo do buffer é descartado, e para quem ouve isso é igual a um pacote perdido.

A RFC 3550 define como o RTP calcula o jitter entre chegadas: a cada pacote, a estimativa anda 1/16 da diferença entre a variação medida e a estimativa anterior, **$J = J + (|D| - J) \div 16$**. Esse é o valor que os relatórios RTCP trazem e que muitos equipamentos mostram. Ele é uma média suavizada: picos curtos de jitter, que são os que estouram o buffer, quase não aparecem nele.

A conta que importa é a do atraso total. Um exemplo, com valores ilustrativos: 40 ms de rede, 20 ms de empacotamento e um buffer de jitter de 60 ms somam 40 + 20 + 60 = 120 ms num sentido. Dobrar o buffer para absorver mais jitter leva o total para 180 ms, acima da faixa praticamente transparente da G.114. Um MOS-LQO medido mostra o resultado dessa troca no áudio; o número de jitter sozinho não mostra.

No Monitor, o jitter do link de internet de cada local é medido pelo agente de circuito de dados, junto com latência, perda de pacotes, tempo de DNS e velocidade.

Quanta perda de pacotes a voz aguenta?

A perda de pacotes que a voz aguenta depende do codec, da capacidade do telefone de disfarçar o pacote que falta e do jeito como a perda acontece. Perda espalhada, um pacote aqui e outro ali, é disfarçada melhor do que perda em rajadas, quando vários pacotes seguidos somem e uma sílaba inteira desaparece.

O modelo E da G.107 traduz isso no termo Ie,eff, a degradação do equipamento com perda: **Ie,eff = Ie + (95 − Ie) × Ppl ÷ (Ppl ÷ BurstR + Bpl)**. Ie é a degradação do codec sem perda, Ppl a porcentagem de pacotes perdidos, Bpl a robustez do codec à perda e BurstR o quanto a perda é concentrada em rajadas. Quanto maior BurstR, maior a degradação para a mesma porcentagem de perda de pacotes. A fórmula deixa claro que a mesma perda pesa diferente em codecs diferentes, e por isso uma regra única de “perda aceitável” engana.

Uma medição com referência evita a discussão: ela ouve o resultado depois do disfarce, do buffer e do codec, e dá a nota do que chegou. A escolha do codec de voz também conta: cada conversão de codec no caminho degrada o áudio um pouco, e um codec de taxa baixa começa com uma nota menor antes de qualquer perda.

Quanto atraso é aceitável numa chamada VoIP?

O atraso aceitável numa chamada VoIP, pela ITU-T G.114, é de até 400 ms num sentido para fins de planejamento de rede. Abaixo de 150 ms, o atraso é praticamente transparente para a maior parte das aplicações. Entre os dois valores, a conversa funciona, mas os interlocutores começam a falar ao mesmo tempo e a esperar a resposta.

O atraso não estraga o som, estraga a conversa. A voz chega limpa e atrasada. Por isso um MOS-LQO, que é qualidade de escuta, não vê o atraso, e o modelo E, que estima qualidade de conversação, vê, pelo termo Id. O atraso também torna o eco mais incômodo: um eco que chega rápido se confunde com a própria voz, e um que chega tarde é ouvido como uma segunda voz.

As parcelas do atraso num sentido, para fazer a conta da sua rota:

- **empacotamento**: o tempo de áudio em cada pacote, por exemplo 20 ms;
- **processamento do codec** nos dois lados;
- **rede**: o tempo de trânsito, que o agente de circuito de dados mede como latência no link do local;
- **buffer de jitter**: o tempo que o receptor segura os pacotes;
- **conversões no caminho**: cada SBC ou PABX que decodifica e codifica de novo soma o seu tempo.

Por que a gravação de referência importa?

A gravação de referência importa porque um modelo com referência compara dois sinais: o que deveria ter sido ouvido e o que foi ouvido. Sem a referência, não há com o que comparar, e a nota vira uma estimativa. Com ela, a mesma comparação que mede a qualidade também mostra quando a mensagem errada atendeu.

A referência precisa ser o que de fato deveria tocar: a saudação da URA, gravada limpa, ou um tom de teste conhecido. Se a URA troca a saudação de propósito, a referência também precisa mudar, ou toda chamada passa a parecer errada. No Monitor, a 2N5 grava a referência de cada número na implantação. O áudio guardado é o da gravação ou da URA, nunca a voz de uma pessoa, e é guardado pelo prazo que a 2N5 definir.

Como medir a qualidade de voz de um tronco SIP, 0800 ou URA?

A qualidade de voz de um tronco SIP, de um 0800 ou de uma URA se mede ligando para o número e escutando o áudio que chega, comparado com a referência. Uma chamada real vê o caminho inteiro, operadora, tronco, PABX e URA, que nenhum equipamento sozinho vê.

É o que o Monitor faz em cada chamada de teste de cada **circuito de voz**, o tronco SIP, 0800 ou número de atendimento monitorado. A 2N5 grava o áudio que a chamada recebeu e o compara com a gravação esperada usando um modelo perceptual de qualidade de escuta com referência, que devolve um MOS-LQO (ITU-T P.800.1). A qualidade é medida no áudio; o Monitor não estima a nota pela rede.

Com os limites padrão, o circuito está saudável com MOS-LQO a partir de 3,8 e degradado abaixo de 3,0; a 2N5 ajusta os limites com você, por circuito, na implantação. Uma nota abaixo do limite marca a chamada de teste como degradada, e ela passa pelas mesmas novas tentativas de qualquer falha. Se continuar, abre um incidente de qualidade, a escada de escalonamento é avisada, e os contatos do cliente também ficam sabendo do problema e da solução.

A nota de cada chamada aparece na página do circuito, com as linhas de limite, no painel ao lado do estado do circuito e nos relatórios de SLA. Veja os detalhes em qualidade de voz medida.

Como agir quando a nota MOS cai?

Quando a nota MOS cai, o primeiro passo é confirmar que a queda se repete e ver o alcance: um circuito só, vários do mesmo local ou vários da mesma operadora. O alcance diz onde procurar, e a evidência de cada chamada é o que leva o problema para quem pode resolvê-lo.

O que se vê	Causa provável	O que conferir
Nota baixa em todos os circuitos de um mesmo local	Link de internet do local: perda, jitter ou congestionamento	Latência, perda e jitter do circuito de dados no mesmo horário
Nota baixa só nos circuitos de uma operadora	Rota ou codec da operadora	Codec negociado e evidências de cada chamada
Nota baixa em horários de pico	Link de saída saturado, sem prioridade para a voz	Uso do link e priorização do tráfego de voz
Nota baixa constante, sem perda na rede	Codec de taxa baixa, conversões de codec, nível ou ruído na origem	Codecs do caminho e a própria gravação na URA
Nota muito baixa de repente, com a chamada completa	Mensagem diferente da referência ou áudio de um lado só	O áudio da chamada e o guia de ligação muda

Na prática, a sequência:

1. **Confirme.** Uma nota baixa isolada não é tendência. No Monitor, a chamada degradada é repetida antes de qualquer incidente.
2. **Veja o alcance.** Compare os circuitos do mesmo local e os da mesma operadora no mesmo horário.

3. **Olhe o link.** Se o local tem um circuito de dados monitorado, os gráficos das últimas 100 horas mostram latência, perda e jitter no momento da queda.
4. **Confira codecs e conversões.** Cada decodificação e nova codificação no caminho custa nota. Veja se a chamada passa por conversões que poderiam ser evitadas.
5. **Confira a prioridade da voz.** Num link compartilhado, a voz precisa de prioridade sobre o resto do tráfego, sobretudo no sentido de envio, que costuma ser o mais estreito.
6. **Leve à operadora com evidência.** Horário de cada chamada, número chamado, nota de cada uma e a última chamada saudável.

O que pedir num contrato de qualidade de voz?

Num contrato de qualidade de voz, peça que a nota seja definida pelo nome completo: qual MOS, pela terminologia da P.800.1, qual modelo e versão, contra qual referência, medido onde e com que frequência. Sem isso, “MOS mínimo de 4” vale tanto para uma estimativa de rede quanto para uma medição de escuta, que dão números diferentes.

Os itens que tornam a meta verificável:

1. **O tipo de MOS**: MOS-LQO medido ou MOS-CQE estimado.
2. **O modelo**: P.863 ou outro, e a versão; a P.862 foi retirada e não deve ser a base de um contrato novo.
3. **A referência**: qual gravação ou tom é comparado.
4. **O ponto de medição**: uma chamada de fora, como a de um cliente, ou um equipamento dentro da rede.
5. **A regra de violação**: quantas notas abaixo do limite, seguidas, contam como degradação, e se a degradação entra na conta do SLA como indisponibilidade parcial ou como meta separada. O guia de SLA de telefonia mostra como cada escolha muda a conta.

Perguntas frequentes

Qual é uma boa nota de MOS em VoIP?

Depende de qual MOS. Num MOS-LQO medido, perto de 4 a voz soa clara, e abaixo de 3 as pessoas começam a reclamar. No Monitor, o padrão é saudável a partir de 3,8 e degradado abaixo de 3,0. Num MOS estimado pelo modelo E, o máximo é 4,5, e os valores não são comparáveis com uma nota medida.

O que é MOS-LQO?

É a nota de qualidade de escuta, de 1 a 5, calculada por um modelo objetivo a partir do áudio recebido. A sigla vem da ITU-T P.800.1: MOS, nota média de opinião; LQ, qualidade de escuta; O, objetiva. Modelos como a P.863 (POLQA) comparam o áudio recebido com uma referência e devolvem um MOS-LQO.

Quanto jitter é aceitável numa chamada VoIP?

O que o buffer de jitter consegue absorver sem descartar pacotes e sem empurrar o atraso total para além do orçamento. As recomendações citadas aqui não fixam um número único de jitter. A G.114 dá o teto do atraso num sentido, 400 ms para planejamento, e o atraso do buffer entra nessa conta.

Qual modelo de medição usar para comparar notas?

Qualquer modelo com referência que devolva uma nota de qualidade de escuta, como a P.863 (POLQA), a recomendação da ITU-T que substituiu a P.862 (PESQ). O que importa é dizer qual modelo foi usado ao comparar notas, porque cada um tem sua escala e seu teto.

Por que o MOS do meu PABX é diferente do MOS medido?

Porque o PABX normalmente estima a nota a partir de números da rede, como perda de pacotes, jitter e atraso, pelo modelo E da G.107. Essa estimativa não ouve o áudio. Ela não vê um áudio cortado na origem, uma conversão de codec ruim nem uma mensagem errada, que uma medição com referência vê.

Qual a diferença entre MOS e MOS-LQO / POLQA?

O MOS é a escala de 1 a 5 da qualidade de voz; o MOS-LQO é uma nota nessa escala medida no áudio que chegou, comparado com uma gravação de referência. O POLQA é um dos modelos que calculam o MOS-LQO, ao lado do PESQ, hoje retirado pela ITU. Notas de modelos diferentes não se comparam, e um MOS estimado da rede não é um MOS-LQO.

Fontes

1. ITU-T P.800: métodos de avaliação subjetiva e a escala MOS
2. ITU-T P.800.1: terminologia do MOS (LQS, LQO, LQE, CQS, CQO, CQE)
3. ITU-T G.107: o modelo E e o fator R
4. ITU-T G.114: tempo de transmissão num sentido
5. ITU-T P.863: POLQA, qualidade de escuta objetiva
6. ITU-T P.862: PESQ, retirada em 5 de janeiro de 2024
7. RFC 3550: RTP e RTCP, incluindo o cálculo do jitter entre chegadas

GUIA

SLA de telefonia: como calcular a disponibilidade no ano e no mês

O SLA de um tronco SIP ou de um 0800 é uma conta simples, mas cheia de detalhes que mudam o resultado: o tamanho do período, a manutenção programada, o que conta como queda e a resolução com que se mede. Este guia mostra a conta e cada um desses detalhes.

Por Equipe 2N5 Publicado em 7 de outubro de 2026 Atualizado em 7 de outubro de 2026

Resumo

- Disponibilidade = (período − manutenção − tempo fora do ar) ÷ (período − manutenção) × 100.
- 99,9% permite cerca de 8 h 46 min fora do ar em um ano de 365 dias, e cerca de 43 min em um mês de 30 dias.
- No Brasil, o SLA de telefonia costuma ser medido no ano; o mês serve de referência e de alerta.
- Uma queda só entra na conta se alguém mediu: quanto mais frequente o teste, mais exato o número.
- Ficar sem visibilidade do próprio monitoramento não é queda do circuito e deve ficar fora da conta.

Tempo fora do ar permitido por cada meta de disponibilidade

Período	99%	99,5%	99,9%	99,95%	99,99%
Ano de 365 dias	3 d 15 h 36 min	1 d 19 h 48 min	8 h 45 min 36 s	4 h 22 min 48 s	52 min 34 s
Ano bissexto (366 dias)	3 d 15 h 50 min	1 d 19 h 55 min	8 h 47 min 2 s	4 h 23 min 31 s	52 min 42 s
Mês de 31 dias	7 h 26 min 24 s	3 h 43 min 12 s	44 min 38 s	22 min 19 s	4 min 28 s
Mês de 30 dias	7 h 12 min	3 h 36 min	43 min 12 s	21 min 36 s	4 min 19 s
Fevereiro bissexto (29 dias)	6 h 57 min 36 s	3 h 28 min 48 s	41 min 46 s	20 min 53 s	4 min 11 s
Fevereiro (28 dias)	6 h 43 min 12 s	3 h 21 min 36 s	40 min 19 s	20 min 10 s	4 min 2 s
Semana	1 h 40 min 48 s	50 min 24 s	10 min 5 s	5 min 2 s	1 min
Dia	14 min 24 s	7 min 12 s	1 min 26 s	43 s	9 s

Como calcular o SLA de disponibilidade?

Divida o tempo em que o circuito funcionou pelo tempo em que ele deveria funcionar. Em fórmula: **disponibilidade = (período − manutenção programada − tempo fora do ar) ÷ (período − manutenção programada) × 100**. O período é contado em minutos, com o calendário de verdade: um ano tem 525.600 minutos (527.040 nos anos bissextos), e um mês tem de 40.320 a 44.640.

O caminho inverso responde à pergunta mais comum na negociação de um contrato: quanto tempo fora do ar uma meta permite. **Tempo permitido = (período − manutenção programada) × (100% − meta)**. Para 99,9% em um ano de 365 dias, são 525.600 × 0,001 = 525,6 minutos, ou 8 horas, 45 minutos e 36 segundos.

A calculadora e a tabela acima usam exatamente essa fórmula. A tabela vale sem manutenção programada; com manutenção, use a calculadora.

Quanto tempo fora do ar cabe em cada meta?

Os números que mais aparecem em contratos de telefonia, em um ano de 365 dias:

Meta	Por ano	Por mês de 30 dias
99%	3 d 15 h 36 min	7 h 12 min
99,5%	1 d 19 h 48 min	3 h 36 min
99,9%	8 h 45 min 36 s	43 min 12 s
99,95%	4 h 22 min 48 s	21 min 36 s
99,99%	52 min 34 s	4 min 19 s

Cada “9” a mais divide o tempo permitido por dez. A diferença entre 99,9% e 99,99% é a diferença entre uma tarde inteira fora do ar e menos de uma hora no ano. Antes de assinar uma meta alta, vale perguntar como ela será medida: uma meta que ninguém mede é só um número no contrato.

O que conta como tempo fora do ar?

Essa é a parte que o contrato precisa dizer, e muitas vezes não diz. Para um circuito de voz, as situações que costumam ser tratadas como indisponibilidade são:

- **a chamada não completa**: a operadora recusa com um código SIP de falha, como SIP 503 ou SIP 404, ou não responde;
- **a chamada completa sem áudio**, em um ou nos dois sentidos: para quem liga, um 0800 mudo está fora do ar;
- **a mensagem errada atende**: a URA trocada, ou a gravação da operadora dizendo que o número não existe;
- **a qualidade de voz cai abaixo do combinado**: alguns contratos tratam isso como indisponibilidade parcial, outros como uma meta separada.

E o que normalmente fica fora da conta:

- **manutenção programada**, avisada e dentro da janela combinada;
- **falhas causadas pelo próprio cliente**, como um PABX desligado na filial, quando o contrato é com a operadora e o defeito não está nela;
- **o tempo em que o monitoramento ficou sem visibilidade** por um problema dele mesmo. Um teste que não pôde ser feito não diz nada sobre o circuito, e não pode virar indisponibilidade.

Quem mede precisa separar essas situações, e o relatório precisa mostrá-las. No Monitor, um período em que o teste não pôde ser feito por um problema do lado da 2N5 sai da conta e aparece separado.

SLA anual ou mensal: qual vale?

O que o contrato disser. Na telefonia corporativa brasileira, é comum a meta de disponibilidade ser anual, e os números de cada mês servirem de referência. As duas medidas contam histórias diferentes:

	Meta anual	Meta mensal
O que tolera	Um mês ruim, se o ano fechar dentro da meta	Nenhum mês fora da meta
Tempo permitido em 99,9%	8 h 45 min 36 s no ano	43 min 12 s em cada mês de 30 dias
Quando a multa é calculada	No fechamento do ano	Todo mês
Para que o número mensal serve	Para agir antes que o ano estoure	É o próprio SLA

Um exemplo: um tronco fica 6 horas fora do ar em março e nada no resto do ano. Na meta mensal de 99,9%, março estourou (6 horas contra 44 minutos e 38 segundos permitidos em um mês de 31 dias). Na meta anual de 99,9%, o ano fechou em 99,932%, dentro da meta.

Por isso os relatórios do Monitor mostram os **últimos 12 meses** como o número que decide o SLA, e o mês e os últimos 30 dias para referência.

Como descontar a manutenção programada?

Tire a manutenção do período antes da conta, dos dois lados da fração. Um mês de 30 dias tem 43.200 minutos; com uma janela de manutenção de 4 horas (240 minutos), o período que conta passa a ter 42.960. Se o circuito ficou mais 30 minutos fora do ar fora da janela, a disponibilidade é (42.960 − 30) ÷ 42.960 = 99,930%.

Dois cuidados:

1. **A janela precisa estar registrada antes**, com início e fim. Uma “manutenção” declarada depois da queda é só uma queda.
2. **O que passa da janela é queda.** Se a manutenção marcada para terminar às 4h terminou às 5h30, a hora e meia extra entra no tempo fora do ar.

No Monitor, uma janela de manutenção cobre os circuitos escolhidos num horário marcado, e as falhas desses circuitos durante a janela não abrem incidente.

Como medir o tempo fora do ar de verdade?

Com um teste que veja o que o cliente vê, numa frequência compatível com a meta. Dois erros comuns tornam o número do SLA sem valor:

- **Medir o equipamento, não a chamada.** Um PABX ligado e um tronco registrado não provam que uma chamada completa com áudio. O tempo fora do ar só é real se o teste for uma chamada real.
- **Medir pouco.** Se o teste acontece a cada hora, uma queda de 40 minutos pode passar sem ser vista, e o SLA sai melhor do que foi. Para uma meta de 99,9% ao mês, que tolera 43 minutos, o intervalo entre testes precisa ser bem menor do que isso.

No ritmo padrão do Monitor, cada circuito recebe uma chamada de teste a cada 15 minutos. Quando uma falha, a chamada é repetida três vezes, a cada 2 minutos; quatro falhas seguidas abrem um incidente, e duas chamadas boas seguidas confirmam a volta. Assim, o início e o fim de cada queda ficam marcados com poucos minutos de margem, e uma oscilação isolada não entra no SLA.

O que pedir no contrato com a operadora?

Antes de aceitar uma meta, combine por escrito:

1. **o período de medição** (ano ou mês) e o fuso horário;
2. **o que conta como indisponibilidade**: só falta de completamento, ou também chamada muda e qualidade abaixo do limite;
3. **como a manutenção é avisada** e qual a janela máxima;
4. **quem mede, e como**: a medição da operadora, a sua, ou uma medição independente;
5. **qual evidência vale** para abrir uma contestação: horário, número chamado, código SIP e causa Q.850 de cada falha.

O último item é o que mais pesa na hora de cobrar. Uma queda registrada com o código SIP e a causa Q.850 de cada chamada de teste é difícil de contestar; uma queda percebida por um cliente que reclamou, não.

E o atendimento ao consumidor?

Para os SACs dos setores regulados, a disponibilidade não é só uma questão de contrato. O Decreto nº 11.034/2022, até 1º de novembro de 2026, exige que o acesso ao SAC fique disponível 24 horas por dia, 7 dias por semana, por pelo menos um canal, e torna obrigatório o atendimento por telefone; a partir de 2 de novembro de 2026, o Decreto nº 13.135/2026 mantém o telefone obrigatório e exige ao menos um canal eletrônico 24 horas. Para as prestadoras de telecomunicações, o Regulamento Geral de Direitos do Consumidor da Anatel (Resolução nº 765/2023) pede o atendimento telefônico disponível 24 horas. Medir a disponibilidade do 0800 é a forma de mostrar que essas regras foram cumpridas.

Perguntas frequentes

Qual a fórmula do SLA de disponibilidade?

Disponibilidade é o tempo em que o serviço funcionou dividido pelo tempo em que ele deveria funcionar, em porcentagem: (período − manutenção − tempo fora do ar) ÷ (período − manutenção) × 100. Um tronco que ficou 60 minutos fora do ar em um mês de 30 dias, sem manutenção, teve 99,861% de disponibilidade.

99,9% de disponibilidade é quanto tempo fora do ar?

Em um ano de 365 dias, 8 horas, 45 minutos e 36 segundos. Em um mês de 30 dias, 43 minutos e 12 segundos. Em uma semana, 10 minutos e 5 segundos. Em um dia, 1 minuto e 26 segundos.

SLA anual ou mensal: qual é melhor?

Depende do contrato. A meta anual tolera um mês ruim desde que o ano feche dentro dela; a mensal pune cada mês ruim. Na telefonia corporativa brasileira é comum a meta ser anual, com o mês acompanhado para referência e para agir antes que o ano estoure.

Manutenção programada conta como tempo fora do ar?

Normalmente não, se ela foi avisada com a antecedência que o contrato pede e ficou dentro da janela combinada. Ela sai do período antes da conta. Uma manutenção que passou da janela conta como queda a partir do momento em que a janela terminou.

Como medir o tempo fora do ar de um 0800?

Ligando para ele em intervalos curtos e registrando quando as chamadas param e voltam a completar. A precisão depende do intervalo: com uma chamada a cada 15 minutos e novas tentativas a cada 2 minutos depois de uma falha, o início e o fim da queda ficam marcados com poucos minutos de margem.

Fontes

1. ITU-T E.800: definições de termos de qualidade de serviço, incluindo disponibilidade
2. Decreto nº 11.034/2022, art. 4º: acesso ao SAC 24 horas por dia, 7 dias por semana (vale até 1º de novembro de 2026)
3. Decreto nº 13.135/2026, arts. 12 e 14: canal eletrônico 24 horas e telefone obrigatório (vale a partir de 2 de novembro de 2026)
4. Anatel, Resolução nº 765/2023 (RGC), art. 15: atendimento telefônico disponível 24 horas

Termos e privacidade

Versão 1, em vigor desde 2026-10-06 Versão 1 Versão 2 Versão 3

Termos de Uso

O Voice Circuits é um serviço da **2N5 Global Enabler**. Esta página tem duas partes:

1. Os **Termos de Uso da 2N5 Global Enabler**, que valem para todos os serviços da 2N5.
2. **Voice Circuits**, as condições próprias deste serviço.

A Parte 2 complementa a Parte 1. Onde as duas divergirem, a Parte 2 vale para o Voice Circuits. Um contrato ou proposta comercial assinado entre a 2N5 e o Cliente prevalece sobre ambas.

Parte 1 — Termos de Uso da 2N5 Global Enabler (LGPD – Brasil)

Válido para operações no Brasil – legislação aplicável: LGPD (Lei 13.709/2018), Marco Civil da Internet e Regulamentações da Anatel.

Bem-vindo à 2N5 Global Enabler ("2N5", "nós", "nosso"). Estes Termos de Uso regulam a utilização de nossos serviços e plataformas, incluindo soluções de telecomunicações (STFC/VoIP), Cloud PBX, IVR, Integrações Omnichannel, APIs e Inteligência Artificial.

Ao utilizar nossos serviços, o Usuário declara ter lido, compreendido e concordado integralmente com estes Termos, assim como com nossa Política de Privacidade, que integra este documento.

1. Definições (LGPD)

Para fins destes Termos:

- **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **Dado Sensível:** categorias especiais previstas no art. 5º, II, da LGPD.
- **Controlador:** pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais. (O Cliente é o Controlador.)
- **Operador:** pessoa que realiza o tratamento de dados pessoais em nome do Controlador. (A 2N5 atua como Operadora.)
- **Encarregado (DPO):** pessoa indicada para atuar como canal de comunicação entre Controlador, Titulares e ANPD.
- **Usuário:** qualquer pessoa física ou jurídica que utiliza os serviços da 2N5.
- **Cliente:** Usuário contratante de plano ou serviço.
- **Plataforma:** ambiente web, APIs, aplicativos e sistemas digitais da 2N5.

2. Aceite e Vigência

O uso dos serviços implica aceitação plena e irrestrita destes Termos. O contrato passa a vigorar no primeiro acesso, cadastro ou assinatura.

3. Elegibilidade

Somente podem utilizar os serviços:

- empresas devidamente registradas;

- pessoas físicas maiores de 18 anos e plenamente capazes;
- representantes legais autorizados.

4. Serviços Prestados

A 2N5 oferece:

4.1. Serviços de Telecom (STFC/VoIP)

Conforme regulamentação da Anatel, incluindo:

- Números telefônicos (DID), portabilidade e interconexão;
- Tráfego inbound e outbound;
- Anti-fraude;
- Tarifa por minuto, assinatura ou franquia.

4.2. Cloud PBX

- Ramais, URA, filas de atendimento;
- gravação de chamadas conforme legislação (responsabilidade do Cliente obter consentimento);
- relatórios e dashboards.

4.3. IVR / URA Inteligente

- fluxos avançados;
- roteamento dinâmico;
- coleta de DTMF/voz.

4.4. Serviços de Inteligência Artificial

- agentes virtuais;
- transcrição, análise semântica, classificação;
- automação de atendimento;
- ferramentas de produtividade com linguagem natural.

4.5. APIs e Integrações Omnichannel

- telefonia, SMS, WhatsApp (quando autorizado), e-mail, webhooks;
- integrações nativas ou customizadas.

5. Responsabilidades do Usuário

O Usuário concorda em:

1. Cumprir a legislação brasileira, incluindo Anatel, LGPD e Marco Civil da Internet.
2. Não realizar spam, abuso, chamadas fraudulentas ou ilegais.
3. Manter dados cadastrais verdadeiros e atualizados.
4. Proteger senhas, tokens de API e credenciais.
5. Obter consentimento de seus clientes para gravação de chamadas, uso de IA, coleta de dados e qualquer finalidade exigida pela LGPD.
6. Responder integralmente por dados inseridos na plataforma.

6. Condições Específicas — Telecom, Cloud PBX, IVR e IA

6.1. Uso de Telecom

É proibido:

- mascaramento ilícito de Caller ID;
- tentativas de fraude, robochamada abusiva, spam e telemarketing ilegal;
- uso para fins criminosos ou contrários às normas da Anatel.

A 2N5 poderá suspender imediatamente o serviço em caso de abuso.

6.2. Gravação de Chamadas

- A funcionalidade é opcional.
- O Cliente é exclusivamente responsável por informar e obter consentimento do Titular.
- A 2N5 apenas armazena e processa conforme instruções do Controlador.

6.3. Inteligência Artificial

O Usuário reconhece que:

- A IA opera por modelos estatísticos e pode conter imprecisões;
- A responsabilidade pelas decisões tomadas com base em resultados de IA é exclusivamente do Cliente;
- O Cliente deve dispor de bases legais adequadas para tratar dados pessoais via IA (Legítimo Interesse, Consentimento, Execução de Contrato, etc.);
- A 2N5 não se responsabiliza por vieses, interpretações equivocadas ou erros derivados do uso inadequado da IA.

6.4. WhatsApp e Mensageria

- Sujeito às políticas Meta/WhatsApp;
- Contas irregulares podem ser bloqueadas sem reembolso;
- A 2N5 não controla regras da Meta e é apenas integradora.

6.5. Segurança e Logs

A 2N5 mantém logs pelo prazo legal:

- 6 meses conforme Marco Civil da Internet (art. 15);
- prazos adicionais mediante ordem judicial.

7. Proteção de Dados (LGPD)

7.1. Papéis de Tratamento

- Cliente = Controlador
- 2N5 = Operadora de Dados

7.2. Tratamento de Dados pela 2N5

A 2N5 realiza tratamento apenas conforme:

- instruções do Cliente;

- contrato;
- legislação vigente.

7.3. Medidas de Segurança

A 2N5 adota:

- criptografia;
- controle de acesso;
- segregação lógica;
- backups;
- políticas internas de segurança;
- data centers certificados (ISO, SOC, etc.).

7.4. Armazenamento e Retenção

Dados são retidos pelo período necessário à finalidade, compliance regulatório e execução contratual.

7.5. Compartilhamento

Dados podem ser compartilhados com:

- operadoras de telefonia;
- provedores tecnológicos;
- autoridades mediante ordem legal.

8. Pagamentos, Cobrança e Créditos

- Planos pós-pagos, pré-pagos ou híbridos;
- Créditos não são reembolsáveis;
- Inadimplência pode gerar suspensão imediata;
- Chamadas excedentes e serviços adicionais são cobrados por uso.

9. Propriedade Intelectual

Todo código, infraestrutura, marcas e conteúdos são de propriedade exclusiva da 2N5. É proibido copiar, redistribuir, fazer engenharia reversa ou reproduzir partes dos sistemas.

10. Limitação de Responsabilidade

Até o limite permitido pela lei, a 2N5 não se responsabiliza por:

- perdas de lucro, faturamento ou dados;
- danos indiretos;
- indisponibilidade causada por terceiros (operadoras, provedores, Meta, etc.);
- mau uso dos serviços;
- decisões tomadas por IA.

A responsabilidade total da 2N5 é limitada ao valor pago pelo Cliente nos últimos 90 dias.

11. Suspensão e Encerramento

O serviço pode ser suspenso por:

- descumprimento destes Termos;
- uso abusivo;
- fraude;
- inadimplência;
- ordem judicial.

O Cliente pode encerrar a conta a qualquer momento. Valores pagos não são reembolsáveis.

12. Suporte Técnico

Oferecido via tickets, e-mail ou painel administrativo. Planos com SLA podem ser contratados à parte.

13. Alterações destes Termos

A 2N5 pode atualizar este documento a qualquer momento. O uso contínuo implica concordância automática.

14. Contato do Encarregado / DPO

Para exercer seus direitos, esclarecer dúvidas ou solicitar informações adicionais, contate:

- **Encarregado / Data Protection Officer (DPO)**, 2N5 Global Enabler
- **E-mail:** privacidade@2n5.com.br
- **Telefone:** +55 (11) 2050-1096
- **Website:** www.2n5.com.br

Parte 2 — Voice Circuits

1. Aceite

O Cliente aceita estes Termos ao assinar o contrato ou a proposta. Cada Usuário os aceita, junto com a Política de Privacidade, no primeiro acesso, e a 2N5 registra a versão aceita e quando. Os Usuários agem em nome do Cliente.

2. O serviço

O Voice Circuits é um **serviço gerenciado de monitoramento**. Conforme o que o Cliente contratar, ele:

- **faz chamadas de teste** para os números de telefone do Cliente e avalia se cada linha completa a chamada e transmite áudio com qualidade aceitável;
- **mede os circuitos de dados do Cliente**, por um agente instalado no local do Cliente ou por verificações feitas de fora;
- **verifica os sites e a entrega de e-mails do Cliente**;
- **avisa as pessoas que o Cliente escolher**, em etapas, quando uma falha é confirmada, e informa quando ela é resolvida;
- **produz relatórios de serviço**, incluindo índices de disponibilidade.

A 2N5 configura o monitoramento a partir das informações fornecidas pelo Cliente. Os Usuários do Cliente também podem vê-lo e, quando permitido, alterá-lo.

O serviço **mede e informa**. Ele não conserta linhas, redes de operadoras nem sites, e não é um serviço de emergência. Um teste pode deixar de detectar um problema, ou apontar um que um teste seguinte não confirme. As decisões que o Cliente tomar com base em um resultado são do Cliente.

3. Limites do plano

O plano do Cliente limita a quantidade de circuitos de voz, circuitos de dados, sites e verificações de e-mail, e o número de chamadas de teste por hora. Ao atingir um limite, não é possível adicionar mais itens daquele tipo até que a 2N5 o aumente. O monitoramento do que já existe continua.

4. Chamadas de teste

1. O Cliente só pode pedir à 2N5 que chame números que tenha **o direito de mandar chamar**, como suas próprias linhas ou linhas que administra com a concordância do titular.
2. Uma chamada de teste que pode ser atendida por uma pessoa toca antes uma mensagem gravada avisando que se trata de um teste automático.
3. **Vozes nunca são guardadas.** O áudio só é guardado quando a chamada é atendida pela gravação ou pelo menu automático (URA) que o Cliente informou à 2N5, e apenas para provar a linha e medir sua qualidade. O áudio de uma chamada atendida por qualquer outra pessoa ou coisa é destruído ao fim da chamada.
4. O Cliente avisa a 2N5 quando um número deixar de ser seu e planeja janelas de manutenção para trabalhos planejados, para que os alertas e os índices permaneçam corretos.
5. A 2N5 pode reduzir ou interromper chamadas de teste que possam prejudicar uma operadora ou terceiros, ou que violem as normas de telecomunicações.

5. O agente de monitoramento

A 2N5 instala o agente de circuitos de dados somente em um computador escolhido pelo Cliente, e **somente com autorização escrita do Cliente**. O agente envia medições de rede e informações básicas sobre o computador, conforme a Política de Privacidade. Ele não abre portas e não lê arquivos nem tráfego. O Cliente pode pedir à 2N5 que o remova a qualquer momento.

6. Responsabilidades do Cliente

Além da Parte 1, seção 5, o Cliente deve:

1. informar sua equipe e seus demais contatos de que os dados deles são usados para enviar alertas e relatórios;
2. ser titular, ou ter o direito de uso, das gravações que fornecer para comparação;
3. avisar a 2N5 imediatamente sobre qualquer acesso não autorizado às suas contas.

7. Dados pessoais

1. **Papéis.** Para os dados de monitoramento que o Cliente fornece ou que o serviço gera para ele, o Cliente é o controlador e a 2N5 a operadora, como diz a Parte 1, seção 7. Para pedidos de demonstração, contas de acesso e registros de acesso e de segurança, a 2N5 é a controladora.
2. **Como operadora, a 2N5:**
    - usa somente os tipos de prestadores listados na Política de Privacidade e avisa o Cliente antes de incluir um novo tipo;
    - ajuda o Cliente a responder às solicitações dos titulares e da ANPD;

  - avisa o Cliente **sem demora indevida, e em no máximo 48 horas**, sobre qualquer incidente de segurança que afete os dados do Cliente;
  - só transfere dados para fora do Brasil por mecanismo admitido pelo art. 33 da LGPD.

8. Disponibilidade

A 2N5 busca manter o serviço sempre disponível, mas não o garante. Manutenções programadas são avisadas com antecedência sempre que possível. Compromissos de disponibilidade ou créditos de serviço só valem se estiverem no contrato.

9. Os dados do Cliente

O Cliente mantém todos os direitos sobre seus dados e gravações e autoriza a 2N5 a usá-los somente para prestar o serviço. Após o fim do contrato:

- o Cliente pode pedir a exportação dos seus relatórios e resultados em até **30 dias**;
- depois disso, a 2N5 elimina os dados do Cliente em até **90 dias**, incluindo as cópias de segurança à medida que expirarem;
- a 2N5 guarda somente o que a lei exigir, como os registros de acesso por 6 meses.

10. Alterações

A 2N5 publica qualquer alteração destes Termos com a data e avisa o Cliente e os Usuários com pelo menos **30 dias** de antecedência. O Cliente que não aceitar uma alteração relevante pode encerrar o contrato antes que ela entre em vigor.

Versão 1, em vigor desde 2026-10-06 Versão 1 Versão 2 Versão 3 Versão 4

Política de Privacidade

O Voice Circuits é um serviço da **2N5 Global Enabler**. Esta página tem duas partes:

1. A **Política de Privacidade da 2N5 Global Enabler**, que vale para todos os serviços da 2N5.
2. **Voice Circuits**, que diz exatamente o que este serviço coleta, por quê e por quanto tempo.

A Parte 2 complementa a Parte 1. Onde as duas divergirem, a Parte 2 vale para o Voice Circuits.

Parte 1 — Política de Privacidade da 2N5 Global Enabler (LGPD, GDPR, PIPEDA e CCPA/CPRA)

1. Introdução

A 2N5 Global Enabler está comprometida com a proteção de dados pessoais e com a transparência no tratamento das informações. Esta Política de Privacidade estabelece como coletamos, utilizamos, compartilhamos, armazenamos e protegemos dados pessoais, em conformidade com:

- Lei Geral de Proteção de Dados – LGPD (Brasil)
- General Data Protection Regulation – GDPR (União Europeia)
- Personal Information Protection and Electronic Documents Act – PIPEDA (Canadá)
- California Consumer Privacy Act / California Privacy Rights Act – CCPA/CPRA (EUA – Califórnia)

Ao acessar nossos serviços, o titular declara ter lido, compreendido e concordado com esta Política.

2. Definições Importantes

Para fins desta Política:

- **Dado Pessoal:** qualquer informação relacionada a pessoa natural identificada ou identificável.
- **Dado Pessoal Sensível:** origem racial, convicção religiosa, saúde, biometria, etc.
- **Titular:** pessoa a quem os dados se referem.
- **Controlador:** quem decide sobre o tratamento (2N5 Global Enabler).
- **Operador/Processor:** quem realiza o tratamento em nome do controlador.
- **Encarregado/DPO:** responsável pelo canal de comunicação com titulares e autoridades.
- **Consentimento:** manifestação livre, informada e inequívoca do titular.

3. Dados Pessoais Coletados

3.1. Informações fornecidas diretamente pelo titular

- Nome, sobrenome
- E-mail, telefone, WhatsApp
- Empresa, cargo e informações comerciais
- Dados inseridos em formulários, chat ou e-mail
- Registros de suporte e atendimento

3.2. Informações coletadas automaticamente

- Endereço IP (anonimizado quando possível)
- Dados de navegação, geolocalização aproximada e identificadores online

- Cookies, tags e pixels de rastreamento
- Dados de dispositivo e sistema utilizado
- Registros de logs, uso do site e comportamento de acesso

3.3. Informações de terceiros

Podemos receber informações de:

- Plataformas de análise (Google Analytics, Meta, LinkedIn)
- Ferramentas de marketing e CRM
- Parceiros comerciais e plataformas integradas

4. Bases Legais para o Tratamento

A 2N5 Global Enabler realiza o tratamento com base em fundamentos legais, incluindo:

4.1. LGPD – Bases

- Consentimento
- Execução de contrato
- Legítimo interesse
- Cumprimento de obrigação legal/regulatória
- Exercício regular de direitos

4.2. GDPR – Bases

- Consent
- Contractual necessity
- Legitimate interests (quando não sobrepuser direitos do titular)
- Legal obligation
- Protection of vital interests (situações excepcionais)

4.3. PIPEDA – Princípios

- Consentimento informado
- Limitação de coleta e retenção
- Responsabilidade e transparência
- Salvaguardas apropriadas

4.4. CCPA/CPRA – Direitos e Obrigações

- Transparência
- Opt-out para venda/compartilhamento de dados
- Limitação de uso de dados sensíveis
- Proibição de discriminação contra titulares que exercem seus direitos

5. Finalidades do Tratamento

Tratamos dados pessoais para:

- Prestação e melhoria de serviços
- Atendimento ao cliente e suporte técnico

- Gestão de contas, integrações e comunicações
- Execução de contratos e obrigações comerciais
- Análises, métricas e inteligência operacional
- Marketing autorizado, remarketing e campanhas publicitárias
- Prevenção a fraudes, incidentes e atividades suspeitas
- Cumprimento de obrigações legais, fiscais e regulatórias
- Segurança, auditoria e controle interno

Não utilizamos dados pessoais para decisões exclusivamente automatizadas que produzam efeitos jurídicos significativos sem intervenção humana, exceto quando permitido pela legislação.

6. Compartilhamento e Transferência Internacional

Dados podem ser compartilhados com:

- Prestadores de serviço (hospedagem, analytics, cloud computing, automação, telefonia, CRM)
- Empresas do grupo 2N5
- Parceiros comerciais sob contrato de confidencialidade
- Autoridades governamentais, quando legalmente requerido

Transferência Internacional

Dados podem ser armazenados ou processados em servidores no Brasil, Canadá, EUA, Europa ou outros países. Garantimos mecanismos adequados, tais como:

- Standard Contractual Clauses – SCC (UE)
- Cláusulas contratuais específicas
- Política de privacidade compatível com GDPR, LGPD, PIPEDA e CCPA
- Acordos de processamento de dados – DPA

7. Retenção e Eliminação de Dados

Mantemos os dados apenas pelo período necessário para:

- Cumprimento das finalidades desta Política
- Obrigações legais e regulatórias
- Defesa em processos judiciais ou administrativos

Após o prazo, os dados são eliminados ou anonimizados conforme padrões técnicos seguros.

8. Direitos dos Titulares

8.1. Direitos previstos na LGPD

- Confirmação de tratamento
- Acesso
- Correção de dados incompletos
- Anonimização, bloqueio ou eliminação
- Portabilidade
- Informação sobre compartilhamento

- Revogação de consentimento
- Oposição ao tratamento

8.2. Direitos previstos no GDPR

- Access
- Rectification
- Erasure (“right to be forgotten”)
- Restriction of processing
- Data portability
- Objection
- Not to be subject to automated decisions

8.3. Direitos PIPEDA

- Acesso
- Correção
- Revogação de consentimento
- Transparência

8.4. Direitos CCPA/CPRA

- Right to know
- Right to delete
- Right to correct
- Right to opt-out of sale/sharing
- Right to limit sensitive data use
- Non-discrimination

O exercício dos direitos pode ser solicitado diretamente ao DPO/Encarregado.

9. Medidas de Segurança

Utilizamos medidas técnicas, administrativas e organizacionais compatíveis com padrões internacionais:

- Criptografia em repouso e em trânsito
- Controles de acesso e autenticação multifator
- Firewalls, IDS/IPS e monitoramento 24/7
- Data Loss Prevention (DLP)
- Segmentação de rede
- Backup seguro e redundância
- Políticas internas e auditorias periódicas
- Treinamento de colaboradores

10. Cookies

Utilizamos cookies essenciais, analíticos, funcionais e de marketing. Para mais informações, consulte nossa Política de Cookies.

11. Atualizações

Esta Política pode ser atualizada periodicamente. A versão mais recente estará sempre disponível no site.

12. Contato do Encarregado / DPO

Para exercer seus direitos, esclarecer dúvidas ou solicitar informações adicionais, contate:

- **Encarregado / Data Protection Officer (DPO)**, 2N5 Global Enabler
- **E-mail:** privacidade@2n5.com.br
- **Telefone:** +55 (11) 2050-1096
- **Website:** www.2n5global.com

Parte 2 — Voice Circuits

O Voice Circuits monitora os circuitos de voz, os circuitos de dados e os serviços online de uma empresa e avisa as pessoas certas quando algum falha. Ele é vendido a **empresas** como serviço gerenciado, e a 2N5 configura o monitoramento de cada cliente a partir das informações que o cliente fornece.

1. Quem decide como os dados são usados

Dados	Controlador	Papel da 2N5
Pedidos de demonstração do nosso site, contas usadas para entrar no sistema, registros de acesso e de segurança	2N5	Controladora
Dados de monitoramento que um cliente nos fornece ou que o serviço gera para ele: contatos de alertas e relatórios, números chamados, gravações, resultados e relatórios	A empresa cliente	**Operadora**: usamos esses dados somente conforme as instruções do cliente

Se seus dados foram fornecidos pelo seu empregador ou por outra empresa, por exemplo como contato de alertas, essa empresa é a controladora. Nós a ajudaremos a atender sua solicitação.

2. O que coletamos, por quê e por quanto tempo

2.1. Agendamento de demonstração no nosso site

- **O quê:** seu nome, e-mail profissional, empresa (opcional), idioma, o que deseja monitorar e o tamanho aproximado.
- **O que não coletamos:** não guardamos seu endereço IP, dados do navegador nem qualquer identificador de rastreamento. Seu IP fica em memória por poucos minutos, apenas para impedir abuso do formulário.
- **Por quê:** para responder a você e agendar a demonstração.
- **Base legal:** procedimentos preliminares a contrato, a seu pedido (art. 7º, V, da LGPD).
- **Por quanto tempo:** 12 meses após nosso último contato com você, a menos que você se torne cliente. Você pode pedir a exclusão antes disso.

2.2. Sua conta de acesso

- **O quê:** seu nome, e-mail e idioma; sua senha, guardada somente como hash irreversível e nunca em forma legível; as partes da sua organização que você pode ver; quando você entrou pela última vez.

- **Por quê:** para permitir seu acesso, mostrar o monitoramento da sua organização e manter a conta segura.
- **Base legal:** execução do contrato com a sua organização (art. 7º, V) e nosso legítimo interesse em manter o serviço seguro (art. 7º, IX).
- **Por quanto tempo:** enquanto você tiver acesso. A conta é excluída junto com a sua organização ou a seu pedido.

2.3. Contatos que recebem alertas e relatórios

- **O quê:** nome, cargo, e-mail profissional, números de telefone e de WhatsApp, idioma e os horários em que você não quer receber ligações. Também guardamos as mensagens que enviamos a você e se foram entregues ou reconhecidas.
- **Por quê:** para avisar as pessoas certas quando uma linha ou serviço falha e para enviar os relatórios que a sua organização pediu.
- **Base legal:** instruções do cliente, como controlador (art. 39).
- **Por quanto tempo:** enquanto a sua organização mantiver você como contato. As mensagens já enviadas são guardadas por 13 meses, para que os relatórios anuais mostrem quem foi avisado e quando.

2.4. Chamadas de teste

- **O que guardamos:** o número chamado, o registro técnico da chamada (sinalização, tempos e códigos de resultado), o veredito e a qualidade medida.
- **Antes que uma pessoa possa ouvir:** uma chamada que pode ser atendida por uma pessoa toca antes uma mensagem gravada avisando que se trata de um teste automático.
- **Nunca guardamos a voz de uma pessoa que atende.** O áudio só é guardado quando a chamada é atendida pela gravação ou pelo menu automático (URA) que o cliente nos informou, e apenas para provar que a linha funciona e medir sua qualidade. Se qualquer outra coisa atender, inclusive uma pessoa, o áudio é destruído ao fim da chamada e só o resultado é guardado.
- **Áudio guardado:** fica criptografado e é excluído após 90 dias, ou no prazo menor que o cliente definir.
- **Base legal:** instruções do cliente, como controlador (art. 39).
- **Por quanto tempo:** registros técnicos das chamadas, 90 dias; vereditos e índices de qualidade, durante o contrato, para que os relatórios e os índices anuais fiquem completos.

2.5. Agente de monitoramento de circuitos de dados

A pedido escrito do cliente, a 2N5 instala um pequeno agente em um computador no local do cliente.

- **O que ele envia:** o nome do computador, o sistema operacional e a versão do agente; o IP local do computador, o endereço do roteador e o IP público de onde vêm as medições; medições de rede como latência, perda, jitter, tempo de DNS e velocidade; uso de processador e de memória.
- **O que ele nunca coleta:** arquivos, navegação, conteúdo do tráfego, nomes de usuários, programas, nomes de redes Wi-Fi ou outros aparelhos da rede.
- **Base legal:** instruções do cliente (art. 39).
- **Por quanto tempo:** 13 meses.

2.6. Verificação de sites e de e-mail

- A **verificação de sites** acessa somente endereços públicos informados pelo cliente.

- A **verificação de e-mail** envia uma mensagem de teste por hora para uma caixa de teste criada pelo cliente para esse fim. Ela lê somente os cabeçalhos da nossa própria mensagem de teste, para saber se e onde chegou, e depois a exclui. Nenhuma outra mensagem dessa caixa é lida.
- **Base legal:** instruções do cliente (art. 39).
- **Por quanto tempo:** resultados durante o contrato.

2.7. Registros de acesso e de segurança

- **O quê:** para cada requisição, o endereço IP, a data e hora e o que foi pedido; para cada tentativa de acesso, se teve sucesso; um registro das alterações feitas no serviço: quem fez o quê, e quando.
- **Base legal:** cumprimento de obrigação legal pelo art. 15 do Marco Civil da Internet (art. 7º, II) e legítimo interesse em segurança (art. 7º, IX).
- **Por quanto tempo:** registros de acesso, 6 meses, ou mais somente por ordem de autoridade ou do Judiciário; registro de alterações, durante o contrato.

3. Cookies e armazenamento no seu navegador

Os cookies analíticos, funcionais e de marketing da Parte 1 **não são usados** no Voice Circuits. Ele não tem ferramentas de análise, publicidade, pixels de rastreamento nem cookies de terceiros, e não carrega nada de outros sites, por isso não pede que você aceite cookies. Ele guarda somente o necessário para funcionar:

Cookies e armazenamento no navegador

Nome	Tipo	Finalidade	Duração	Atributos
`vcia_session`	cookie	Mantém você conectado	Até você sair ou expirar	HttpOnly, Secure, SameSite=Lax
`vcia.language`	cookie + armazenamento local	Lembra inglês ou português	1 ano	Secure, SameSite=Lax
`vcia.signed-in`	armazenamento local	Mostra Abrir o app na página inicial	Até você sair	—
`vcia.sidebar`	armazenamento local	Lembra se a barra lateral está aberta	Até ser apagado	—
`vcia.theme`	armazenamento local	Lembra o tema claro, escuro ou o do seu computador	Até ser apagado	—
`vcia.staleBuildReloadAt`	armazenamento da sessão	Evita recarregar sem parar após uma atualização	Até fechar a aba	—
`vcia.toast`	armazenamento da sessão	Leva uma confirmação para a próxima página	Um carregamento de página	—
`vcia.mailbox-link`	armazenamento da sessão	Guarda o link de conexão de uma caixa de teste durante o acesso	Até fechar a aba	—

Você pode apagá-los nas configurações do navegador. Sem o `vcia_session` não é possível permanecer conectado.

4. Com quem compartilhamos dados

Não vendemos dados pessoais e não os usamos para publicidade. Compartilhamos somente com:

- **Prestadores que operam o Voice Circuits para nós:** hospedagem e infraestrutura em nuvem, envio de e-mails, alertas por SMS e por chamada de voz, e as operadoras de telefonia que cursam as chamadas de teste. Cada um está obrigado por contrato a usar os dados somente para essa finalidade e a protegê-los.
- **O provedor de e-mail do próprio cliente**, quando o cliente conecta uma caixa de e-mail para enviar mensagens ou fazer a verificação de e-mail.
- **A empresa cliente** a quem os dados de monitoramento pertencem.
- **Autoridades públicas**, quando a lei ou uma ordem judicial exigir.

Alguns desses prestadores armazenam ou tratam dados fora do Brasil, inclusive nos Estados Unidos. Fazemos essas transferências conforme o art. 33 da LGPD, usando as **cláusulas-padrão contratuais aprovadas pela ANPD** ou outro mecanismo que a ANPD admita.

5. Como protegemos os dados

- Todo o tráfego com o serviço é criptografado, e os navegadores são instruídos a usar criptografia sempre.
- O áudio das chamadas, as gravações, as senhas guardadas de serviços conectados e as chaves de assinatura são criptografados individualmente no banco de dados. A chave que os criptografa nunca fica no disco do servidor.
- Os dados de cada organização ficam separados, e um gestor vê somente as partes da organização que lhe foram atribuídas.
- Os administradores da 2N5 entram com verificação em duas etapas. Todo gestor pode ativá-la, e uma organização pode exigi-la de todos os seus gestores.
- Tentativas de acesso com erro repetido pausam o acesso daquele endereço, e o titular é avisado por e-mail. A troca de senha encerra todas as outras sessões.
- O acesso administrativo aos servidores só é possível por uma rede privada. As cópias de segurança diárias são guardadas por 14 dias.

Se um incidente de segurança puder acarretar risco ou dano relevante, comunicaremos a ANPD e os titulares afetados em até 3 dias úteis após sabermos que dados pessoais foram afetados. Para dados que tratamos para um cliente, avisaremos esse cliente sem demora.

6. Decisões automatizadas

O Voice Circuits decide automaticamente se uma **linha, link, site ou caixa de e-mail** está funcionando. Ele não toma decisões automatizadas sobre pessoas. Ainda assim, você pode pedir a revisão de uma decisão tomada unicamente com base em tratamento automatizado (art. 20 da LGPD).

7. Crianças e adolescentes

O Voice Circuits é um serviço para empresas. Ele não se destina a menores de 18 anos, e não coletamos intencionalmente dados deles.

8. Seus direitos

Você tem os direitos da Parte 1, seção 8. Como exercê-los no Voice Circuits, e em quanto tempo respondemos, está na nossa página LGPD. Você também pode reclamar à **Autoridade Nacional de Proteção de Dados (ANPD)** em gov.br/anpd.

9. Alterações

Quando esta página mudar de forma relevante, publicaremos a nova versão aqui com a data e avisaremos os usuários conectados com pelo menos 30 dias de antecedência. As versões anteriores continuam disponíveis no próprio endereço.

10. Contato

Escreva ao **Encarregado / DPO** da 2N5 Global Enabler, **Cláudio Longo Dacome Jr**, em **privacidade@2n5.com.br** ou ligue para **+55 (11) 2050-1096**.