intelbras

Guia de configuração

Integração GW 521 usando Webhook

intelbras

Integração GW 521 usando Webhook
Especificações e configurações com integradores usando Webhook

Parabéns, você acaba de adquirir um produto com a qualidade e segurança Intelbras.

Sistemas de portaria remota realizam atividade de controle de acesso e de monitoramento de eventos de dispositivos cadastrados. O GW 521 possibilita que eventos gerados pela Central de Incêndio da Intelbras sejam enviados para integradores e sistemas de portaria remota.

Esse guia tem como objetivo orientá-lo nas configurações necessárias para que o GW 521 consiga enviar eventos utilizando Webhooks.

Cuidados e segurança

- Leia todas as instruções do guia antes de configurar e utilizar o produto.
- Esse produto se comunica exclusivamente com as centrais de alarme de incêndio da linha CIE modelos 1125, 1250 e 2500 e não opera independentemente.
- LGPD - Lei Geral de Proteção de Dados Pessoais: LGPD - Lei Geral de Proteção de Dados Pessoais: a Intelbras não acessa, transfere, capta, nem realiza qualquer outro tipo de tratamento de dados pessoais a partir deste produto.
- LGPD - Segurança do produto no tratamento de dados: esse produto possui criptografia nas transmissões de dados, quando habilitado.

Índice

1. Características 5

2. Conexão 5

2.1. Conexão com a CIE 1125/1250/2500. 5

2.2. Conexão com o sistema integrador. 5

3. Webhook 6

4. Configuração 6

4.1. Configuração do GW 521 e o Sistema Integrador 6

4.2. Configuração no GW 521. 6

5. Autenticação HMAC ou HTTPS 7

5.1. HMAC 7

5.2. HTTPS (SSL/TLS) 8

6. Funcionamento 9

7. Orientações e solução de problemas 9

8. Indicações de problemas do LED Status 10

Termo de garantia 11

1. Características

Protocolo IP	Somente IPV4
Meio de transmissão	Ethernet
Protocolo de Comunicação	HTTP / HTTPS
Porta de comunicação	80/8080 ou outro para HTTP
	443/8433 ou outra para HTTPS
Tipo de autenticação	HMAC ou SSL/TLS

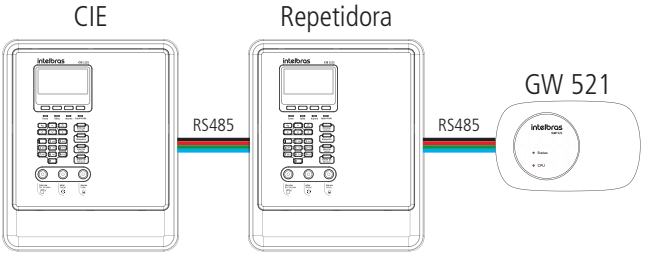
2. Conexão

2.1. Conexão com a CIE 1125/1250/2500

O GW 521 comunica-se com a central CIE pelo conector das repetidoras presente na placa display da central. A comunicação acontece via RS485 e a conexão segue o mesmo padrão utilizado para as repetidoras.

Para mais informações consulte o Manual do Usuário GW 521 e o Manual do Usuário CIE 1125/1250/2500.

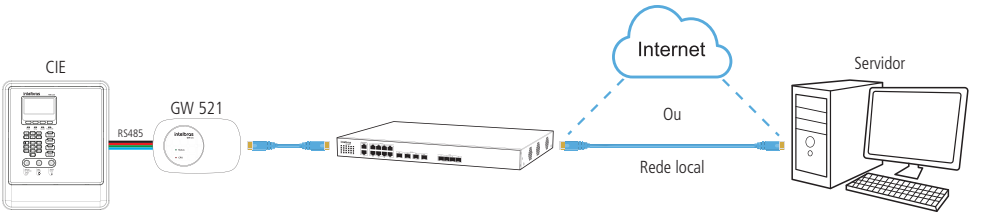
Conexões na placa display CIE	Conexão no GW 521
D+	D+
D-	D-
24V	24V
GND	GND



A comunicação entre a CIE e o GW 521 deve ser habilitada na central através do ProgramadorCIE ou manualmente no *Menu > Configurações > Endereços Repetidoras > GW 521 (Ativo).*

2.2. Conexão com o sistema integrador

A comunicação entre o GW 521 e o sistema integrador pode acontecer na rede local interna ou externamente na internet, a depender do tipo do sistema.

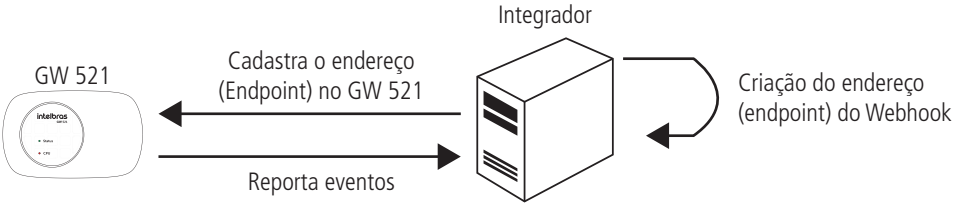


3. Webhook

Webhook é um endereço HTTP que o sistema integrador deve criar para receber os eventos reportados pelo GW 521 em tempo real.

O GW 521 atua como um *Webhook Sender*, ou seja, trabalha enviando dados para o servidor, enquanto o integrador é um *Webhook Listener*, recebendo os dados do dispositivo.

Quando um evento é identificado pela Central de Incêndio e coletado pelo GW 521, imediatamente acontece o envio ao endereço HTTP (*endpoint*) definido para o Webhook.



4. Configuração

4.1. Configuração do GW 521 e o Sistema Integrador

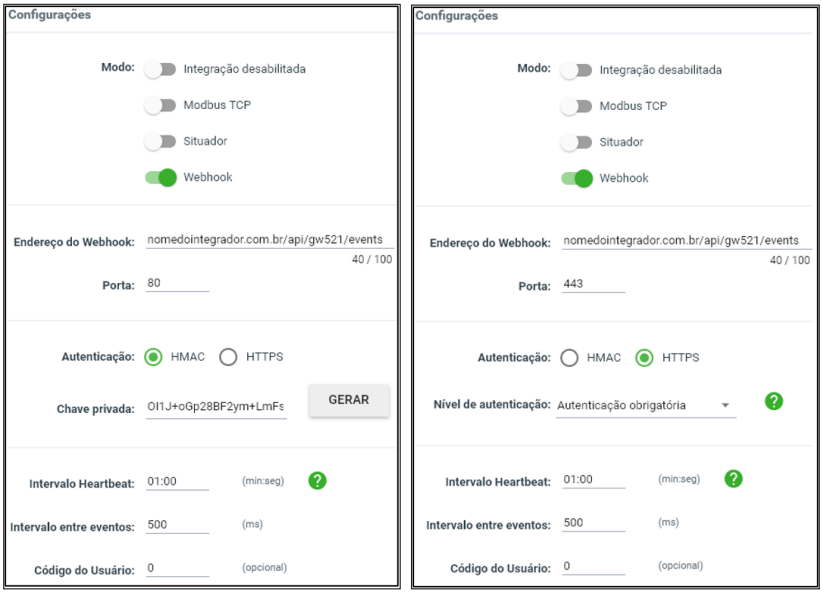
Para que a integração entre o Sistema Integrador e o GW 521 funcione corretamente, algumas configurações são necessárias.

4.2. Configuração no GW 521

A configuração do GW 521 é realizada via ProgramadorCIE pela conexão USB.

Atenção: o software ProgramadorCIE pode ser baixado gratuitamente no nosso site: *www.intelbras.com.br.*

Na aba de configurações, você terá a seguinte tela:



Descrição dos campos:

- **Modo:** determina o tipo de integração que será utilizada.
- **Endereço do Webhook:** é o endereço completo criado na API do integrador no qual o sistema irá receber os dados do GW521. Pode ser um endereço IP seguido do endpoint ou o nome do host seguido do endpoint.

  Ex: 10.1.54.133/api/gw521/event ou nomedoservidor/api/gw521/event.
- **Porta:** porta de comunicação com o servidor de integração
- **Autenticação:** pode-se optar por dois métodos de autenticação, conforme abaixo
  - **HMAC:** tipo de autenticação mais simples, requer que uma chave privada seja compartilhada entre o GW 521 e o servidor de integração.
  - **HTTPS:** utiliza o protocolo de segurança SSL/TLS. Nesse caso será necessário importar o certificado raiz do servidor e pode ser necessário carregar os certificados do equipamento, a depender da configuração do sistema integrador.
- **Chave Privada:** utilizado somente quando a autenticação HMAC é selecionada. Essa chave privada deve ser compartilhada entre o GW 521 e o Sistema Integrador para que ele possa verificar a autenticidade das mensagens enviadas pelo GW 521. Pode-se inserir uma chave previamente criada ou gerar uma chave clicando em *Gerar*.
- **Nível de Autenticação:** Utilizado somente quando a autenticação HTTPS é selecionada. Define qual o nível de segurança que o GW 521 irá tratar os certificados recebidos dos servidores de integração durante o processo de negociação inicial do protocolo SSL/TLS. Existem três níveis possíveis:
  - **Somente Criptografia:** o GW 521 não solicita o certificado do Servidor de Integração, portanto, não há verificação de autenticidade, mas ainda assim as mensagens são criptografadas.
  - **Autenticação Opcional:** o GW 521 solicita o certificado do Servidor de Integração, mas qualquer erro na verificação do certificado é ignorado prosseguindo com o processo de negociação das chaves de criptografia.
  - **Autenticação Obrigatória:** o GW 521 solicita o certificado do Servidor de Integração e qualquer falha de verificação do certificado interrompe o processo de negociação do protocolo SSL/TLS. A conexão com o servidor é encerrada impossibilitando o envio dos eventos.
- **Intervalo Heartbeat:** intervalo de tempo entre eventos que são enviados ao integrador e que sinalizam que o GW 521 continua ativo.
- **Intervalo entre eventos:** tempo de espera entre um evento e outro quando houver mais de um evento na fila esperando para ser enviado ao integrador.
- **Código do Usuário:** código opcional que pode ser utilizado pelo sistema integrador para identificar o equipamento que está realizando o envio.

Atenção: após o término das configurações no ProgramadorCIE é necessário enviá-las ao GW 521 clicando em *Enviar.* Para que as alterações tenham efeito, o GW 521 precisa ser reiniciado, para isso, clique em *Desconectar no ProgramadorCIE*.

5. Autenticação HMAC ou HTTPS

Para que o servidor de integração consiga garantir que as mensagens recebidas são do GW 521, podemos optar por duas formas de autenticação diferentes.

5.1. HMAC

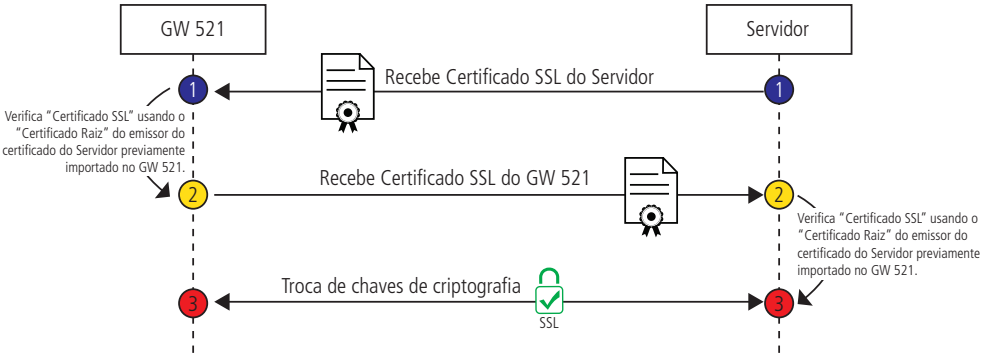
Na autenticação HMAC, o GW 521 envia junto com a mensagem um código de verificação, que é gerado a partir de uma chave privada previamente configurada. Essa mesma chave privada é cadastrada também no servidor de integração, que ao receber as mensagens do GW 521 pode gerar o código de verificação usando essa chave e comparar com o código de verificação recebido. Sendo iguais, podemos garantir a autenticidade da mensagem pois somente o GW 521 e o Servidor conhecem a chave privada utilizada para gerar o código de verificação.

Atenção:

- A mesma chave privada deve ser configurada previamente no GW 521 e no Servidor de Integração, pois não é enviada junto com as mensagens.
- O servidor de integração deve ter suporte à autenticação HMAC, contudo, essa etapa de verificação da mensagem pode ser ignorada, a critério do sistema integrador.

5.2. HTTPS (SSL/TLS)

Na autenticação HTTPS é utilizado o protocolo de segurança SSL/TLS. Esse protocolo prevê uma negociação inicial que engloba a troca de certificados para que um possa validar a autenticidade do outro, bem como a troca de chaves de criptografia para que ambos possam criptografar e descriptografar as mensagens enviadas e recebidas.



O GW 521 trabalha com dois tipos de certificados: *O certificado SSL* e o *certificado raiz da autoridade de certificação.*

A autoridade de certificação é a empresa que assina digitalmente os certificados SSL dos seus clientes usando o seu certificado raiz (Ex: GlobalSign, DigiCert, Verisign, Entrust, etc).

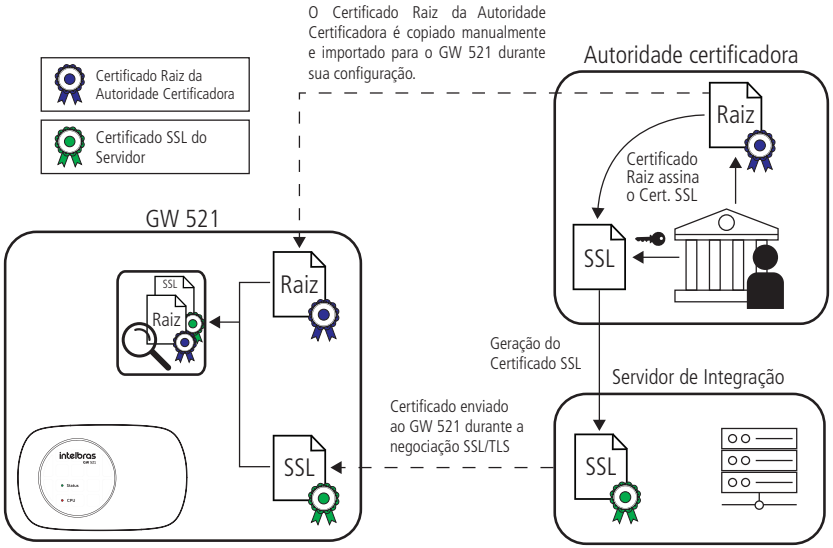
O servidor de integração por exemplo, terá um certificado SSL assinado por uma autoridade de certificação.

Quando o GW 521 inicia a conexão com o servidor e solicita o certificado do servidor, receberá um certificado SSL assinado por uma autoridade de certificação.

Para que o GW 521 consiga verificar a autenticidade desse certificado SSL, ele precisa ter uma cópia do certificado raiz da autoridade de certificação.

Essa cópia deve ser importada previamente no GW 521 utilizando o ProgramadorCIE, acessando o menu *Sistema > Configurações TLS/SSL* e clicando em *Importar* da seção *Certificado Raiz do Servidor de Integração.*

Atenção: a cópia do certificado raiz pode ser obtida diretamente no site da autoridade certificadora, ou solicitando à empresa do sistema integrador.



Da mesma forma que o GW 521 pode solicitar e fazer a verificação do Certificado SSL do servidor, o servidor de integração pode também solicitar e verificar o Certificado SSL do GW 521.

Isso significa que tanto no GW 521 quanto no servidor de integração, existe uma configuração independente quanto ao nível de autenticação que será utilizado.

Para o GW 521 é possível selecionar entre esses três níveis de autenticação:

- **Somente Criptografia:** o GW 521 não solicita o certificado do Servidor de Integração, portanto, não há verificação de autenticidade, mas ainda assim são trocadas as chaves de criptografia. Nesse caso, o servidor não necessita ter um certificado SSL e não é necessário importar o Certificado Raiz do emissor.
- **Autenticação Opcional:** o GW 521 solicita o certificado do Servidor de Integração, mas qualquer erro na verificação do certificado é ignorado prosseguindo com o processo de negociação do protocolo SSL/TLS
- **Autenticação Obrigatória:** o GW 521 solicita o certificado do Servidor de Integração e qualquer falha de verificação do certificado interrompe o processo de negociação do protocolo SSL/TLS e a conexão com o servidor, impossibilitando o envio de mensagens.

Para o servidor de integração, também existe a possibilidade de configurar o nível de autenticação. Geralmente os servidores são configurados como *Somente Criptografia*, o que significa que o servidor não irá solicitar nenhum certificado do GW 521. Entretanto, se o servidor estiver configurado para *Autenticação Opcional* ou *Autenticação Obrigatória* o certificado SSL do GW 521 será solicitado.

Para esses casos, é necessário importar no GW 521 Certificado SSL e a sua Chave Privada usando o ProgramadorCIE.

O certificado SSL do equipamento pode ser obtido diretamente com as autoridades certificadoras (Ex: GlobalSign, DigiCert, Verisign, Entrust, etc), porém existem custos envolvidos e prazos de validade curtos.

Opcionalmente, pode-se gerar certificados autoassinados sem custo e com validade de 10 anos utilizando o ProgramadorCIE. Certificados autoassinados não são emitidos por autoridades certificadores reconhecidas, e por esse motivo, para que o servidor de integração possa autenticar certificados SSL autoassinados gerados pelo ProgramadorCIE, é necessário incluir o certificado raiz do ProgramadorCIE no repositório de autoridades certificadoras do servidor de integração.

Atenção: o Certificado Raiz autoassinado do ProgramadorCIE pode ser encontrado no nosso site: *www.intelbras.com.br.*

Entre em contato com a empresa do sistema de integração para maiores detalhes de como fazer a inclusão no sistema.

6. Funcionamento

O GW 521 permite a integração das Centrais de Incêndio (CIE 1125, CIE 1250 e CIE 2500) com sistemas integradores como portarias remotas.

Por meio do conector das repetidoras da CIE, os eventos registrados pela Central de Incêndio são coletados pelo GW 521. Esses eventos são enviados para o Sistema Integrador e geralmente aparecem em formato de ocorrências dentro de um painel de controle.

O formato das informações e como as ocorrências são mostradas dependem do tipo do sistema integrador.

Atenção:

- A data e hora do evento informada pelo GW 521 é a data coletada na Central de Incêndio, portanto, sempre mantenha a Central com a data e hora atualizada.
- Não é possível enviar informações nem comandos ao GW 521 e nem para a Central de Incêndio por meio da interface ethernet.

7. Orientações e solução de problemas

- Certifique-se que o GW 521 está se comunicando com a CIE verificando se o LED STATUS se mantém apagado.
- Caso o servidor de integração esteja fora da rede local onde o GW 521 está instalado, certifique-se de que o equipamento tenha acesso à internet e que tenha permissão para fazer requisições do tipo DNS.
- Caso necessário utilize o software WireShark para analisar o tráfego de rede.
- Caso o LED Status comece a piscar, verifique as informações do item *6. Funcionamento* para solucionar o problema.

Atenção: deve ser dada ao utilizar HTTPS devido a necessidade de importar certificados para o funcionamento correto.

8. Indicações de problemas do LED Status

Para facilitar o diagnóstico de problemas, o LED Status do GW 521 pisca uma quantidade de vezes diferente para cada tipo de problema a ser sinalizado.

A sinalização acontece de forma repetitiva, iniciando por um intervalo em que o Led fica desligado e seguido pelas piscadas na quantidade determinada para aquele problema.

Para determinar qual o problema que o GW 521 está sinalizando, o usuário deve contar quantas vezes o LED Status piscou e procurar o valor na tabela abaixo.

Para encontrar a descrição do problema associado ao tipo reportado, pode-se utilizar o ProgramadorCIE em *Sistema > Informações da Central*.

Número de piscadas do LED Status	Descrição do Problema	Possíveis soluções
1	Relógio Interno: 1. Falha no Relógio Interno	2. Reinicie o equipamento. Caso o problema persista, entrar em contato com o suporte técnico Intelbras.
2	Memória Flash: 1. Falha de escrita na Memória flash	1. Reinicie o equipamento. Caso o problema persista, entrar em contato com o suporte técnico Intelbras.
3	Interface Ethernet: 1. Link-Down 2. Endereço IP inválido ou não atribuído pelo DHCP 3. Inicialização da Interface Ethernet	1. Verifique se o cabo de rede está integro e devidamente conectado no equipamento. 2. Se estiver configurado para IP Fixo, verifique se o IP digitado está correto. Se a configuração for DHCP, verifique o servidor DHCP. 3. Reinicie o equipamento. Caso o problema persista, entrar em contato com o suporte técnico Intelbras.
4	Comunicação com a Central: 1. Falha de comunicação com a CIE	1. Verifique o cabo do Conector RS485 e certifique-se de que a comunicação com o GW 521 esteja ativa na Central CIE.
5	Modbus TCP: 1. Falha ao iniciar o servidor Modbus	1. Verifique a configuração da Porta e reinicie o equipamento. Caso o problema persista, entrar em contato com o suporte técnico Intelbras.
6	Seventh Situator: 1. Nome do Host 2. IP do Sevidor 3. Autenticação no Situator 4. Envio de Eventos 5. Conexão	1. Verifique se o nome do host digitado está correto. Certifique-se também que o DNS consegue resolver o nome do host em IP através do comando ping pelo prompt de comando no computador. 2. Verifique se o IP do servidor está correto. 3. Revise as informações de Usuário/Senha ou Token, e certifique-se de que o usuário está criado no Situator com perfil de Cliente da API. 4. Certifique-se de que a lista de eventos foi devidamente cadastrada no Situator. Verifique se o código da conta cadastra está correta. 5. Verifique se o Servidor está respondendo e se a porta de comunicação com o Servidor está correta.
7	Webhook: 1. Nome do Host 2. IP do Servidor 3. Conexão 4. Envio de Eventos 5. HTTPS	1. Verifique se o nome do host digitado está correto. Certifique-se também que o DNS consegue resolver o nome do host em IP através do comando ping pelo prompt de comando no computador. 2. Verifique se o IP do servidor está correto. 3. Verifique se o Servidor está respondendo e se a porta de comunicação com o Servidor está correta. 4. Certifique-se de que o endereço do Webhook está correto e que requisições do tipo POST são respondidas com o status HTTP 200-OK 5. Falha ao estabelecer uma conexão segura HTTPS. Verifique o tipo de autenticação configurada e os certificados importados no GW 521.

Termo de garantia

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais vícios de fabricação, que porventura venham a apresentar, pelo prazo de 1 (um) ano – sendo este de 90 (noventa) dias de garantia legal e 9 (nove) meses de garantia contratual –, contado a partir da data da compra do produto pelo Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo o território nacional. Esta garantia contratual compreende a troca gratuita de partes, peças e componentes que apresentarem vício de fabricação, incluindo as despesas com a mão de obra utilizada nesse reparo. Caso não seja constatado vício de fabricação, e sim vício(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com essas despesas.
2. A instalação do produto deve ser feita de acordo com o Manual do Produto e/ou Guia de Instalação. Caso seu produto necessite a instalação e configuração por um técnico capacitado, procure um profissional idôneo e especializado, sendo que os custos desses serviços não estão inclusos no valor do produto.
3. Constatado o vício, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que conste na relação oferecida pelo fabricante – somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isso não for respeitado, esta garantia perderá sua validade, pois estará caracterizada a violação do produto.
4. Na eventualidade de o Senhor Consumidor solicitar atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, como as de transporte e segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
5. A garantia perderá totalmente sua validade na ocorrência de quaisquer das hipóteses a seguir: a) se o vício não for de fabricação, mas sim causado pelo Senhor Consumidor ou por terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o manual do usuário ou decorrentes do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto tiver sido adulterado ou rasurado; e) se o aparelho tiver sido violado.
6. Esta garantia não cobre perda de dados, portanto, recomenda-se, se for o caso do produto, que o Consumidor faça uma cópia de segurança regularmente dos dados que constam no produto.
7. A Intelbras não se responsabiliza pela instalação deste produto, e também por eventuais tentativas de fraudes e/ou sabotagens em seus produtos. Mantenha as atualizações do software e aplicativos utilizados em dia, se for o caso, assim como as proteções de rede necessárias para proteção contra invasões (hackers). O equipamento é garantido contra vícios dentro das suas condições normais de uso, sendo importante que se tenha ciência de que, por ser um equipamento eletrônico, não está livre de fraudes e burlas que possam interferir no seu correto funcionamento.
8. Após sua vida útil, o produto deve ser entregue a uma assistência técnica autorizada da Intelbras ou realizar diretamente a destinação final ambientalmente adequada evitando impactos ambientais e a saúde. Caso prefira, a pilha/bateria assim como demais eletrônicos da marca Intelbras sem uso, pode ser descartado em qualquer ponto de coleta da Green Eletron (gestora de resíduos eletroeletrônicos a qual somos associados). Em caso de dúvida sobre o processo de logística reversa, entre em contato conosco pelos telefones (48) 2106-0006 ou 0800 704 2767 (de segunda a sexta-feira das 08 ás 20h e aos sábados das 08 ás 18h) ou através do e-mail suporte@intelbras.com.br.

Sendo estas as condições deste Termo de Garantia complementar, a Intelbras S/A se reserva o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

Todas as imagens deste manual são ilustrativas.

intelbras

fale com a gente

Suporte a clientes: (48) 2106 0006
Fórum: forum.intelbras.com.br
Suporte via chat: chat.intelbras.com.br
Suporte via e-mail: suporte@intelbras.com.br
SAC: 0800 7042767
Onde comprar? Quem instala?: 0800 7245115

Produzido por: Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia SC 281, km 4,5 – Sertão do Maruim – São José/SC – 88122-001
CNPJ 82.901.000/0014-41 – www.intelbras.com.br

01.22
Indústria brasileira