



Política Atualizações de Firmware

Versões

Versão	Data	Responsável	Alteração
00	24/11/2025	Rafael Saraiva	Emissão do documento

Versões.....	2
1. Objetivo.....	4
2. Escopo.....	4
3. Diretrizes e Princípios Gerais.....	4
3.1. Conformidade normativa e regulatória.....	4
3.2. Desenvolvimento seguro (Security by Design).....	5
4. Diretrizes Gerais para Atualizações.....	5
4.1. Classificação das Atualizações.....	5
4.2. Garantia de Provimento de Atualizações de Segurança.....	5
4.3. Periodicidade e Disponibilização.....	6
5. Processo de Tratamento de Vulnerabilidades.....	6
5.1. Canais Oficiais de Recebimento.....	6
5.2. Requisitos para submissão.....	6
5.3. Confirmação de Recebimento.....	7
5.4. Critérios de Aceitação do Relato.....	8
5.5. Transferência Interna para Análise.....	8
5.6. Correção e Liberação.....	8
6. Divulgação Coordenada de Vulnerabilidades.....	9
6.1. Princípios.....	9
6.2. Conteúdo Mínimo da Comunicação.....	9
7. Canais Oficiais de Comunicação e Distribuição.....	9
8. Responsabilidades Internas.....	10

1. Objetivo

Estabelecer diretrizes formais para o desenvolvimento, provimento, comunicação e gestão das atualizações de firmware dos produtos Aligera, garantindo conformidade com:

- a Política de Segurança da Informação e Privacidade da Aligera;
- a ISO 27001;
- o Código de Defesa do Consumidor;
- o Ato nº 16417/2023 da ANATEL;
- boas práticas de Security by Design e Privacy by Design.

Esta política é complementar e subordinada à Política de Segurança da Informação da Aligera.

Em caso de conflito interpretativo, prevalecem as diretrizes estabelecidas na Política de Segurança da Informação.

2. Escopo

Esta política aplica-se a:

- todos os firmwares utilizados nos produtos fabricados pela Aligera;
- componentes de software embarcado, bibliotecas, módulos internos ou de terceiros;
- equipes de desenvolvimento, suporte técnico, segurança da informação e engenharia de produto.

2.1. Definições

- Software embarcado: Software projetado para operar em um dispositivo específico, com funções dedicadas.
- Biblioteca: Uma coleção de recursos não voláteis usados por programas de computador, para desenvolvimento de software.

- Módulos internos: Componentes de software desenvolvidos pelos próprios funcionários ou contratados da empresa Aligera.

3. Diretrizes e Princípios Gerais

3.1. Conformidade normativa e regulatória

A sistemática de atualização segue:

- requisitos de controle e melhoria contínua definidos na ISO 27001 (especialmente A.8.8, A.8.9, A.8.32 e A.5.7);
- direitos do consumidor (informação adequada, suporte pós-venda, correção de defeitos);
- obrigações do fabricante estabelecidas no Ato 16417 da ANATEL, incluindo:
 - disponibilização de atualizações de segurança;
 - comunicação tempestiva sobre vulnerabilidades;
 - mecanismos seguros para distribuição de firmware;
 - garantia de suporte ao longo do ciclo de vida;
 - disponibilização de canais formais de comunicação.

3.2. Desenvolvimento seguro (Security by Design)

Todo firmware deverá:

- seguir práticas de codificação segura;
- ser submetido a testes de segurança (estáticos, dinâmicos e fuzzing quando aplicável);
- respeitar requisitos de minimização de superfície de ataque e hardening;
- incluir mecanismos para atualização segura e autenticada.

4. Diretrizes Gerais para Atualizações

4.1. Classificação das Atualizações

As atualizações de firmware podem conter correções, melhorias e novas funcionalidades de forma conjunta.

Somente as atualizações que incluam correções de segurança serão explicitamente identificadas e comunicadas como “Atualização de Segurança”.

4.2. Garantia de Provisão de Atualizações de Segurança

A Aligera garante o fornecimento de atualizações de segurança:

- por, no mínimo, 2 (dois) anos após o lançamento do produto, ou enquanto o equipamento estiver sendo distribuído ao mercado consumidor, sendo aplicável o prazo que mais se estender.

Este prazo cumpre integralmente o Ato nº 16417 da ANATEL.

4.3. Periodicidade e Disponibilização

As atualizações serão disponibilizadas conforme necessidade técnica, criticidade da vulnerabilidade ou evolução funcional.

O firmware será distribuído exclusivamente por canais oficiais da Aligera (listados no item 7).

5. Processo de Tratamento de Vulnerabilidades

5.1. Canais Oficiais de Recebimento

A Aligera aceitará exclusivamente relatos de vulnerabilidades enviados pelos seguintes canais formais:



- E-mail dedicado de segurança: security@aligera.com.br
- Canais oficiais de suporte técnico (tipo Segurança)
- Comunicações provenientes de auditorias, testes internos ou parceiros técnicos autorizados

Relatos enviados por outros meios (ex.: redes sociais, contatos pessoais de colaboradores) deverão ser imediatamente redirecionados para os canais oficiais.

5.2. Requisitos para submissão

Para permitir triagem adequada e cumprimento dos prazos de análise, o relato deve conter, no mínimo:

1. Identificação do remetente

- Nome ou organização
- E-mail para retorno

2. Descrição técnica do problema

- Comportamento observado
- Condição suspeita ou indício da vulnerabilidade
- Serviço, protocolo ou funcionalidade afetada

3. Produtos e versões impactadas

- Modelo do equipamento
- Versão exata do firmware (ex.: v5.12)

4. Passos para reprodução

- Ambiente utilizado
- Configurações relevantes
- Sequência objetiva de ações para replicar o problema

5. Evidências complementares

- Logs sanitizados

- Capturas de pacotes
- Prints de tela
- Scripts de prova de conceito limitados

Relatos incompletos serão aceitos, mas o retorno ao remetente incluirá solicitação dos dados faltantes.

5.3. Confirmação de Recebimento

Após o envio do relato, a Aligera procederá da seguinte forma:

- Envio de confirmação automática ou manual em até 2 dias úteis, informando:
 - número de protocolo;
 - canal de comunicação oficial para continuidade;
 - orientações sobre confidencialidade e coordinated disclosure.
- Garantia de sigilo: as informações recebidas serão tratadas com confidencialidade, limitadas ao time técnico envolvido.

5.4. Critérios de Aceitação do Relato

Será considerado válido qualquer relatório que:

- indique potencial falha que comprometa segurança, privacidade, integridade, disponibilidade, configuração ou autenticidade do equipamento;
- tenha alguma base técnica mínima, ainda que incompleta;
- provenha de cliente, pesquisador ou terceiro de boa-fé.

Não serão aceitos:

- ataques ou conteúdo malicioso capaz de causar dano operacional deliberado;
- tentativas de extorsão;
- material contendo dados de terceiros sem sanitização.
- relatórios associados a versões de firmware desatualizadas.

5.5. Transferência Interna para Análise

Após validação do recebimento, o relato será imediatamente encaminhado para:

- **P&D** – análise técnica detalhada;
- **Segurança da Informação** – avaliação de risco;

5.6. Classificação de severidade

As severidades das vulnerabilidades serão classificadas de acordo com o CVSS seguindo as criticidades abaixo:

- Crítica
- Alta
- Média
- Baixa

5.7. Correção e Liberação

Vulnerabilidades classificadas como críticas ou altas receberão prioridade.

Quando aplicável, será publicada uma Atualização de Segurança, identificada como tal.

Quando a correção exigir alteração de configuração, será fornecido procedimento técnico.

O prazo estimado para a correção será de 10 dias úteis, contados a partir da aceitação do relato.

6. Divulgação Coordenada de Vulnerabilidades

6.1. Princípios

A divulgação seguirá os preceitos de coordinated vulnerability disclosure:

- comunicação inicial restrita;
- correção ou mitigação antes da divulgação pública;
- transparência com clientes afetados;
- respeito aos prazos razoáveis para tratamento.

6.2. Conteúdo Mínimo da Comunicação

Sempre que houver Atualização de Segurança, a comunicação incluirá:

- descrição resumida da vulnerabilidade;
- impacto potencial nos serviços;
- produtos e versões afetadas;
- medidas de mitigação;
- link para firmware atualizado;
- orientações de configuração quando aplicável.

7. Canais Oficiais de Comunicação e Distribuição

A Aligera utiliza exclusivamente os seguintes canais para comunicar vulnerabilidades e distribuir firmware:

Canais de Distribuição de Firmware

- Portal de documentação: <https://docs.aligera.com.br>
- Portal de Suporte Técnico: <https://suporte.aligera.com.br>

Canais de Comunicação de Vulnerabilidades

- E-mail do suporte técnico: suporte@aligera.com.br
- Portal de documentação: <https://docs.aligera.com.br>

8. Responsabilidades Internas

P&D

- Desenvolvimento, manutenção e testes do firmware;
- Análise técnica de vulnerabilidades;
- Priorização de correções.

Segurança da Informação

- Coordenação do processo de tratamento de vulnerabilidades;
- Avaliação de impacto e risco;
- Interface com o SGSIP e com a Política de Segurança da Informação.

Suporte Técnico

- Comunicação com clientes;
- Distribuição de instruções de atualização;
- Orientação sobre mitigação.

9. Encerramento do ciclo de vida (EOL)

Produtos em end of life serão sinalizados na página de documentação, local onde poderá ser obtida a última versão de firmware e informações adicionais.