1. APRESENTAÇÃO

Atuando desde 2004 na área de Tecnologia da Informação e Comunicação, a Plenatech prima pela qualidade e segurança de seus sistemas e equipamentos. Por isso, elaboramos essa Política de Suporte aos Produtos, que deve nortear as ações da nossa empresa sempre que ofertar um novo produto ao mercado.

2. ABRANGÊNCIA

Esta Política se aplica a todos os colaboradores e fornecedores envolvidos no desenvolvimento de produtos e sistemas na Plenatech, bem como na área de suporte ao cliente.

3. OBJETIVO

O objetivo desta Política é dar transparência aos usuários sobre a forma e os períodos mínimos para disponibilização de atualizações de segurança para os produtos da Plenatech.

4. REFERÊNCIAS

I. Ato nº 77, de 5 de janeiro de 2021, da Anatel

II. Resolução nº 715, de 23 de outubro de 2019, da Anatel

III. Ato nº 2436, de 7 de março de 2023, da Anatel

IV. Política de Segurança Cibernética da Plenatech

5. CONCEITOS E DEFINIÇÕES

Firmware: *software* acessível somente para leitura, programado em um *hardware* de propósito específico e armazenado de forma funcionalmente independente do armazenamento principal do equipamento.

Métodos adequados de autenticação: protocolos ou algoritmos de autenticação baseados em padronização internacionalmente reconhecida, em suas versões atualizadas.

Usuário: aquele que manipula, configura, se aproveita das utilidades e está sujeito aos impactos resultantes de vulnerabilidades e falhas apresentadas por equipamentos para telecomunicações.

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

6. PRINCÍPIOS E DIRETRIZES

I. Serão disponibilizados os recursos humanos, técnicos e financeiros necessários para a efetividade desta Política.

II. Serão conduzidos treinamentos periódicos para que todos na Plenatech conheçam e compreendam esta Política e as demais normas a ela relacionadas.

III. Serão empregados todos os esforços economicamente razoáveis para manter os usuários protegidos contra falhas e vulnerabilidades de nossos produtos.

IV. Os equipamentos terminais produzidos pela Plenatech que se conectem à Internet deverão contar com mecanismos para informar ao usuário as alterações de *software/firmware* implementadas devido às atualizações, especialmente as relacionadas à segurança.

V. A Plenatech manterá um canal público de suporte, em língua portuguesa, para informar e manter um histórico sobre as vulnerabilidades identificadas em seus produtos e sistemas, as medidas de mitigação adotadas e as correções de segurança associadas.

VI. O canal de suporte disponibilizará acesso gratuito às correções de segurança e/ou às novas versões de *software/firmware* para seus produtos, além de manuais e materiais orientativos relativos à configuração, atualização e uso seguro dos equipamentos.

VII. A Plenatech prestará, em seu canal de suporte, informações sobre as vulnerabilidades identificadas em seus equipamentos e sistemas, incluindo, no mínimo, as seguintes informações: (i) código de identificação do comunicado; (ii) título; (iii) breve resumo sobre a vulnerabilidade; (iv) descrição da vulnerabilidade; (v) produto(s) afetado(s); (vi) impacto da vulnerabilidade; (vii) instruções para a correção ou mitigação da vulnerabilidade; (viii) créditos do descobridor ou notificador; (ix) histórico da revisão.

VIII. Não serão divulgadas informações que possam permitir a exploração das vulnerabilidades identificadas.

IX. Serão providas atualizações gratuitas de segurança para os equipamentos disponibilizados ao mercado pela Plenatech por, no mínimo, dois anos após o lançamento do produto ou enquanto o equipamento estiver sendo distribuído ao mercado consumidor, sendo aplicável a opção que mais se estender.

X. A Plenatech manterá um canal público para a comunicação de falhas e vulnerabilidades identificadas em seus equipamentos e sistemas, disponível no endereço https://produto.plenatech.com/report.php.

XI. A Plenatech manterá e disponibilizará publicamente, em sua página na Internet, uma Política de Divulgação Coordenada de Vulnerabilidade.

XII. A proteção e a segurança do usuário sempre terão prioridade no desenvolvimento dos produtos e sistemas da Plenatech.

7. INDICADORES DE EFETIVIDADE

I. Frequência da disponibilização de atualizações e correções.

II. Número de downloads das atualizações e correções.

III. Desempenho colaboradores em avaliações periódicas que meçam o grau de conhecimento desta Política e demais normas internas a ela relacionadas.

8. RESPONSABILIDADES

São responsabilidades da Direção:

- Garantir a disponibilidade dos recursos necessários para a efetivação desta Política.
- Aprovar ou não qualquer alteração desta Política.
- Acompanhar os indicadores de efetividade.
- Propor melhorias e revisões a esta Política e às demais normas internas a ela relacionadas.
- Esclarecer dúvidas relacionadas a esta Política e às demais normas a ela relacionadas.

São responsabilidades dos colaboradores da Plenatech:

- Observar integralmente as disposições desta Política e demais normas a ela relacionadas.
- Comunicar imediatamente qualquer falha ou vulnerabilidade sobre a qual tenha conhecimento relativa aos equipamentos e sistemas da Plenatech.
- Conhecer as disposições desta Política e das demais normas a ela relacionadas.

São responsabilidades dos líderes:

- Fazer com que seus liderados conheçam e compreendam esta Política e as demais normas a ela relacionadas.

São responsabilidades dos usuários:

- Acessar periodicamente o canal de suporte da Plenatech para verificar a existência de vulnerabilidades que afetem seus equipamentos.
- Manter atualizado o *firmware/software* de seus equipamentos.
- Não modificar o *firmware/software* de seus equipamentos, salvo para a correção de vulnerabilidades, nos termos estipulados pela Plenatech e divulgados no canal de suporte.

9. DISPOSIÇÕES FINAIS

Para cumprir com o seu compromisso com o desenvolvimento de produtos e sistemas seguros, a Plenatech manterá um programa de adequação progressiva a esta Política.

Sempre que houver alteração, as partes interessadas receberão, na medida do possível, a versão atualizada e serão informadas sobre as mudanças realizadas.

É obrigação das partes interessadas buscar a versão mais atual desta Política sempre que necessário.

Nos colocamos à disposição pelo e-mail suporte@plenatech.com para esclarecer dúvidas relativas à interpretação dos termos ou diretrizes aqui estabelecidos e para receber sugestões de melhoria.

10. CONTROLE

Esta Política foi finalizada e validada no dia 24 de abril de 2024 e homologada pela Diretoria no dia 24 de abril de 2024 com vigência a partir do dia 24 de abril de 2024, devendo ser revisada anualmente ou sempre que necessário.