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 Divulgação Coordenada de Vulnerabilidades, que deve nortear as ações da nossa empresa sempre que forem determinadas falhas ou vulnerabilidades de segurança em nossos produtos e sistemas.

2. ABRANGÊNCIA

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

3. OBJETIVO

O objetivo desta Política é garantir a segurança dos usuários dos produtos e sistemas da Plenatech, divulgando de forma clara e transparente as vulnerabilidades identificadas e oferecendo aos usuários, de forma gratuita e facilitada, as correções de segurança desenvolvidas.

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

V. Política de Suporte aos Produtos da Plenatech

VI. ISO/IEC 29.147/2018.

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 conheçam e compreendam esta Política e as demais normas a ela relacionadas.

III. A Plenatech deseja e encoraja que toda pessoa que tenha conhecimento de falhas ou vulnerabilidades em seus sistemas e equipamentos comuniquem o fato no canal disponível (https://produto.plenatech.com/report.php). Devem ser reportadas as seguintes vulnerabilidades: (i) quebras de controle de acesso; (ii) possibilidade de injeção; (iii) falhas criptográficas; (iv) configurações de segurança incorretas ou em desacordo com as normas vigentes; (v) falhas de autenticação; (vi) falhas que comprometam a integridade de dados; (vii) falhas de registro; (viii) falhas de monitoramento de segurança; (ix) possibilidade de uso de senhas fracas ou em branco; (x) falhas em filtros *antispoofing*; (xi) demais falhas e vulnerabilidades que possam oferecer riscos de segurança ao usuário.

IV. Todas as comunicações de falhas e vulnerabilidade recebidas serão tratadas com zelo e seriedade.

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

VI. A comunicação de falhas e vulnerabilidades identificadas em nossos sistemas e equipamentos poderá ser feita por meio de formulário seguro (HTTPS) disponível no nosso site (https://produto.plenatech.com/report.php).

VII. A comunicação deve incluir, no mínimo: (i) a descrição da vulnerabilidade; (ii) instruções sobre como reproduzir o problema; (iii) o modelo do equipamento em que a vulnerabilidade foi identificada; (iv) a versão do *software/firmware*; (v) identificação do notificador (para darmos os devidos créditos do descobridor); e (vi) e-mail de contato do notificador (para envio de confirmações e atualizações e eventual solicitação de informações adicionais).

VIII. O notificador que reportar uma vulnerabilidade receberá uma mensagem no e-mail indicado confirmando o recebimento da vulnerabilidade reportada, além de atualizações sobre a evolução do caso. Todas as mensagens enviadas terão opção de descadastramento (*opt-out*) e o notificador poderá, a qualquer momento, optar por deixar de receber as mensagens.

IX. As comunicações serão apuradas em prazo razoável, conforme processos e procedimentos internos, e serão priorizadas as que apresentam maiores riscos para a empresa e seus clientes.

X. Sempre que a divulgação da vulnerabilidade antes de sua correção puder trazer riscos significativos à Plenatech, seus colaboradores, clientes ou fornecedores, a empresa não a divulgará até que as medidas corretivas e mitigatórias adequadas sejam tomadas.

XI. As informações recebidas por meio dos canais de comunicação de falhas e vulnerabilidades, bem como os processos e procedimentos posteriores, serão considerados segredo industrial e, portanto, confidenciais, não podendo ser revelados a quem quer que seja.

XII. 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.

XIII. A Plenatech manterá um canal público de suporte 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.

XIV. O canal de suporte disponibilizará acesso 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.

XV. 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.

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

XVII. Quando identificar vulnerabilidades que possam afetar outros fornecedores, a Plenatech envidará esforços razoáveis para comunicá-los antes de divulgá-las publicamente.

XVIII. A Plenatech procurará equilibrar a necessidade de prestar informações públicas sobre as vulnerabilidades de segurança identificadas com a eventual necessidade de tempo de outros fornecedores para respondê-las efetivamente podendo, para isso, buscar o apoio e orientação das autoridades competentes

XIX. A Plenatech só irá encaminhar o nome e as informações de contato do comunicante a outros fornecedores afetados quando expressamente autorizada por ele.

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

7. INDICADORES DE EFETIVIDADE

I. Número de comunicações recebidas.

II. Número de falhas e vulnerabilidades confirmadas divulgadas.

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.
- Deliberar sobre a necessidade de adoção de medidas preventivas ou corretivas destinadas a prevenir riscos decorrentes de falhas e vulnerabilidades identificadas.

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 comunicantes:

- Não explorar as vulnerabilidades identificadas.
- Não divulgar publicamente as vulnerabilidades identificadas até que sejam disponibilizadas nos canais oficiais da Plenatech.
- Reportar as vulnerabilidades detectadas nos canais apropriados e com as informações necessárias para sua devida apuração e correção.

São responsabilidades dos usuários:

- Verificar periodicamente o canal de suporte da Plenatech para verificar a existência de vulnerabilidades que afetem seus equipamentos.
- Não explorar vulnerabilidades dos 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.