Política de Gestão de Vulnerabilidades

1. **Objetivo:**

Assegurar a integridade, confidencialidade e disponibilidade das transações financeiras processadas pela **M5 Conta Digital LTDA**,
através da identificação, avaliação e mitigação proativa de vulnerabilidades nos sistemas, aplicativos e redes envolvidos.

2. **Abrangência**

Esta política abrange todos os sistemas, recursos e informações pertencentes à **M5 Conta Digital LTDA** englobando tanto os sistemas de
tecnologia da informação e comunicação quanto os colaboradores, prestadores de serviço e terceiros com acesso a esses sistemas e informações.

3. **Avaliação de Vulnerabilidades**

São realizadas avaliações regulares de vulnerabilidades em todos os sistemas e aplicativos envolvidos no processamento de transações, utilizando ferramentas automatizadas e testes manuais.

As prioridades de correção serão comunicadas de maneira transparente às equipes responsáveis, incluindo informações detalhadas sobre os riscos associados a cada vulnerabilidade, conforme sua classificação.

As vulnerabilidades serão classificadas de acordo com sua criticidade e impacto, estabelecendo prioridades para a sua correção, através de ferramentas de varredura automatizada, testes de penetração e revisões de código para identificar e classificar as vulnerabilidades.

3.1. Classificação e Correção de Vulnerabilidades

Após serem avaliadas de acordo com o impacto e criticidade, as vulnerabilidades podem ser:

Baixo Risco: Vulnerabilidades consideradas de baixa criticidade e impacto, como questões menores de segurança que têm um impacto limitado nas operações. As correções serão programadas e implementadas de acordo com a disponibilidade de recursos. Podendo se considerar a correção durante a próxima atualização planejada ou ciclo de manutenção.

Médio Risco: Vulnerabilidades com um nível moderado de criticidade e impacto, podem incluir falhas que, se exploradas, podem resultar em consequências significativas, mas não são iminentes. Sendo implementadas correções em um prazo razoável, considerando a gravidade moderada das vulnerabilidades. Programando as correções em uma janela de manutenção apropriada para minimizar o impacto nas operações.

Alto risco: Será corrigido imediatamente as vulnerabilidades críticas, sendo implementadas medidas de mitigação temporárias, se necessário, enquanto as correções permanentes são preparadas, com um processo de correção urgente que envolva todas as partes relevantes.

4. Monitoramento

Implementados sistemas de monitoramento contínuo para detectar atividades suspeitas nos sistemas e redes, juntamente com o desenvolvimento de resposta a incidentes para reagir eficazmente a qualquer exploração ou ameaça identificada.

Além do mais, será monitorado continuamente a eficácia das correções e ajustando as prioridades conforme necessário.

5. Testes de Simulação

Serão realizados testes de simulação regulares para avaliar a prontidão e eficácia dos procedimentos de resposta a incidentes, sendo documentados e analisados os resultados, aprimorando continuamente os processos de segurança.

6. Responsabilidades

A organização da **M5 Conta Digital LTDA** simplifica a identificação dos responsáveis por cada processo crítico. Nesse contexto, cabe à Alta Administração, em colaboração com o setor de Compliance, centralizar o gerenciamento de todas as ações estabelecidas nesta Política.

7. Aprovação e Vigência

O presente Plano foi aprovado pelos membros componentes da Alta Administração, entrando em vigência na data da sua aprovação.

A vigência deste Plano é indeterminada, podendo ser substituído apenas por uma versão atualizada.