POLÍTICA DE SEGURANÇA CIBERNÉTICA DA MULVI INSTITUIÇÃO DE PAGAMENTO S.A.

OBJETIVO

O objetivo desta política é estabelecer diretrizes que são necessárias para assegurar a confidencialidade, integridade e disponibilidade dos dados e sistemas da informação que são utilizados na MULVI, bem como a implementação de controles e procedimentos para o tratamento de incidentes cibernéticos.

ABRANGÊNCIA

A Política de Segurança Cibernética abrange todas as áreas de negócio, bem como todos os colaboradores e prestadores de serviços que manuseiam dados e informações sensíveis à conduta, mediante atividades operacionais da organização.

Todo colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações da MULVI e deve cumprir as determinações da política, normas e padrões de segurança.

DIRETRIZES

A Segurança Cibernética da MULVI tem como diretrizes gerais:

1. Resguardar a proteção dos dados de acessos indevidos contra modificações, destruições ou divulgações não autorizadas;

2. Garantir que os dados e os sistemas estejam protegidos e sendo utilizados somente para cumprimento de suas atribuições;

3. Criar procedimentos e ferramentas implementadas para monitorar e impedir que as informações sensíveis sejam manipuladas sem a devida autorização;

4. Tecnologias e processos devidamente implementados para detectar, prevenir e recuperar o ambiente de ameaças sofisticadas, incluindo detecções a nível de comportamento nos servidores e *endpoints*;

5. Os planos de resposta a incidentes e segurança cibernética, incluem seu fluxo e áreas responsáveis pela atuação e mitigação em cenários de incidentes;

6. O Plano de Continuidade de negócios é administrado de acordo com os requisitos estabelecidos pela Unidade de Segurança da Informação;

7. Todos os ativos críticos da organização que armazenam e processam dados sensíveis são mantidos em ambientes restritos, com segregação de rede e controles de acesso adequados a cada necessidade;

8. Possuímos arquivos de restauração íntegros para garantia do ambiente e serviços, a ser utilizado em situações adversas ou inesperadas;

9. Os softwares devem ser mantidos atualizados e protegidos de vulnerabilidades que possam impactar em comprometimento do ambiente;

10. Processos de gerenciamento de vulnerabilidades, remediações, documentações devidamente implementados e submetidos às áreas de interesse;

11. Monitoramento, registro e análise, bem como o controle de incidentes e plano de continuidade de negócio em cenários relevantes para as atividades da MULVI, que abrangem, inclusive, informações tratadas pelas empresas prestadoras de serviços a terceiros;

12. Adoção de política de trabalho remoto seguro, onde os colaboradores e terceiros possuem acessos ao ambiente de forma segura e monitorada;

13. Toda nova tecnologia, ferramenta ou solução passa por avaliações de segurança antes de serem submetidas para produção;

14. As áreas de desenvolvimento devem garantir que os sistemas estejam seguros e adotar procedimentos e testes periódicos de varreduras para detecção de vulnerabilidades, garantindo a boa qualidade nas entregas;

15. Realizar testes anuais para garantir a eficácia dos processos, além de produzir anualmente um relatório de resposta a incidentes do ambiente tecnológico da MULVI;

16. Designar ações para prevenir, identificar, registrar e responder incidentes e crises no ambiente cibernético, que possam ocasionar o comprometimento dos pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais;

17. Adotar mecanismos para disseminar a cultura de segurança da informação e cibernética na organização.

VIOLAÇÕES DE SEGURANÇA

As violações dos cenários cibernéticos descritas poderão ensejar a aplicação de medidas disciplinares.

CANAIS DE COMUNICAÇÃO

Nossos alertas de segurança e/ou incidentes, como todas as notificações deverão ser enviadas para o canal de comunicação: csirt@banesecard.com.br