POLÍTICA DE SEGURANÇA CIBERNÉTICA

Belo Horizonte, Setembro de 2023

Controle do Documento							
Elaborador (es)	Gestão de Riscos	**Mês**	Maio/2022	**Revisão 2:**	03	**Mês**	Setembro/2023
Revisor:	Diretoria de Compliance	**Mês**	Maio/2022	**Revisor**	Diretoria de Compliance	**Mês**	Setembro/2023

ÍNDICE

1. INTRODUÇÃO.....3
2. ESCOPO.....3
3. OBJETIVO.....3
4. PRINCÍPIOS.....4
5. DIRETRIZES.....4
6. RECOMENDAÇÕES DE SEGURANÇA PARA OS CLIENTES/USUÁRIOS.....6

Controle do Documento							
Elaborador (es)	Gestão de Riscos	**Mês**	Maio/2022	**Revisão 2:**	03	**Mês**	Setembro/2023
Revisor:	Diretoria de Compliance	**Mês**	Maio/2022	**Revisor**	Diretoria de Compliance	**Mês**	Setembro/2023

Monettar

1. INTRODUÇÃO

A Monettar S/A surgiu a partir da união de experientes profissionais do mercado financeiro e do ramo tecnológico, formando uma equipe multidisciplinar que oferece ao mercado uma solução inovadora para as operações de crédito.

A atuação da Monettar é pautada pela observância de todos os ditames legais acerca do tema.

A Segurança da Informação está em seu DNA, disponibilizando aqui um resumo da sua Política de Segurança Cibernética ("Política") para que você possa conhecer um pouco mais dos parâmetros da empresa para a proteção de seus dados.

2. ESCOPO

Sujeita-se à Política, a Monettar S/A (doravante denominada "Monettar"), juntamente com todos os funcionários e sócios (denominados aqui, "Colaboradores"), fornecedores e parceiros, caso tenham acesso, armazenem, processem ou transmitam informações pertencentes ou sob a guarda da Monettar.

3. OBJETIVO

A intenção da Monettar com a criação desta política é:

a) Manter a confidencialidade, integridade e disponibilidade das informações de propriedade ou sob sua guarda;
b) Estabelecer medidas para a proteção da infraestrutura que suporta os serviços e atividades de negócio;

Monettar

c) Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

4. PRINCÍPIOS

a) Confidencialidade: garantir que as informações disponibilizadas pelos clientes serão acessadas apenas por indivíduos, entidades ou processos autorizados;
b) Integridade: garantir que as informações serão precisas, completas e protegidas de alterações indevidas, intencionais ou acidentais;
c) Disponibilidade: garantir que as informações são acessíveis e utilizáveis sob demanda, por indivíduos, entidades ou processos autorizados.

5. DIRETRIZES

O acesso a sistemas, recursos e outros ativos de informação deve ser concedido mediante uma autenticação válida e baseado em:

a) Necessidade do negócio;
b) Princípio do menor privilégio;
c) Segregação de funções.

Os acessos devem ser gerenciados através de um ciclo de vida desde a criação até a desativação, incluindo revisões periódicas quanto à precisão e adequação.

Logs e trilhas de auditoria devem ser habilitados em ambientes de produção, protegidos de acessos e alterações não autorizados e registrar:

a) Que atividade foi executada;
b) Por quem a atividade foi executada;

Monettar

c) Quando a atividade foi executada;
d) No que a atividade foi executada;
e) Devem ser usados algoritmos criptográficos conforme a necessidade;
f) Uso de ferramentas e processos que impeçam que as informações sensíveis deixem o ambiente interno sem autorização;
g) Adoção de soluções e/ou processos que possibilitem a prevenção, detecção e identificação de ataques a componentes da infraestrutura da Monettar;
h) Processo de gerenciamento do ciclo de vida de vulnerabilidades, desde a identificação até a remediação, incluindo diretrizes para documentação, emissão de relatórios e divulgação, deve estar implementado;
i) Soluções de software anti-malware de detecção, prevenção e recuperação ou controles equivalentes, devem estar implementados para proteger o ambiente da Monettar;
j) Ativos de informação considerados críticos, que armazenem e/ou processem informações sensíveis devem ser restringidos às áreas segregadas da rede, com controle de acesso apropriado;
k) Bancos de dados de produção devem possuir backups suficientes para restaurar o funcionamento dos sistemas no evento de uma perda de dados ou interrupção do serviço;
l) Durante o ciclo de vida de desenvolvimento de software, requisitos de segurança devem ser aplicados para garantir a confidencialidade, integridade e disponibilidade das informações;
m) Deve ser feita uma avaliação de segurança antes da implementação de qualquer nova tecnologia, ferramenta ou solução em produção;
n) Procedimentos e controles voltados à prevenção, tratamento e redução da vulnerabilidade da Monettar a incidentes de segurança cibernética, além das diretrizes para registro, análise de causa e impacto e avaliação da relevância de incidentes, devem estar implementados;

Monettar

o) Informações devem ser classificadas para auxiliar no mapeamento consistente dos ativos de informação e estabelecer o nível de proteção adequado em seu armazenamento, transmissão e uso;

p) Treinamentos de conscientização são obrigatórios, devendo ser feitos sempre que necessário, ao menos uma vez ao ano, apresentando os princípios da segurança da informação para auxiliar os funcionários a reconhecer situações de risco e agir corretamente;

A Política de Segurança Cibernética da Monettar deve ser revisada, no mínimo, uma vez ao ano.

6. RECOMENDAÇÕES DE SEGURANÇA PARA OS CLIENTES/USUÁRIOS

i. Criação de senhas complexas, sem a utilização de dados pessoais na composição (ex: data de nascimento, nome de familiar, entre outros);

ii. Sempre que houver algum indício ou suspeita de vazamento ou comprometimento de suas credenciais, altere sua senha o mais rápido possível;

iii. Se possível, não utilize a mesma senha para vários serviços. Sugerimos que utilize um gerenciador de senhas para o armazenamento seguro;

iv. Não compartilhe sua senha com terceiros. Ela é pessoal e intransferível;

v. Se possível, habilite um segundo fator de autenticação (ex: biometria ou SMS);

vi. Procure instalar uma solução de antivírus no seu computador e a mantenha atualizada;

vii. Nunca informe dados pessoais, corporativos ou financeiros em ligações, ou mensagens recebidas de pessoas desconhecidas. Isso vale para sites suspeitos. Verifique sempre se o site que está acessando é realmente o verdadeiro;

viii. Mantenha consigo sempre uma cópia de segurança (backup) de dados importantes.