meep

Política de **segurança cibernética e da informação**

Política de **segurança cibernética e da informação**

Nome: POL-SEGURANÇA- CIBERNÉTICA-E-DA-INFORMAÇÃO | **Versão**: 0003 |
Classificação: Público | **Data**: 05/12/2025 | **Próxima Revisão**: 05/12/2026

Empresa:	MEEP PAGAMENTOS S.A.
CNPJ:	44.807.087/0001-89
Representante do Empresa:	Samuel Antunes
Elaborado por:	Área de Compliance
Verificado por	Jurídico
Aprovado por:	Samuel Antunes
Nome do Documento:	Política de Segurança Cibernética e da Informação
Distribuição:	**Interna:** Diretoria de Operações, Diretoria de Finanças, Diretoria de Tecnologia, Arquivo MEEP PAGAMENTOS S.A.
	Externa: Pública

Meep - Todos os direitos reservados

Política de **segurança cibernética e da informação**

Sumário

1. OBJETIVO **3**
2. BASE LEGAL E REGULATÓRIA **3**
3. DESTINATÁRIOS **3**
4. TERMOS E DEFINIÇÕES **4**
5. DIRETRIZES **5**
6. PRINCÍPIOS **7**
6.1. Controle de Acesso à Informação 8
6.2. Classificação de Acessos 8
6.3. Rotulagem e Manuseio 9
6.4. Dados Pessoais 9
6.5. Desenvolvimento de Aplicações e Sistemas 9
6.6. Processamento, Armazenamento de Dados e Computação em Nuvem 9
6.7. Cópias de Segurança (Backup) 12
6.8. Continuidade de Segurança da informação 12
6.9. Gestão de Riscos e Incidentes de Segurança 12
6.10. Plano de Continuidade de Negócios 14
6.11. Cenários Considerados nos Testes de Continuidade dos Negócios 14
7. PAPÉIS E RESPONSABILIDADES **15**
7.1. Área de Segurança da Informação 15
7.2. Gestor de Segurança da informação 16
7.3. Acionistas, Diretores, Colaboradores, Prestadores de Serviços e Parceiros 16
8. EFETIVIDADE E VIOLAÇÃO **18**
9. DOCUMENTOS RELACIONADOS **19**
10. ATUALIZAÇÕES E CONTROLE DE REVISÕES DESTA POLÍTICA **20**

Meep - Todos os direitos reservados

Política de **segurança cibernética e da informação**

1. OBJETIVO

A presente Política de Segurança Cibernética e da Informação (“Política”) visa, através do estabelecimento de diretrizes e regras, a proteção dos ativos de informação, de propriedade da MEEP PAGAMENTOS S.A. (“MEEP” ou “Instituição”) de modo seguro e transparente, através da prevenção, detecção e redução dos riscos associados, de forma alinhada ao porte, ao perfil de risco, ao modelo de negócio, a natureza e complexidade das atividades, produtos e serviços oferecidos, bem como com a sensibilidade dos dados e das informações sob responsabilidade da Instituição, além de fiel observância aos requisitos legais e exigências dos órgãos regulatórios.

2. BASE LEGAL E REGULATÓRIA

Esta Política cumpre fielmente a legislação concernente e as disposições do Banco Central do Brasil (“BCB”) e Conselho Monetário Nacional (“CMN”), em especial:

- Resolução BCB n° 85, de 8 de abrilde 2021 que dispõe sobrea política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.

3. DESTINATÁRIOS

Esta Política se aplica a todos os sócios, diretores, gestores, administradores, funcionários, prestadores de serviços, prepostos, terceirizados e quaisquer demais pessoas físicas ou jurídicas contratadas ou outras entidades que participem, de forma direta ou indireta, das atividades diárias e negócios da MEEP (“Destinatários”).

Os Destinatários devem atender a todas às diretrizes e procedimentos estabelecidos nesta Política, desde o momento de início do relacionamento, em que tomem ciência do mesmo, e, naquilo o que se prolongar no tempo, pelo prazo de 20 (vinte) anos contados do término do vínculo do Destinatário com a MEEP.

Meep - Todos os direitos reservados

4. TERMOS E DEFINIÇÕES

Para fins dessa Política, compreendem-se da seguinte forma os termos:

- **Confidencialidade:** Garantir que somente o usuário da informação, devidamente autorizado pelo gestor da informação, terá acesso às Informações, respeitando os critérios de segregação de funções;
- **Integridade:** Garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;
- **Disponibilidade:** Garantir que as informações estejam sempre disponíveis para o usuário da informação;
- **Conformidade:** Processo que visa verificar o cumprimento das normas estabelecidas;
- **Autenticidade:** Garantir a identidade de quem está enviando a Informação, ou seja, gera o não- repúdio que se dá quando há garantia de que o emissor não pode se esquivar da autoria da mensagem (irretratabilidade);
- **Informação:** Conjunto de dados, imagens, textos, códigos ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja vinculado;
- **Ativos de Informação:** São os meios de produção, transmissão, armazenamento e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que possuem acesso às informações, bem como todas as informações processadas, produzidas, coletadas, armazenadas ou descartadas pela MEEP;
- **Riscos Cibernéticos:** Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação;
- **Ameaça:** Qualquer fator ou ação capaz de interferir e causar danos à integridade, à confidencialidade, à autenticidade e à disponibilidades de dados e informações sobre a MEEP;

Meep - Todos os direitos reservados

- **Vulnerabilidade:** São fraquezas ou falhas que, se exploradas por ameaças maliciosas, podem resultar no comprometimento da integridade, confidencialidade ou disponibilidade das informações;

- **Controle de Acesso:** Conjunto de regras, processos, procedimentos, recuros e meios para permitir ou negar o acesso;

- **Negação de serviço:** Um ataque de negação de serviço (também conhecido como DoS Attack, um acrônimo em inglês para Denial of Service), é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga;

- **Adequação:** Garantir que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo gestor da informação;

- **Fraudes Externas e invasões:** Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, com o uso de conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico;

- **BACEN:** Banco Central do Brasil.

5. DIRETRIZES

O cumprimento da Política é de responsabilidade de todos os Destinatários, os quais devem seguir as diretrizes abaixo:

a) Proteger as informações contra acesso,modificações, destruiçãoou divulgação não autorizada;

b) Prover a adequada classificação da informação, considerando os critérios de confidencialidade, integridade e disponibilidade;

c) Assegurar que os recursos utilizados para o desempenho da sua função sejam utilizados apenas para as finalidades desempenhadas a sua atividade;

Meep - Todos os direitos reservados

d) Garantir que os sistemas e as informações que estão sob a sua responsabilidade sejam adequadamente protegidos;

e) Atender às leis que regulamentam as atividades da MEEP e seu mercado de atuação;

f)Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;

g) Garantir a continuidade do processamento das informações críticas de negócios;

h) Comunicar imediatamente aos responsáveis quaisquer descumprimentos desta Política.

A Diretoria da Instituição, ao aprovar esta Política de Segurança Cibernética, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética, buscando sempre manter a Instituição em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à Instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A MEEP nomeia um diretor responsável por esta política e garante a ausência de conflitos de interesses ao desempenhar outras funções na Instituição.

Visando o fortalecimento da cultura de Segurança da Informação através da disseminação dos princípios e diretrizes descritos nesta Política, a Instituição possui processos de treinamento e comunicação, que consistem no processo de capacitação e conscientização, de todos os níveis, ao que se refere à segurança da informação, contemplando segurança de dados, segurança cibernética, inclusive com relação aos terceiros e demais contrapartes.

Meep - Todos os direitos reservados

A Instituição conta com ferramentas, mecanismos e controles adequados para garantir a efetividade do objetivo, diretrizes, princípios, regras,papéis, responsabilidades e demais conteúdosabordados nesta Política,dentre eles: processo, métricas,indicadores, trilhas de auditorias e testes. Esta política e o seu conteúdo são parte integrante do plano de auditoria interna e, eventuais deficiências identificadas são tempestivamente tratadas.

Toda documentação que suporta e comprova o correto funcionamento do conteúdo aqui estabelecidos permanecerá a disposição da autoridade reguladora pelo prazo mínimo de 5 (cinco) anos.

6. PRINCÍPIOS

A estratégia de Segurança da Informação da MEEP é baseada em arquitetura com os seguintes domínios: Governança de Segurança da Informação, Segurança Cibernética Ofensiva, Segurança Cibernética Defensiva e Treinamento, Conscientização e Cultura.

Todos os princípios adotados pela MEEP visam atingir as diretrizes e objetivos desta política, reduzindo a vulnerabilidade da empresa quanto aos riscos de segurança cibernética.

Os procedimentos e os controles da segurança cibernética são implementados de modo a abranger a autenticação, criptografia, prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes de invasão e de outras metodologias de operações ofensivas para detecção e correção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores, a manutenção de cópias de segurança dos dados e das informações, e a prevenção e reposta de incidentes de segurança da informação.

Aos mecanismos acima indicados, a MEEP realiza acompanhamento e controle com vistas a assegurar a implementação e a efetividade da Segurança Cibernética e da Informação, seguindo as diretrizes desta Política, do Plano de Ação e de Resposta a Incidentes e os requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Meep - Todos os direitos reservados

Tal acompanhamento é realizado através da:

a) definição de processos, testes e trilhas de auditoria;

b) definição de métricas e indicadores adequados; e

c) identificação e a correçãode eventuais deficiências.

Os procedimentos de acompanhamento de controle devem ser submetidos a testes periódicos pela auditoria interna, quando aplicável, compatíveis com os controles internos da MEEP.

6.1. Controle de Acesso à Informação

Os acessos à informação, em conformidade com a Política de Gestão de Acessos, são controlados, monitorados e restritos de forma a garantir sua utilização apenas para a realização das atividades inerentes a cada um dos Destinatários, sendo revisados periodicamente.

As concessões, revogações, transferências e revisões de acesso devem respeitar os fluxos de aprovação e execução determinados pela empresa, bem como se utilizar das ferramentas oficiais disponibilizadas paraestes processos. Todos os acessos são rastreáveis, possibilitando auditoria e responsabilidade individual de um usuário.

Adicionalmente, a empresa possui procedimentos para proteger equipamentos e informações contra usuários que não possuem autorização para acessá-los. Para a execução deste processo, são solicitadas autorizações aos gestores responsáveis e conferidos os titulares, junto ao Departamento de Recursos Humanos, quando aplicável, inclusive para a concessão de acesso às dependências da MEEP, segregando áreas com acessorestrito, por força de norma regulatória.

6.2. Classificação de Acessos

A classificação das informações deve respeitar o ciclo de vida da informação desde a sua geração até o descarte.

Meep - Todos os direitos reservados

Os dados e informações sob responsabilidade da MEEP serão classificados quanto à relevância, observando os seguintes parâmetros:

a) Público: podem ser acessados por qualquer pessoa;

b) Interno: podem ser acessados apenas por colaboradores da empresa;

c) Reservado: podem ser acessados apenas por um grupo de pessoas ou cargos específicos

d) Confidencial: podem ser acessadospor apenas algumas pessoas.

6.3. Rotulagem e Manuseio

A rotulagem e o manuseio apropriado da informação e os seus ativos relacionados, no formato físico e eletrônico, deve ser realizado refletindo os níveis de classificação das informações.

6.4. Dados Pessoais

A MEEP possui Política de Proteção de Dados que define os procedimentos e controles relativos à coleta, processamento, proteção e compartilhamento de informações pessoais, respeitando os direitos de privacidade, à intimidade, honra, e outros direitos reservados ao titular dos dados, seguindo as leis e regulamentações de proteção de dados aplicáveis.

6.5. Desenvolvimento de Aplicações e Sistemas

A MEEP possui princípios que garantem o desenvolvimento segurode aplicações e sistemas, cujos procedimentos seguem as boas práticas de mercado, como segregações de função, testes, homologação, e gestão de mudanças, garantindo que a segurança da informação esteja projetada e implementada no ciclo de vida do desenvolvimento dos sistemas de informação.

6.6. Processamento, Armazenamento de Dados e Computação em Nuvem

As contratações de serviços de terceiros para o processamento e armazenamento de dados, e de computação na nuvem seguem todos requisitos de segurança, avaliando a relevância do serviço contratado, criticidade, e a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo serviço.

Meep - Todos os direitos reservados

Política de **segurança cibernética e da informação**

Todos os prestadores deste tipo de serviço que são contratados pela MEEP passam por uma rígida avaliação de sua capacidade, garantindo a conformidade (com a legislação e regulamentação em vigor, com as certificações exigidas e com os critérios de qualidade desejados) do prestador de serviços, assim como a confidencialidade, integridade, disponibilidade e recuperabilidade dos dados e das informações processadas e armazenadas pelo contratado. Estes prestadores garantem o acesso da MEEP, sempre que solicitado, aos dados e às informações a serem processados ou armazenados, às informações e recursos de gestão adequados ao monitoramento dos serviços, aos relatórios de auditoria e as evidências dos controles de identificação e segregação dos dados por parte do prestadorde serviços. Na execução de aplicativos por meio da internet, compete a MEEP assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

Os contratos firmados pela MEEP para contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever, minimamente:

a) a indicação dos países e da região em cada país onde os serviçospoderão ser prestados e onde os dados poderão ser armazenados, processados e gerenciados;

b) a adoção de medidas de segurança para a transmissão e armazenamento dos dados;

c) a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controlesde acesso

d) para proteção das informações dos clientes;
e) a obrigatoriedade, em caso de extinção do contrato, de:

I. transferência dos dados ao novo prestador de serviços ou à MEEP;

II. exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos;

f) o acesso da MEEP a:

I. informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nas alíneas “a”, “b” e “c” da diretriz 5 desta política;

II. informações relativas às certificações e aos relatórios de auditoria especializada;

III. informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a obrigação de a empresa contratada notificar a MEEP sobre a subcontratação de serviços relevantes para a Instituição;

h) a permissão de acesso do BACEN aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

i) a possibilidade de adoção de medidas pela MEEP, em decorrência de determinação do BACEN; e

j) a obrigação de a empresa contratada manter a MEEP permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

k) No caso da decretação de regime de resolução da MEEP pelo BACEN:

I. a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso que estejam em poder da empresa contratada;

II. a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a. a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

Meep - Todos os direitos reservados

b. a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

A MEEP mantém a disposição do BACEN, por ao menos 5 (cinco) anos, as informações contratuais e todos os documentos relativos ao contrato de prestação de serviços.

6.7. Cópias de Segurança (Backup)

A MEEP possui instituídos procedimentos onde são definidos os requisitos da organização para as cópias de segurança das informações, dos softwares e dos sistemas. A Instituição mantém o registro completo e exato das cópias de segurança, provendo documentação apropriada sobre os procedimentos de restauração da informação.

6.8. Continuidade de Segurança da informação

A política determina que todos os dados classificados como essenciais, incluindo bases operacionais, registros financeiros, logs críticos e documentos de governança, devem possuir cópias de segurança geradas de forma periódica. Esses backups devem ser armazenados em ambiente seguro, com controle de acesso restrito e testes regulares de restauração para garantir que possam ser usados em caso de falhas, incidentes ou interrupções operacionais.

6.9. Gestão de Riscos e Incidentes de Segurança

Os riscos de segurança da informação são identificados e acompanhados através de um processo de análise de vulnerabilidades, quantificando e qualificando as ameaças e seus respectivos impactos sobre os ativos de informação, para associação dos níveis de proteção adequados.

Para garantir rastreabilidade, controle e adequada resposta a incidentes, todos os ativos de TI da MEEP incluindo notebooks, desktops, dispositivos móveis, servidores, equipamentos de rede e demais recursos tecnológicos devem ser devidamente identificados com etiqueta de patrimônio, contendo o número único do ativo.

Após a identificação física, cada ativo deve ser registrado na ferramenta oficial de gestão de ativos de TI, onde são mantidas informações como:

Meep - Todos os direitos reservados

- responsável pelo uso;
- localização;
- categoria do ativo;
- número de patrimônio;
- status operacional;
- histórico de manutenção ou substituições.

A rastreabilidade dos ativos é fundamental para análise de riscos, investigação de incidentes, mitigação de danos e identificação de causas raiz. Divergências ou ausência de registros devem ser tratadas como não conformidade de segurança, devendo ser corrigidas imediatamente.

O processo de respostas aos incidentes de segurança da informação estabelece diretrizes para garantir o tratamento e a resposta adequada a cada tipo de incidente de segurança da informação que possa impactar ativos/serviços de informação ou recursos computacionais da instituição.

Todas as ocorrências que possam vir a ter impacto negativo sobre a confidencialidade, integridade ou disponibilidade das informações/ativos/serviços da Instituição são caracterizadas como um incidente de segurança da informação, devendo as referidas ocorrências serem tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados o mais rápido possível.

Todos os incidentes, ou suspeitas de incidentes, devem ser imediatamente comunicados a equipe de segurança da informação através dos canais disponíveis. Cabe a esta equipe determinar a criticidade do incidente e, quando pertinente, comunicar as partes interessadas (alta administração, colaboradores, clientes, órgãos regulamentadores etc.).

A extensão dos danos do incidente de segurança é avaliada de maneira tempestiva para, em seguida, ser identificado o melhor curso de ação para a resolução completa do incidente e restauração dos ativos de informação afetados. Durante a avaliação são verificados planos de ações previstos. Durante o tratamento os envolvidos devem preservar, quando possível, todasas evidências, para que seja efetuada uma análise de causa raiz.

Meep - Todos os direitos reservados

Identificar o nível real de impacto, vulnerabilidades exploradas, a efetividade do tratamento aplicado e a necessidade de maiores ações para evitar a recorrência do incidente.

Quando completamente tratado, os envolvidos devem preencher o Relatório de Incidente de Segurança da Informação para controle interno, divulgação às partes interessadas e consolidação.

A MEEP possui ainda em suas atividades iniciativas para o compartilhamento com outras instituições de informações sobre incidentes considerados relevantes, sendo que estes abrangem aquelas recebidas de empresas prestadoras de serviços, disponibilizando tais informações igualmente ao BACEN.

A relevância de Incidentes será classificada dentre as escalas de gravidade abaixo, com base nos parâmetros de classificação dos dados e informações atingidos pelo Incidente:

a) Alto: Acima de 10% dos dados afetados

b) Médio: Acima de 2% e Abaixo de 10%

c) Baixo: Abaixo de 2%

6.10. Plano de Continuidade de Negócios

A Instituição adota plano de continuidade de negócios e recuperação de desastres que contempla a alocação de profissionais, os principais processos e ativos de tecnologia e negócio da MEEP.

6.11. Cenários Considerados nos Testes de Continuidade dos Negócios

O processo de gestão de continuidade de negócios relativo à segurança da informação, deve ser implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

Inclui-se no processo referido acima a continuidade de negócios relativos aos serviços de segurança, processamento e armazenamento de dados contratados,

Meep - Todos os direitos reservados

relativo aos cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da MEEP:

I. desastres e catástrofes naturais,

II. indisponibilidade de fornecimento de energia,

III. indisponibilidade de região de provedor de nuvem.

7. PAPÉIS E RESPONSABILIDADES

7.1. Área de Segurança da Informação

a) Responsável por elaborar e validar as diretrizes e princípios de segurança cibernética implementadas na empresa, e garantir que os seus acionistas, diretores, colaboradores, prestadores de serviços e parceiros trabalhem em conformidade com elas.

b) Trabalha em conjunto com o time de tecnologia da informação ("TI") para implementar monitoramentos de acesso e de vulnerabilidades de dependências.

c) Realiza a Gestão de Incidentes de Segurança da Informação, além de:

I. Verificar a conformidade desta Política;

II. Implantar controles de Segurança da Informação de acordo com as diretrizes desta Política;

III. Desenvolver e atualizar, sempre que necessário, as diretrizes gerais para a Gestão de Riscos de Segurança da Informação e Segurança Cibernética;

IV. Registrar, analisara causa e o impacto, bem como controlar os efeitos de incidentes relevantes para as atividades da instituição, bem como abranger informações recebidas de empresas prestadoras de serviços a terceiros;

V. Elaborar diretrizes para coleta e preservação de evidências de incidentes de segurança da informação;

VI. Elaborar/aprovar procedimentos técnicos de tratamento de incidentes de segurança da informação, com apoio das áreas de TI da MEEP;

Meep - Todos os direitos reservados

VII. Implementar melhorias no tratamento de incidentes de segurança da informação;

VIII. Proteger o valor e a reputaçãoda MEEP;

IX. Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicose lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;

X. Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

XI. Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;

XII. Conscientizar, educar e treinar os colaboradores nas suas atividades diárias com foco na Segurança Cibernética;

XIII. Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

7.2. Gestor de Segurança da informação

Atuar como proprietário do Processo de Gestão de Tratamento e Resposta a Incidentes de Segurança da Informação, conforme previsto no Plano de Ação e Resposta a Incidentes.

7.3. Acionistas, Diretores, Colaboradores, Prestadores de Serviços e Parceiros

- Conhecer e cumprir as diretrizes estabelecidas nesta Política.
- Reportar qualquerincidente de Segurançada Informação, mesmo que suposto,o mais rapidamente possível, por meio do canal apropriado.

Meep - Todos os direitos reservados

8. EFETIVIDADE E VIOLAÇÃO

A MEEP promoverá, visando a efetividade da presente política, programa de conscientização em Segurança Cibernética para garantir a disseminação da cultura de Segurança Cibernética e o cumprimento dos objetivos e diretrizes definidos nesta Política, que incluirá treinamentos e avaliações periódicas, levando em consideração as necessidades e responsabilidades específicas de cada acionista, diretor e colaborador e, quando pertinente, de terceiros relacionados à Instituição.

A Instituição garantirá a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

A presente Política de Segurança Cibernética será divulgada ao público, resumidamente, contendo suas linhas gerais, bem como aos destinatários desta Política no âmbito da Instituição e às empresas prestadoras de serviços contratadas pela Instituição, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações.

Todo colaborador é responsável por garantir a segurança cibernética, com o objetivo de evitar que ela possa ser acessada por pessoa não autorizada. Sendo assim, é vedado:

- Expor a MEEP à uma perda monetária efetiva ou perda potencial por meio do comprometimento da segurança de dados ou de informações ou, ainda, por meio da perda de equipamento;
- Revelar dados confidenciais e negociações;
- Usar indevidamente e sem autorização direitos autorais, patentes e dados corporativos;
- Utilizar dados para propósitos ilícitos que violem qualquer lei, regulamento ou seja qual for outro dispositivo governamental.

Todo e qualquer descumprimento a esta Política está sujeito a ações disciplinares. Caso haja conhecimento de alguma violação a este documento, esta deverá ser comunicada imediatamente ao Responsável, por qualquer meio, para a adoção das medidas cabíveis.

Meep - Todos os direitos reservados

Dentre as penalidades aplicáveis, destacam-se a utilização, a critério do Responsável, de advertência, verbalou escrita, suspensão e demissão ou término de vínculo contratual.

Caberá ao responsável a averiguação e monitoramento das comunicações de violação recebidas ou das violações que de qualquerforma houver conhecimento, deliberando sobre as eventuais penalidades disciplinares aplicáveis, incluindo o eventual desligamento imediato de colaborador.

Dada a impossibilidade de prever todas as situações em que os destinatários desta Política possam ser confrontados com questões atinentes à segurança cibernética e da informação, todos são igual e solidariamente responsáveis por evitar tais riscos, devendo agir sempre de forma proativa, íntegra, com bom senso, e, em caso de dúvida, consultar o gestor responsável pela respectiva área.

9. DOCUMENTOS RELACIONADOS

Esta Política deve ser lida e interpretada em conjunto com os seguintes documentos, embora não a limitem em sua abrangência:

- Código de Ética;
- Código de Conduta;
- Política de Conformidade;
- Política de Gestão de Acessos;
- Política de Continuidade do Negócio;
- Política de Governança;
- Política de Proteção de Dados;
- Plano de Resposta a Incidente de Segurança da Informação;

Meep - Todos os direitos reservados

- Plano de Continuidade Operacional;
- Plano de Recuperação de Desastre;
- Plano de Resposta a Incidente de Segurança com Dados Pessoais.

Meep - Todos os direitos reservados

10. ATUALIZAÇÕES E CONTROLE DE REVISÕES DESTA POLÍTICA

Esta Política está sujeita a revisões anuais, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos da MEEP.

A versão atualizada desta Política será publicada na Intranet da MEEP, além de comunicadas para ciência dos Colaboradores, Parceiros e Prestadores de Serviços.

Ainda, no processo de controles internos, é confirmado, via self assessment, se os colaboradores leram e compreenderam a Política, além do Código de Ética e Conduta e as demais Políticas informadas no item 12 desta política, se atentando ao total cumprimento dos procedimentos pertinentes às suas atividades.

REVISÃO		PÁGINAS ALTERADAS	RESPONSÁVEL ALTERAÇÃO	MOTIVO ALTERAÇÃO
Nº	DATA			
1	06/03/2023	2	João Alfredo Barros	Alteração de Razão Social
2	25/07/2024	Todas	João Alfredo Barros	Alteração de Layout, Termos e Definições, ordenação e documentos relacionados
3	05/12/2025	11	Keliane Mendes	Atualização texto – Item 6.8 Continuidade de Segurança da Informação

Meep - Todos os direitos reservados