POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

MULTIPLIKE

Sumário

Objetivo e abrangência:

A Multiplike SCFI reconhece a informação como ativo estratégico e define nesta Política as diretrizes para garantir sua confidencialidade, integridade, disponibilidade e autenticidade, conforme normas do Banco Central, Conselho Monetário Nacional e legislação vigente.

O documento estabelece princípios, responsabilidades e medidas para proteger dados, sistemas e infraestrutura tecnológica, prevenindo e respondendo a incidentes cibernéticos, assegurando a continuidade dos serviços e a segurança dos dados de clientes, colaboradores, parceiros e da instituição.

Aplica-se a todos que acessam ou manipulam informações sob responsabilidade da Multiplike SCFI.

Fundamento Normativo

Esta política está alinhada e estruturada conforme:

- **Resolução CMN nº 4.893/2021** – Política de Segurança Cibernética e requisitos para contratação de serviços de processamento e armazenamento de dados.
- **Resolução CMN nº 4.968/2021** – Sistema de Controles Internos.
- **Lei nº 13.709/2018 (LGPD)** – Lei Geral de Proteção de Dados Pessoais.
- **Lei Complementar nº 105/2001** – Sigilo das operações financeiras.
- Normas e boas práticas internacionais de segurança da informação (ISO/IEC 27001 e 27002).

Princípios de Segurança da Informação

A gestão da segurança da informação e cibernética na Multiplike SCFI observa os seguintes princípios:

1. **Confidencialidade:** garantir que as informações sejam acessíveis apenas a pessoas autorizadas.
2. **Integridade:** preservar a exatidão, completude e consistência das informações.
3. **Disponibilidade:** assegurar que as informações e sistemas estejam acessíveis sempre que necessário.
4. **Autenticidade:** garantir a veracidade da origem da informação e dos acessos realizados.
5. **Responsabilização:** todos os usuários de informações são responsáveis pelo uso adequado e seguro dos dados.
6. **Proporcionalidade e adequação:** os controles devem ser proporcionais à criticidade e aos riscos de cada ativo.

Diretrizes Gerais

Gestão de Ativos e Classificação da Informação

Todos os ativos de informação devem ser identificados, inventariados e classificados conforme sua criticidade e sensibilidade.

A informação deve ser rotulada como Pública, Interna, Confidencial ou Restrita.

Controle de Acesso

O acesso às informações e sistemas será concedido com base no princípio do menor privilégio, de forma individualizada e rastreável.

A gestão de acessos deve incluir processos de concessão, revisão periódica e revogação imediata em casos de desligamento ou mudança de função.

É vedado o compartilhamento de credenciais, senhas ou dispositivos de autenticação, sob qualquer hipótese.

Segurança Lógica e Física

Os ambientes tecnológicos devem possuir controles de autenticação, criptografia, firewall, antivírus e detecção de intrusão.

O acesso físico a áreas restritas deve ser limitado, registrado e monitorado.

Todos os equipamentos utilizados para tratamento de informações da Multiplike SCFI devem estar configurados e protegidos de acordo com padrões definidos pela área de Segurança da Informação.

Gestão de Terceiros e Provedores

A contratação de prestadores de serviços com acesso a informações da Multiplike SCFI exige avaliação prévia de segurança e cláusulas contratuais específicas de confidencialidade, proteção de dados e notificação de incidentes.

As diretrizes complementares constarão no Manual de conheça seu parceiro.

Computação em Nuvem

O uso de ambientes de computação em nuvem deve observar requisitos de segurança, continuidade e privacidade definidos pela área de Segurança da Informação.

Contratação ou alteração de serviços em nuvem devem ser comunicados as entidades regulatórias necessárias dentro do prazo e com informações necessárias.

Todos os provedores devem garantir níveis adequados de criptografia, segregação lógica, conformidade regulatória e acesso a dados e relatórios de auditoria pela Multiplike SCFI

Prevenção e Resposta a Incidentes

A instituição manterá um Plano de Resposta a Incidentes Cibernéticos, abrangendo detecção, comunicação, mitigação e reporte.

Incidentes relevantes devem ser comunicados ao Banco Central do Brasil e, quando envolverem dados pessoais, à ANPD e aos titulares afetados, conforme a LGPD.

Continuidade e Resiliência Operacional

Devem existir planos de contingência, backup e recuperação de desastres testados periodicamente.

Os ambientes críticos devem dispor de redundância e mecanismos de alta disponibilidade.

Conscientização e Capacitação

Todos os colaboradores e terceiros devem participar de treinamentos periódicos de segurança da informação, adequados à sua função e nível de acesso.

Monitoramento e Auditoria

A aderência a esta política será avaliada por meio de controles internos, auditorias e testes periódicos.

Os resultados e planos de ação serão reportados ao setor de Gestão de riscos, controles internos e Compliance e à Diretoria.

Será elaborado anualmente um Relatório de Segurança Cibernética, a ser submetido à Diretoria, contendo efetividade das ações, resultados dos testes de continuidade e incidentes relevantes ocorridos.

Gestão de Riscos Cibernéticos

A gestão dos riscos cibernéticos segue a estrutura estabelecida na Política de Gestão de Riscos da Multiplike SCFI, integrando-se ao processo corporativo de identificação, avaliação e tratamento de riscos operacionais.

Os riscos de segurança da informação devem ser registrados, avaliados e monitorados de forma contínua.

Responsabilidades:

A gestão da segurança da informação e cibernética é uma responsabilidade compartilhada entre a Diretoria, o Responsável pela Segurança da Informação e Cibernética e todos os colaboradores e terceiros que mantenham vínculo com a Multiplike SCFI. Cada um desses agentes desempenha papel essencial na proteção dos ativos informacionais e na manutenção da integridade, confidencialidade e disponibilidade dos dados sob guarda da instituição.

Diretoria

Compete à Diretoria assegurar que a Multiplike SCFI disponha de condições adequadas para a implementação e o cumprimento desta Política, garantindo a aderência às normas do Banco Central do Brasil e às boas práticas de governança.

São responsabilidades da Diretoria:

- Designar formalmente um Diretor responsável pela Política de Segurança da Informação e Cibernética e pela execução do Plano de Resposta a Incidentes.
- Aprovar esta Política e suas eventuais revisões;
- Garantir que os recursos humanos, tecnológicos e financeiros necessários à gestão da segurança da informação estejam disponíveis;
- Avaliar periodicamente os relatórios e indicadores de segurança apresentados pelo Responsável pela Segurança da Informação e Cibernética;

- Deliberar sobre incidentes relevantes de segurança cibernética, inclusive quanto à necessidade de comunicação ao Banco Central do Brasil e outros órgãos competentes;
- Promover a cultura de segurança da informação em todos os níveis da instituição.

Responsável pela Segurança da Informação e Cibernética (RSIC)

O Responsável pela Segurança da Informação e Cibernética é o encarregado pela coordenação técnica e operacional das ações de proteção das informações e dos sistemas tecnológicos da Multiplike SCFI.

São suas atribuições:

- Implementar e manter atualizadas as diretrizes e controles previstos nesta Política;
- Coordenar as atividades de segurança cibernética e de gestão de riscos de tecnologia;
- Garantir que os controles de acesso, classificação e proteção da informação estejam adequados à natureza e criticidade dos dados tratados;
- Conduzir o plano de resposta a incidentes de segurança, promovendo as ações de registro, análise, mitigação e comunicação;
- Elaborar relatórios periódicos sobre o estado da segurança da informação e submetê-los à Diretoria;
- Apoiar tecnicamente as áreas de negócio e demais setores no cumprimento das boas práticas de segurança;
- Promover ações de treinamento e conscientização sobre segurança da informação e cibernética.

Colaboradores

Todos os colaboradores da Multiplike SCFI, independentemente de cargo ou função, são responsáveis por zelar pela proteção das informações às quais têm acesso e por cumprir integralmente as diretrizes desta Política.

Compete a cada colaborador:

- Adotar conduta ética e diligente no uso dos recursos tecnológicos e informacionais da instituição;
- Manter a confidencialidade de informações internas e de clientes;
- Não compartilhar, sob nenhuma hipótese, senhas, credenciais de acesso, dispositivos de autenticação ou informações de segurança.
- Comunicar imediatamente ao Responsável pela Segurança da Informação qualquer incidente, falha ou suspeita de violação de segurança;
- Participar dos treinamentos e ações de capacitação promovidos pela instituição.

Terceiros e Prestadores de Serviços

Os prestadores de serviços e demais terceiros que, por força contratual, tenham acesso a informações ou sistemas da Multiplike SCFI, devem observar as mesmas exigências de segurança aplicáveis aos colaboradores internos.

São responsabilidades dos terceiros:

- Cumprir as cláusulas de confidencialidade, sigilo e segurança constantes nos contratos firmados;
- Utilizar as informações recebidas exclusivamente para os fins previstos na relação contratual;
- Adotar medidas de proteção compatíveis com as práticas e padrões definidos pela Multiplike SCFI;
- Comunicar imediatamente à instituição qualquer ocorrência ou incidente que possa comprometer a segurança da informação.

Sanções e Responsabilidades

O descumprimento das disposições desta Política constitui falta grave, sujeitando o infrator às medidas disciplinares previstas nas normas internas, sem prejuízo das responsabilidades civis, administrativas e penais cabíveis.

Revisão e Vigência

Esta Política será revisada anualmente ou sempre que houver alterações significativas no ambiente regulatório, tecnológico ou organizacional.

Sua revisão será coordenada pelo Responsável pela Segurança da Informação e aprovada pela Diretoria.