Índice

---

1. OBJETIVO

A informação é um dos patrimônios mais importantes a ser preservado pela instituição. Assim, a GETMONEY CÂMBIO estabelece a presente política, a fim de orientar e garantir a aplicação das diretrizes estratégicas e princípios para proteção dos ativos tangíveis e intangíveis da Instituição, dos clientes e interesses do público em geral.

Ainda, é objetivo desse normativo atender às leis e normas regulamentadoras do mercado, principalmente no tocante a Resolução nº 4.658/2018 do Banco Central do Brasil, fazendo com que se torne parte da cultura de segurança cibernética, por meio de programas de capacitação, prestação de informações à clientes e usuários sobre precaução na utilização de produtos e serviços e o comprometimento da Alta Administração com a melhoria contínua dos procedimentos.

A GETMONEY CÂMBIO estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

- Proteger o valor e a reputação da empresa;
- Garantir a confidencialidade, integração e disponibilidade das informações da GETMONEY, e de informações de terceiros por ele custodiados, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidade nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;
- Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
- Conscientizar, educar e treinar os colaboradores por meio de Política de Segurança Cibernética, normas e procedimentos internos aplicáveis as suas atividades diárias;
- Estabelecer e melhorar continuamente um processo de Gestão de Riscos de Segurança Cibernética.

2. Importância da Segurança da Informação

Os pilares da segurança da informação nos dão subsídios para proteger as informações da GETMONEY CÂMBIO. Portanto, quando mencionamos "segurança da informação" estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, clausulas e demais questões que juntas formam a proteção adequada para qualquer empresa.

O que é política de Segurança da Informação?

É um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos profissionais em relação à segurança dos

recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável.

A informação é só o que está nos sistemas?

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo.
Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, documentos na mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas ao nosso meio.

3. Princípios da Segurança da Informação

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

- **Confidencialidade:** Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.
- **Integridade:** garantia da veracidade da informação, pois a mesma não deve ser alterada, enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.
- **Disponibilidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu

correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

- **Acesso controlado:** O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece quando há descuido ou possível quebra de confidencialidade das senhas de acesso.

4. Público-alvo

Está política visa atender o público geral, especialmente clientes e parceiros, administradores, gestores, colaboradores, estagiários e prestadores ou fornecedores de serviços que se relacionam com a GETMONEY CÂMBIO, direta ou indiretamente.

5. Regras de uso da tecnologia

- Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na GETMONEY CÂMBIO ou para outras situações formalmente permitidas.
- Quando o usuário se comunicar através de recursos de tecnologia da GETMONEY CÂMBIO, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da empresa.
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia da GETMONEY CÂMBIO devem ser legais, e devem contribuir para as atividades profissionais do usuário.
- Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas instalados.
- Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de riscos e controles internos.

6. PROCEDIMENTOS E CONTROLES

As violações das Políticas e procedimentos de segurança da GETMONEY CÂMBIO, após apuração e constatação de responsabilidades, poderão desencadear ações disciplinares, rescisão de contrato de trabalho e medidas administrativas/judiciais cabíveis.

7. COMPROMISSO DE SIGILO E CONFIDENCIALIDADE

Terceiros e parceiros deverão assumir o dever de sigilo, por si, seus empregados, prepostos ou terceiros sob suas ordens e efetuar uso, com prévia autorização, das informações críticas sobre todos os processos de negócio da GETMONEY CÂMBIO.

8. CONTRATAÇÃO DE FORNECEDORES E PRESTADORES DE SERVIÇOS

A contratação de fornecedores deverá observar diretrizes internas, a fim de assegurar a contratação de fornecedores parceiros idôneos, de boa conduta social, ambiental e ética, que incentivem adoção de boas práticas, bem como contratar bens e serviços por preções coerentes praticados pelo mercado.

Caso o serviço a ser contratado utilize armazenamento de dados relevantes em nuvem, após procedimento interno de averiguação, deverá haver a comunicação ao Banco central do Brasil, em até 60 dias antes do início da prestação do serviço, coforme preceitua a Resolução nº 4658/2018.

9. PROTEÇÃO CONTRA VÍRUS E SOFTWARES MALICIOSOS

Servidores, estações de trabalho ou notebook, deverão ser protegidos por software de antimalware homologado pela Instituição. As estações de trabalho serão gerenciados pelos administradores, impossibilitando que o colaborador desabilite os softwares de proteção.

10. CÓPIA DE PROTEÇÃO (BACKUP)

A área de tecnologia da informação realizará controle de backup, estabelecendo dados a serem copiados e a periodicidade de retenção, a fim de garantir a recuperação em caso de

falha ou desastre e ainda atender requisitos legais e fiscais. O armazenamento deverá ser efetuado com a identificação de cada mídia, data do backup e tempo de retenção.

11. USO DA REDE CORPORATIVA

Os usuários autorizados possuem acesso à rede corporativa para disponibilidade e armazenamento de arquivos pertinentes ao negócio, devendo o acesso ser tratado conforme classificação de informação e não como informação particular. O acesso deverá ser realizado de forma a atender normas internas.

12. MONITORAMENTO

Com o objetivo de identificar atividades não autorizadas, os sistemas e recursos de rede são monitorados e os eventos de segurança analisados.

13. CONTROLE DE ACESSO

O acesso a informações, serviços de rede e aplicações são controlados visando evitar o acesso indevido. Existem regras para controle de acesso, considerando as permissões de acordo com a sensibilidade da informação. A Getmoney possui procedimentos formais, que são passíveis de controle e auditoria. Toda violação de acesso identificada deve ser registrada e analisada pelas áreas responsáveis.

14. GERENCIAMENTO DE SENHAS DE ACESSO

A senha de autenticação é a forma de certificar a identificação do usuário .

15. DIRETRIZES CORPORATIVAS

O cumprimento da Política Corporativa de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, os quais devem obedecer as seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela GETMONEY;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Atender às leis que regulamentam as atividades da GETMONEY e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Comunicar imediatamente à área de Segurança Cibernética, quaisquer descumprimentos da Política Corporativa de Segurança Cibernética.

16. GESTÃO DE VULNERABILIDADES

Os procedimentos e controles adotados para reduzir a vulnerabilidade dos incidentes na Instituição e demais quesitos, determinam a necessidade de adoção de diretrizes para correção de fragilidade, que deverão ser instalados em todos os componentes de sistema, estações de trabalho, servidores ou dispositivos de rede adotados pela instituição.

17. RESPOSTA A INCIDENTES DE SEGURANÇA

A resposta aos incidentes deverá ser tratada de forma a limitar os danos e minimizar o tempo e os custos de recuperação, que envolve um método organizado para lidar com as consequências de um ataque contra a segurança de um sistema computacional.

O processo de resposta aos incidentes de segurança compreende: detecção, triagem e análise, mitigação, investigação, resposta e educação.

As tratativas dos incidentes deverão ocorrer, ressalvadas as características principais e considerando os quesitos de origem, vulnerabilidade, criticidade, impacto e ativo alvo. Não obstante, deverão ser observadas os tipos de severidades – média e baixa, alta ou severidade crítica.

18. COMPARTILHAMENTO DE INFORMAÇOES SOBRE OS INCIDENTES RELEVANTES

Exceto em casos que exigem sigilo de informações estratégicas para o negócio, será adotado o padrão de soluções de ferramentas disponibilizadas ou sugeridas pela associações das quais a GETMONEY CÂMBIO faz parte para que o compartilhamento de incidentes seja eficiente e garanta a assimilação do processo.

19. ESTRUTURA DE GERENCIAMENTO

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos pela Política de Segurança Cibernética.

19.1. Gestão de acessos às informações

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégio possíveis, revistos periodicamente com a aprovação do gestor responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

19.2. Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração

segura de redes de comunicações, incluindo a gestão de séricos contratados de processamento e armazenamento de dados e informações em nuvem.

19.3. Segurança Física e Lógica

Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores e terceiros da GETMONEY são treinados periodicamente sobre os conceitos de Segurança da Informação, através de um programa efetivo de conscientização.

19.4. Continuidade de negócios

Os procedimentos e a metodologia adotados peça Instituição serão base para as simulações de teste de continuidade de negócio, a fim de garantir a confidencialidade, integridade e disponibilidade dos serviços contratados em nuvem. Neste sentido, as áreas de Tecnologia e Segurança da Informação deverão garantir a continuidade e recuperação nos serviços de nuvem contratados, além do gerenciamento das interrupções que possam ocorrer.

19.5. Processamento, armazenamento de dados e computação em nuvem

Conforme a Resolução 4.658/2018 do Banco Central do Brasil, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a GETMONEY, assegura-se um procedimento efetivo para aderência às regras previstas na regulamentação em vigor.

20. CONFORMIDADE

Visando assegurar a inexistência de irregularidade nas atividades executadas pela GETMONEY CÂMBIO, deverão ser tomados os devidos cuidados para atendimento à conformidade com os requisitos de negócio, leis civis, contratuais e regras de segurança.

21. Mecanismos para disseminação da cultura de segurança cibernética na instituição:

A GETMONEY CÂMBIO, periodicamente, proverá treinamento de conscientização de segurança aos colaboradores, com apoio e envolvimento da Alta Administração.

22. Divulgação da política de segurança cibernética

22.1. A política de segurança cibernética deve ser divulgada aos funcionários da instituição e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, sendo comprovado através de e-mail ou protocolo de recebimento.

22.2. A divulgação ao público será através de resumo contendo as linhas gerais desta.

23. COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o endereço de e-mail: segurancacibernetica@getmoney.com.br.