MANUAL DE CONTROLES INTERNOS DE SEGURANÇA

VERSÃO: SETEMBRO 2018

GoMoney.me

Sumário

1. INTRODUÇÃO

Este Manual de Controles Internos de Segurança ("Manual de Segurança") especifica os controles internos aplicáveis à segurança e ao sigilo da informação e à continuidade dos negócios da GoMoney Serviços Digitais ME (“GOMONEY”), com o objetivo de prover a segurança necessária para realização de suas operações, ainda que em situações adversas.

O presente Manual foi elaborado e deve ser interpretado em consonância com os demais manuais e políticas da GOMONEY, e deve ser revisado e atualizado anualmente pela área de Compliance, com o apoio da de Tecnologia, a fim de incorporar medidas relacionadas a atividades e riscos novos ou anteriormente não abordados.

Estão sujeitos ao disposto no presente documento, todos os colaboradores da GOMONEY, independente do departamento e cargo em que trabalhem, sendo sua obrigação conhecer a versão mais recente na íntegra do documento.

O presente Manual de Segurança está dividido em 03 (três) capítulos que cobrem, respectivamente, a segurança das informações (a "Política de Segurança das Informações"), o sigilo das informações (a "Política de Sigilo das Informações") e a continuidade dos negócios (o "Plano de Continuidade dos Negócios).

2. DEFINIÇÕES

Para o perfeito entendimento deste Manual, faz-se necessário definir o significado de alguns termos mencionados, são eles:

Antivírus: programa que detecta e elimina vírus de computador.

Ativos: todo e qualquer bem material pertencente ou geridos pela GOMONEY, que podem ser:

Ativos de informação: base de dados e arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas, etc.

Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.

Ativos físicos: equipamentos computacionais (computadores, processadores, monitores, laptops, modems, etc), equipamentos de comunicação (roteadores, PABX, telefones fixos, etc), mídias (fitas e discos magnéticos, discos ópticos, etc), outros equipamentos técnicos (no-breaks, aparelhos de ar-condicionado, etc), mobília, acomodações, etc.

Backup: cópia exata de um programa, disco ou arquivo de dados feito para fins de arquivamento ou para salvaguardar informações.

Blockchain: sistema de registros coletivo, descentralizado/distribuído e imutável, utilizado, entre outros fins, para validar e registrar transações envolvendo criptomoedas.

Cavalo de Tróia: programa que pode danificar áreas da máquina e torná-la vulnerável ao ataque de hackers.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Controle de Acesso: conjunto de restrições ao acesso às informações de um sistema exercido pela equipe de segurança da informação.

Criptografia: arte/ciência de utilizar matemática para tornar a informação segura, criando um grande nível de confiança no meio eletrônico.

Direito de Acesso: privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Download: transferência de arquivo de um computador remoto para outro computador através da rede.

Ferramentas: conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades.

Handheld: computadores que cabem na palma da mão (palmtops) e que tem recursos para organização pessoal e comunicação móvel.

Incidente de Segurança: qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo.

Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

Junk mail: e-mails não solicitados por usuários não interessados em recebê-los. Log: registro das transações ou atividades realizadas em sistema de computador.

No-Break: sistema com baterias, que mantém o computador funcionando por um determinado período.

Peer-to-Peer: rede por meio da qual usuários compartilham entre si seus recursos, possibilitando a provisão de conteúdo e serviços à rede.

Plataforma: conjunto de tecnologias, sistemas, banco de dados, interfaces, site, e demais soluções gerenciadas internamente pelo GOMONEY, por onde são realizadas as transações de compra, transferência e venda de GMCs(moeda virtual);

Política de Segurança: conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos sistemas de informação.

Proteção dos Ativos: processo pelo qual os ativos devem receber classificação quanto ao respectivo grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém.

Segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação.

Senha Fraca ou Óbvia: senha que utiliza caracteres de fácil associação ao seu dono, que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome do usuário, nome de seus familiares, sequências numéricas simples, palavras com significado, dentre outras.

Spam: e-mail não solicitado enviado a grande número de endereços eletrônicos, que geralmente visam fazer propaganda de produtos e serviços.

Usuário: código/conta exclusivo que, juntamente com a respectiva senha, possibilita o modo de acesso à plataforma GOMONEY.

Vírus: programa construído para causar danos aos softwares do computador.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Esta Política tem como objetivos:

a) **Permitir que a GOMONEY atenda à regulamentação, legislação e autorregulação aplicáveis;**

b) **Manter o nível de segurança da organização em um patamar definido como adequado pela GOMONEY;**

c) **Garantir que as diretrizes explicitadas nesta Política sejam praticadas, por meio da implementação de controles que visam garantir a confidencialidade, a integridade e a disponibilidade das informações.**

Para atingir este objetivo, a GOMONEY estabelece a presente Política como um dos pilares de sua estratégia de segurança, que deve ser seguida e implementada para garantir que os dados compartilhados por meio de suas plataformas sejam protegidos.

A Política de Segurança da Informação se define como um documento que expressa a posição da organização sobre a segurança, quais são seus valores e direcionamentos para minimizar os riscos sobre suas atividades e seus Usuários. Desta forma ela estabelece a linha mestra de atuação da GOMONEY em relação a todos os aspectos da segurança da informação, incluindo equipamentos, bens, informações e pessoas.

A Política de Segurança da Informação tem como princípios assegurar a:

Identificação: garantir que qualquer indivíduo seja identificado unívoca e inequivocamente, independente da privacidade com que suas informações são tratadas;

Confidencialidade: garantir que as informações sejam acessadas apenas por aqueles expressamente autorizados;

Integridade: preservar a integridade das informações, salvaguardando-as contra ações não autorizadas e garantindo que todas as informações estejam exatas e completas durante a sua criação, uso, guarda e destruição;

Disponibilidade: garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

Com a finalidade de assegurar que os princípios acima sejam observados, a GOMONEY desenvolve as seguintes atividades:

- ✓ Classificação da informação:
  - Controle de acesso às informações;
  - Rastreamento e monitoramento das operações de 100%(cem por cento) de seus Usuários,
- ✓ Avaliação de risco:
  - Segurança física dos dispositivos onde é armazenada e por onde transita a informação.
- ✓ Testes de segurança e de continuidade dos negócios.

Este documento serve como um guia de melhores práticas definida pela GOMONEY em relação à segurança da informação e tem o propósito de oferecer uma base comum de atuação para ser usado por aqueles que são responsáveis pela criação, implementação e manutenção de processos, procedimentos, sistemas, tecnologias, conhecimento, estratégias, serviços, campanhas e quaisquer outros ativos que compõem o dia-a-dia da GOMONEY. A empresa tem como compromisso assegurar que as orientações definidas neste documento sejam seguidas por toda a organização.

Esta Política se aplica aos colaboradores e Ativos descritos abaixo:

Colaboradores: todas as pessoas que, de alguma forma, prestem serviços para a GOMONEY, sejam elas diretores, empregados, estagiários ou terceiros contratados. Todos devem dar cumprimento às regras definidas nesta Política de Segurança da Informação.

Ativos: todo equipamento, instalação, sistema e informações, bem como a quaisquer outros bens, tangíveis ou intangíveis, de propriedade ou geridos pela GOMONEY. Da mesma forma, se aplica a todas as plataformas de hardware e a todos os sistemas operacionais e aplicativos utilizados. Aplica-se também a qualquer meio onde a informação possa ser armazenada, incluindo mídias magnéticas, discos ópticos, “nuvens” de armazenamento, informações impressas em papel e material de marketing.

Antes de efetuar ações que envolvam acesso, uso, alteração, armazenamento, transmissão, destruição ou qualquer outra atividade envolvendo Ativos da empresa, o usuário deve consultar esta Política para certificar-se de que a atividade é permitida. Toda e qualquer atividade que não seja claramente permitida é proibida. Em caso de dúvida o usuário deve consultar a área de Compliance e o responsável pela Tecnologia para assegurar-se que a atividade seja permitida.

Cabe ao responsável pela Tecnologia e a área de Compliance avaliar os riscos das atividades não previstas nas diretrizes de segurança da empresa.

3.1. PRIVACIDADE

Todos os Ativos pertencem à GOMONEY e, portanto, a GOMONEY tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede ou ''nuvem'', que se encontrem fisicamente no mobiliário da empresa, como, por exemplo, em mesas, estantes, gaveteiros, armários, etc. Dessa forma, ainda que o colaborador possa se utilizar da estrutura de tecnologia da empresa para algum uso particular não conflitante, tais informações podem ser acessadas pela GOMONEY mesmo sem o prévio consentimento do respectivo colaborador.

3.2. DEVERES E RESPONSABILIDADES

São deveres de todos os colaboradores no âmbito desta Política:

- ✓ Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
- ✓ Cumprir a presente Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
- ✓ Utilizar os Sistemas de Informações e os recursos relacionados somente para os fins previstos pela área de Tecnologia;
- ✓ Cumprir as regras específicas de proteção estabelecidas aos Ativos de informação;
- ✓ Manter o caráter sigiloso da senha de acesso aos recursos e sistemas;
- ✓ Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
- ✓ Responder por todo e qualquer acesso aos recursos da empresa, bem como pelos efeitos decorrentes de acesso efetivado através de seu código de identificação, ou outro atributo para esse fim utilizado;
- ✓ Solicitar acesso a informações restritas somente quando houver real necessidade de acessar o recurso;

- ✓ Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, sob pena de violação da legislação de propriedade intelectual pertinente;

- ✓ Comunicar a área de Compliance o conhecimento de qualquer irregularidade ou desvio verificado no âmbito da presente Política.

3.3. Responsabilidade dos Gestores de Áreas

- ✓ Gerenciar o cumprimento desta Política, por parte de seus funcionários e prestadores de serviço;

- ✓ Proteger os ativos de informação e de processamento da GOMONEY;

- ✓ Inobstante a natureza de anonimato aplicável às criptomoedas, assegurar que 100% (cem por cento) de seus Usuários sejam identificados e rastreados.

3.3.1. Responsabilidades da Área de Tecnologia

- ✓ Estabelecer as regras de proteção dos ativos da GOMONEY;

- ✓ Revisar frequentemente as regras de proteção estabelecidas;

- ✓ Restringir e controlar o acesso e privilégios de usuários remotos e externos;

- ✓ Auxiliar a área de Compliance a elaborar e a manter atualizado o Plano de Contingência e Continuidade dos Negócios;

- ✓ Executar as regras de proteção estabelecidas por esta Política;

- ✓ Detectar, identificar, registrar e comunicar à chefia violações ou tentativas de acesso não autorizadas;

- ✓ Excluir ou desabilitar os perfis inativos;

- ✓ Garantir o cumprimento do procedimento de Backup para os servidores e ativos;

3.3.2. Responsabilidades da Área de Compliance

- ✓ Assessorar a GOMONEY na elaboração e verificação da legalidade de eventuais regulamentos, termos, políticas e controles utilizados para proteger os Ativos de informação;

- ✓ Liderar o processo de apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de segurança da informação aos regulamentos internos e externos da GOMONEY, ainda que auxiliado pela área de Tecnologia;

- ✓ Assegurar que as atividades da GOMONEY sejam desenvolvidas com base nos princípios estabelecidos em seus manuais/políticas internos e em consonância com a regulamentação, legislação e autorregulação aplicáveis;

- ✓ Monitorar os perfis dos Usuários de forma que, independente da natureza de anonimato aplicável às criptomoedas, 100%(cem por cento) de seus Usuários possam ser identificados e rastreados.

3.4. Uso dos Recursos de Informática

3.4.1. Uso do e-mail

O uso do e-mail na GOMONEY está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. Com isso em vista, seguem as regras que devem ser observadas por todos os colaboradores quando da utilização desta ferramenta:

- ✓ O usuário é o único responsável pelo conteúdo das transmissões feitas através do e-mail a partir de sua senha ou conta;

- ✓ As mensagens de e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela;

- ✓ Não devem ser abertos arquivos ou executados programas anexados aos e-mails sem antes verificá-los com um antivírus;

- ✓ Devem estar desligadas as opções que permitam abrir ou executar automaticamente arquivos ou programas anexados às mensagens;

- ✓ Não deve ser utilizado e-mail, plataformas e redes sociais da GOMONEY, para fins ilegais;

- ✓ Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço;

- ✓ Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual;

- ✓ Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis;

- ✓ O colaborador não pode obter ou tentar obter acesso não-autorizado às plataformas da GOMONEY, sistemas ou redes de computadores conectados ao serviço;

- ✓ Não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

3.5. Backup e Restauração de Sistemas

A importância dos backups na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

O backup dos servidores é executado pela equipe de Tecnologia da Informação responsável pelo mesmo.

3.6. Notificações de Incidentes de Segurança

Qualquer suspeita de ocorrência de incidente de segurança deve ser informada à área de Tecnologia. Nenhum colaborador deve investigar por conta própria ou tomar ações para se defender de eventual ataque, a não ser que seja instruído desta forma pela área de Tecnologia. A área de Tecnologia está capacitada para conter as exposições, analisar os impactos à GOMONEY e conduzir investigações, coletando evidências para possíveis ações jurídicas.

4. Política de Sigilo da Informação

Esta Política de Sigilo das Informações tem os seguintes objetivos:

a) expor as normas e procedimentos de proteção do sigilo das informações, em cumprimento das determinações legais aplicáveis, em especial às normas que tratam do sigilo bancário que são adotadas por analogia pela GOMONEY;

b) evitar a divulgação de dados e informações sobre as operações passivas (resgate) e ativas (aquisição) da GOMONEY, de forma a mantê-las sob sigilo;

c) determinar as condições em que dados e informações sobre as operações passivas e ativas da GOMONEY podem ser reveladas a terceiros.

A aplicação e monitoramento da Política de Sigilo das Informações cabe à area de Compliance, obedecidas as especificações adiante elencadas:

a) São informações confidenciais da GOMONEY (as "Informações Confidenciais") que não devem ser disponibilizadas em domínio público ou a terceiros:

Operações, estratégias, resultados, ativos, dados e projeções relativos às operações ativas e passivas da GOMONEY, dados de seus Usuários e suas plataformas em especial aqueles que possam levar a uma vantagem competitiva da GOMONEY frente a seus concorrentes;

- ✓ informações sobre os planos de negócios da GOMONEY;
- ✓ informações confidenciais sobre Usuários das plataformas da GOMONEY;

Independente da natureza de confidencialidade das informações disponibilizadas pelos Usuários das plataformas, a GOMONEY assegura que possui as ferramentas e controles necessários que possibilitam o rastreamento e identificação de 100% (cem por cento) de seus Usuários.

5. PLANO DE CONTINUIDADE DOS NEGÓCIOS

A GOMONEY, em atendimento, por analogia, à regulamentação em vigor e às boas práticas no desenvolvimento de suas atividades formulou o presente Plano de Continuidade dos Negócios (“Plano”), que tem por objetivo nortear a forma de identificar, prevenir e atuar em momentos de contingência, definindo as áreas prioritárias e procedimentos para garantir a continuidade do negócio.

A área de Compliance deve se certificar da implementação do Plano para garantir a continuidade das atividades da GOMONEY em casos de eventos inesperados que afetem parte ou a totalidade

da capacidade operacional da GOMONEY, assegurando a realização de testes periódicos que atestem sua efetividade.

Dentre os principais eventos a serem considerados, podem ser verificados os seguintes:

a) incêndio;
b) alagamento;
c) sabotagem;
d) terrorismo/pirataria;
e) furacão;
f) desordem civil;
g) roubo;
h) falta de energia;
i) falha aleatória de sistema crítico para a GOMONEY.

5.1. Modelo de atividade, infraestrutura e necessidades do negócio

A GOMONEY é uma *Fintech* consubstanciada na oferta das chamadas criptomoedas ou moedas digitais, por meio de suas plataformas digitais.

5.1.1. Infraestrutura física e tecnológica (continuidade das atividades realizadas cotidianamente)

A GOMONEY utiliza, em todos os seus servidores, rotinas diárias de backup e de contingência. Além disso, todas as transações de GMC(moeda digital) realizadas são registradas no Blockchain.

Esse procedimento garante aos Usuários que suas informações e transações sejam tratadas e armazenadas sob total sigilo e anonimato de forma que as mesmas somente possam ser identificadas e rastreadas pela GOMONEY.

6. Considerações Finais

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar a área de Compliance.

Este documento é de uso interno, porém, em alguns casos pode ser disponibilizado a terceiros mediante prévio consentimento da área de Compliance, sendo certo que o respectivo envio deve ser realizado exclusivamente em meio físico ou em formato ".pdf", (documento protegido), contendo os devidos disclaimers de confidencialidade.

A expectativa da alta administração da GOMONEY é que em até 12 (doze) meses a contar da data de última revisão deste documento, todos os controles e estruturas aqui citados já estejam em vigor em caráter efetivo(quando aplicáveis), sendo certo que alguns deles já estão em pleno funcionamento nesta data. Vale ressaltar, finalmente, que alguns procedimentos, no momento, não são aplicáveis nem exigidos à GOMONEY tendo em vista a ausência de regulação, número de Colaboradores ou tipo de operações e serviços ofertados aos seus Usuários. No entanto, é nosso compromisso implementa-los tão logo tal quadro renove-se ou altere suas características atuais.

Documento elaborado e revisado sob supervisão jurídica de Massini Advocacia, OAB/SP nº 27223