ASSUNTO	**POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E SEGURANÇA CIBERNÉTICA**
ÁREAS RESPONSÁVEIS	*Compliance* e Tecnologia da Informação

HISTÓRICO DE VERSÕES

Versão	Motivo da Alteração	Data
1	Versão Revogada	-
2	Versão Aprovada	31/08/2017
3	Versão Atualizada	05/02/2019

SUMÁRIO

1. OBJETO

A informação é um dos bens mais valiosos de qualquer organização, independentemente do setor que atue. Dentro do mercado financeiro, esta importância é potencializada, uma vez que os processos e produtos deste setor se baseiam na qualidade da informação. Diante deste panorama, a **SOMMA Investimentos S/A ("SOMMA Investimentos"),** em cumprimento ao Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, estabelece a presente **Política de Segurança das Informações e Segurança Cibernética ("Política")**. A SOMMA Investimentos entende que a adequada proteção das informações é um dos indicadores do seu compromisso com seus ideais de sustentabilidade e perenidade, reforçando sua estrutura de Governança Corporativa, garantindo a aplicação dos princípios

de proteção de todas as informações relativas tanto à organização em si quanto à de seus clientes e parceiros.

Esta Política tem como objetivo fazer jus à confiança de seus clientes e públicos de interesse e fortalecer sua imagem de instituição reconhecidamente sólida, ética e confiável.

2. ABRANGÊNCIA

A presente política é aplicável a todos aqueles que possuam cargo, função, posição e/ou relação, societária, empregatícia, comercial, profissional, contratual ou de confiança **("Colaboradores")** da SOMMA Investimentos.

3. PRINCÍPIOS

São seguidos os seguintes princípios para garantir a segurança da informação:

a) **Confidencialidade:** consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação, buscando assegurar que as pessoas não tomem conhecimento das informações, de forma acidental ou proposital, sem autorização prévia;
b) **Integridade:** consiste na fidedignidade de informações, na conformidade de dados armazenados em relação às inserções, alterações e processamentos autorizados, pressupõem-se a garantia da não violação dos dados com intuito de alteração, gravação ou exclusão, seja acidental ou proposital;
c) **Autenticidade:** consiste na garantia da veracidade da fonte da informação, sendo através da autenticação que se confirma a identidade da pessoa ou entidade que presta as informações; e
d) **Disponibilidade:** consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento em que for requerido, durante o período acordado.

4. PROTEÇÃO DAS INFORMAÇÕES

4.1 Classificação

A SOMMA Investimentos classifica as informações de acordo com o grau de importância, prioridade e nível de proteção necessária. Para isso, leva em consideração as necessidades de compartilhamento ou restrição de acesso e impactos da utilização das informações, sempre avaliadas tendo em vista o *core business.*

Considera-se os seguintes critérios, quanto ao nível de confidencialidade da informação:

a) **Pública:** é toda informação destinada ao público externo ou divulgada em cumprimento a legislação. Possui caráter informativo, como material de marketing, registro regulamentares.
b) **Interna:** é toda informação destinada ao uso interno da SOMMA Investimentos. Sua divulgação não afetaria significativamente a SOMMA Investimentos e seus clientes. Pode ser acessada, sem restrições, por todos os Colaboradores, não possuindo proteção especial.
c) **Confidencial:** é toda informação destinada também para uso interno, mas a sua divulgação não autorizada poderia acarretar em prejuízo financeiro, de imagem, operacional ou sanções administrativas, civis e criminais à SOMMA Investimentos, aos seus clientes e Colaboradores. É sempre restrita à um grupo específico de pessoas, podendo ser composto por empregados, clientes e/ou fornecedores.
d) **Restrita:** é toda informação acessível somente por Colaboradores autorizados explicitamente. A divulgação não autorizada poderá causar danos e/ou comprometer a estratégia de negócio da SOMMA Investimentos. As pessoas autorizadas para o acesso desta informação têm a responsabilidade de garantir sua proteção e armazenamento quanto não tiverem em uso.

4.2 Informação à Mídia, Público e Governo

Somente os Colaboradores autorizados podem falar em nome da SOMMA Investimentos. As informações provenientes de órgãos reguladores, fiscalizadores e agências de *rating* deverão ser encaminhadas a área de *Compliance,* as demais deverão ser encaminhadas a área de Comunicação.

4.3 Controle de Informações Privilegiadas

A informação alcançada em função da atividade profissional desempenhada não pode ser transmitida de forma alguma à terceiros não Colaboradores ou à Colaboradores não autorizados. Neste item, incluem-se as posições compradas ou vendidas, estratégias e conselhos de investimento ou desinvestimento, relatórios, análises e opiniões sobre ativos financeiros, dados a respeito de resultados financeiros de fundos geridos, transações efetuadas e que ainda não foram publicadas. Também se considera informação privilegiada aquela oriunda de estudo realizado pela SOMMA Investimentos, mesmo que os ativos não componham nosso portfólio.

Quanto à confidencialidade e tratamento da informação, o Colaborador deve cumprir o estabelecido nos itens a seguir:

i. Informação Privilegiada:

É qualquer informação importante a respeito de alguma empresa que não tenha sido publicada e que seja obtida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com Colaboradores de empresas estudadas ou investidas ou com terceiros, ou da condição de funcionário. São alguns exemplos de informações privilegiadas: informações verbais ou documentais referentes à resultados operacionais da empresa, alterações societárias, informações sobre compra e venda de empresas, títulos ou valores mobiliários, entre outros acontecimentos caracterizáveis como confidencial de uma empresa com a SOMMA Investimentos ou com terceiros.

Estas informações precisam ser mantidas em sigilo por todos que as acessarem. O Colaborador que tiver acesso à uma informação privilegiada deverá comunicar seu acesso ao seu superior, não podendo comunicá-la a outros Colaboradores, profissionais de mercado, amigos e parentes, tampouco usá-la em benefício próprio ou de terceiros. Caso não haja certeza quanto ao caráter privilegiado da informação, o Colaborador deve se reportar rapidamente à área de *Compliance*.

ii. *Insider Trading* e "Dicas":

Insider Trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício para si ou terceiros (compreendendo a própria SOMMA Investimentos e seus Colaboradores). Já "Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada como benefício na compra e venda de títulos e valores mobiliários.

É proibida a prática dos casos supracitados por qualquer Colaborador, sendo os indícios de prática analisados não só durante a vigência do relacionamento profissional junto a SOMMA Investimentos, como após o seu término, com a comunicação às autoridades, conforme o caso.

A área de *Compliance* é o responsável por verificar e processar, no mínimo trimestralmente, as notificações recebidas pelo Comitê de *Compliance* a respeito do uso de informações privilegiadas e de *Insider Trading* pelos Colaboradores.

4.4 Política de Confidencialidade

Toda informação obtida pelos Colaboradores no exercício de suas funções profissionais deve ser considerada confidencial, sendo vedada a transmissão a terceiros não Colaboradores ou Colaboradores não autorizados. É vedado, ainda, aos Colaboradores fazerem cópias ou imprimir os arquivos utilizados, gerados

ou disponíveis na rede da SOMMA Investimentos, bem como circular com estes documentos em ambientes externos. Com exceção de cópia e impressão de arquivos necessários em prol da execução e do desenvolvimento dos negócios e dos interesses da SOMMA Investimentos e seus clientes. Neste caso, o Colaborador que estiver em posse e guarda da cópia ou impressão será responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Qualquer informação de natureza confidencial relativa às atividades da SOMMA Investimentos, seus sócios e clientes, somente poderão ser compartilhadas*:*

a) Em caso necessidade para a condução dos negócios;
b) Com empresas que sejam necessárias para atender seus clientes, ex-clientes ou potenciais clientes;
c) Com órgãos reguladores e autorreguladores; e
d) Quando for exigido por Lei, Norma, Regulamento, Ordem Judicial emitida por Tribunal de jurisdição competente ou órgão do Judiciário, Executivo ou Legislativo.

4.5 Acordo de Confidencialidade

A SOMMA Investimentos firmará acordos de confidencialidade com terceiros, nos quais se comprometerá a manter a confidencialidade das informações recebidas por estes. A ruptura deste acordo poderá ter consequências severas a SOMMA Investimentos e/ou seus Colaboradores.

5. SEGURANÇA CIBERNÉTICA

A SOMMA Investimentos tem ciência do risco cibernético a qual está exposta, visto o aumento exponencial das ameaças e ataques cibernéticos dos últimos anos, entre eles encontram-se os métodos considerados como comuns:

a) *Malware* – softwares desenvolvidos para corromper computadores e redes, como:
    i. Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
    ii. Cavalo de Tróia: aparece dentro de outro software e cria uma porta para invasão do computador;
    iii. *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
    iv. *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um pagamento financeiro para que o acesso seja reestabelecido.
b) Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas e dados pessoais, entre os quais destacam-se:
    i. *Pharming:* direciona o usuário para um site fraudulento sem o seu conhecimento;
    ii. Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
    iii. *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
    iv. *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens e texto, tenta obter informações confidenciais; e
    v. Acesso pessoal: pessoas localizadas em lugares públicos que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

As ameaças e ataques cibernéticos podem causar consequências como risco de imagem, danos financeiros, perda de vantagem competitiva e perda de dados e informações confidenciais. O impacto do ataque depende da rápida detecção deste e da resposta da SOMMA Investimento após a identificação do ataque. Dessa forma, a SOMMA Investimentos segue Plano de Segurança Cibernética, o qual visa a prevenção e proteção contra tais ações.

6. ACESSO AO AMBIENTE FÍSICO

O acesso ao ambiente físico da SOMMA Investimentos será efetuado pelos seus Colaboradores através de biometria ou senha, que deverá ser cadastrada no início do relacionamento e excluída após o fim do mesmo. O acesso a não Colaboradores fica restrito à recepção e sala de reuniões, exceto se acompanhado por Colaborador e previamente autorizado o acesso pela administração.

7. DIRETRIZES DE SEGURANÇA DO AMBIENTE LÓGICO

7.1 Segregação de Atividades

A SOMMA Investimentos reconhece que a segregação das atividades é um requisito essencial para o efetivo cumprimento às suas estratégias de administração de recursos de terceiros, uma vez que cumpre um papel importantíssimo na defesa dos interesses de seus clientes. Logo, a SOMMA Investimentos segrega suas diversas áreas a partir dos procedimentos operacionais por elas adotados.

Desta forma, cada Colaborador possui um código de usuário, e-mail e usuário na rede interna de comunicação online. A rede de computadores da SOMMA Investimentos permite a criação de usuários com níveis de diferentes de acesso às informações, por meio de uma segregação lógica nos servidores, o qual garante áreas de armazenamento de dados distintos no servidor, com controles de acesso por usuário. Esta segregação visa evitar o compartilhamento e/ou a visualização de informações de outras áreas ou Colaborador, em cumprimento do artigo 24 e 25, inciso I, da Instrução CVM nº 558/15.

A SOMMA Investimentos conta com acesso à rede de arquivos via usuário e senha criptografados, utilizando Active Directory com política de senhas (8 caracteres, letras, números e caracteres especiais). Todos os usuários possuem controle de acesso a pastas específicas da rede de arquivos. A rede de computadores mantém registro de acesso de cada arquivo, permitindo identificar as pessoas que acessam cada dado ou informação. Importante destacar que todo Colaborador deve bloquear sua sessão quando se ausentar de sua mesa de trabalho, a fim de não permitir o acesso de outras pessoas a sua área de trabalho e informações à sua disposição.

A SOMMA Investimentos acredita que as medidas acima relacionadas são eficazes para cumprir os requisitos mínimos de segregação de atividades aplicados a sua realidade, estando sempre em busca de servir adequadamente seus clientes e cumprir com suas obrigações de administrador de carteira de valores mobiliários.

7.2 Utilização de Senhas

Cada Colaborador é responsável pela manutenção e guarda de suas senhas, que é pessoal e intransferível, não podendo ser anotada em arquivos físicos ou de fácil acesso. É de responsabilidade de cada Colaborador a memorização de suas senhas, seja de acesso, de e-mail ou da rede interna de comunicação online, não devendo utilizar códigos comuns como nome próprio, data de nascimento, nome de parente, número de telefone ou números sequenciais.

Para garantir a segurança, o Colaborador que realizar 3 (três) tentativas seguidas de acesso ao sistema de computadores ou de e-mail da SOMMA Investimentos, com senha inválida, terá sua conta bloqueada. O Colaborador deverá contatar a área de **Tecnologia da Informação ("TI")** para a redefinição da senha de acesso ao sistema de computadores e a área de *Compliance* para redefinição da senha de acesso ao sistema de e-mails.

O prazo máximo de duração das senhas de acesso é de 90 (noventa) dias de sua criação/alteração. O sistema notificará o usuário com antecedência de 15 (quinze) dias a expiração das senhas em questão.

Com a finalidade de controles internos, a área de *Compliance* terá acesso a todos os usuários da rede de computadores, bem como acesso à todas as contas de e-mail, meio de comunicação e de softwares utilizados pelos Colaboradores.

7.3 Utilização de E-mail e Rede Interna de Comunicação Online

Todos os Colaboradores da SOMMA Investimentos devem utilizar o e-mail disponibilizado exclusivamente para fins profissionais. O e-mail deverá ser utilizado para comunicações oficiais e internas, as quais não necessitam obrigatoriamente do meio físico, e deve ser endereçado ao correto destinatário desejado. O Colaborador deve ter ciência que o e-mail é um documento formal e possui as mesmas responsabilidades de um documento convencional em papel timbrado da SOMMA Investimentos.

Não é permitido ao Colaborador emitir opinião em nome da SOMMA Investimentos, ou utilizar material, marca e logotipos da SOMMA Investimentos para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se autorizado de forma expressa e prévia para tanto.

O Colaborador não deverá executar ou abrir arquivos anexados enviados por remetentes desconhecidos ou suspeitos. Deste modo, as seguintes extensões não devem ser abertas: .bat; .exe; .src; .lnk e .com, ou outros formatos alertados pela área de TI.

No início do relacionamento do Colaborador junto a SOMMA Investimentos, será criado conta para este na rede interna de comunicação online. Esta deverá ser utilizada como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividade de negócios, sendo monitorado pela área de *Compliance*.

7.4 Utilização de Telefone

A SOMMA Investimentos disponibiliza telefones para utilização de seus Colaboradores no desempenho de suas funções profissionais. São de propriedade da SOMMA Investimentos o telefone disponibilizado e as conversas associadas a esse número. O Colaborador é responsável por todo o conteúdo da conversa durante o uso de telefone. Utiliza-se, ainda, sistema de gravação telefônica em todos os telefones da SOMMA Investimentos. Os arquivos gravados são guardados via rede de arquivos pelo prazo de, no mínimo, 5 (cinco) anos.

7.5 Utilização da Internet

A internet deverá ser utilizada para fins profissionais, enriquecimento intelectual e ferramenta de busca de informações, com objetivo de contribuir para o desenvolvimento de atividades relacionadas à empresa. O acesso à *websites* é de responsabilidade de cada Colaborador, sendo bloqueado o acesso a *websites* com conteúdo impróprio e redes sociais. O acesso à internet será monitorado através da identificação e autenticação do Colaborador.

7.6 Utilização e Instalação de Softwares

A área de TI deverá autorizar previamente a instalação de quaisquer programas, principalmente downloads via internet, seja para uso profissional ou pessoal. Ainda, deve a área de TI ser comunicada, previamente, com a finalidade de vetar ou aprovar a instalação e utilização de novos softwares e suas respectivas licenças. Em ressalva, é proibida a instalação de softwares ilegais ou que possuam direitos autorais protegidos.

A SOMMA Investimentos possui *login* e senha específicos para usuários administrativos que possuem permissão de instalação/remoção de softwares. Para que tal instalação/remoção ocorra, é necessário o uso do *login* e senha citados. Somente colaboradores da área de TI e *Compliance* possuem autorização para uso e conhecimento do *login* e senha de instalação de softwares.

Todas as medidas elencadas neste item impedem a instalação de softwares maliciosos.

7.7 Rede de Arquivos e Backup e Armazenamento de Documentos

O acesso da rede de arquivos da SOMMA Investimentos é efetuado via Data Center interno, no qual todos os Colaboradores possuem acesso controlado, via usuário e senha. Ainda, o acesso poderá ser efetuado remotamente via acesso VPN, utilizando SSL AES-NI CPU Crypto de 2048bit. Este acesso é feito por meio de usuários específicos, com controle de horário e restrição ao acesso. O usuário da VPN possui senha distinta daquela cadastrada para o usuário da rede interna, a qual faz-se necessária para leitura dos arquivos da rede.

São executados 2 (dois) backups, em tempo real, um interno e um externo, das bases de dados de sistema e das áreas de dados da rede, a fim de garantir a recuperação de qualquer informação importante para a SOMMA Investimentos e seus clientes. As informações que necessitam ser armazenadas por prazo superior a 1 (um) ano, por exigência legal e regulamentar, são transferidas para um terceiro backup, que armazena informações a longo prazo.

7.8 Antivírus

Como proteção as ameaças e ataques cibernéticos, a SOMMA Investimentos utiliza-se de antivírus em seus servidores e estações de arquivos, o qual é atualizado automaticamente. A varredura por vírus é feita diariamente nas estações e servidores.

7.9 Plano de Segurança Cibernética

A SOMMA Investimentos segue Plano de Segurança Cibernética de acordo com os seguintes procedimentos:

i. **Identificação e avaliação de riscos:** São vistos como risco cibernético as ameaças e ataques a partir dos métodos de *malware* e engenharia social, anteriormente definidos;

ii. **Ações de Prevenção e Proteção:** Utiliza-se a proteção de antivírus contra os riscos cibernéticos e controle de instalação de softwares por *login* e senha específicos para tal ação; diariamente o servidor *Firewall* envia notificações de tentativas de intrusão. Todos os servidores possuem controle de acesso e no caso de falha de autenticação os administradores da rede recebem notificação de tentativa de instrução em tempo real. Semanalmente os softwares dos servidores são avaliados e devidamente atualizados, mantendo as últimas versões estáveis e seguras das distribuições (Linux/Windows). Todas as máquinas cliente (da operação, não servidores) possuem atualização automática ativa, mantendo os softwares devidamente atualizados; e

iii. **Plano de Resposta:** Após a identificação de ameaça ou ataque via Internet, o atacante é automaticamente bloqueado da rede e, se necessário, é feita a comunicação junto a operadora de Internet para bloqueio da faixa de IP. No caso de intrusão, a máquina contaminada é isolada da rede, caso necessário ela será formatada e a falha identificada é corrigida. Ainda, a rede de arquivos da SOMMA Investimentos é efetuada via usuário e *login* específicos, conforme citado na seção 7.6.

8. VIOLAÇÃO DAS NORMAS E PROCEDIMENTOS

Em caso de violação de quaisquer das normas e procedimentos previstos nesta Política, sanções administrativas e/ou legais poderão ser adotadas, sem aviso prévio, podendo resultar no desligamento do Colaborador e/ou processo judicial. O Colaborador infrator poderá ser notificado, sendo comunicada a ocorrência da violação ao seu superior imediato e ao Comitê de *Compliance*.

9. MELHORIA CONTÍNUA

A proteção da informação não é um ato isolado, mas um processo em constante aperfeiçoamento. Para tanto, a SOMMA Investimentos investe, de maneira continuada, no desenvolvimento de metodologias e

sistemas para a constante adequação de suas práticas de segurança e privacidade da informação aos mais exigentes níveis do praticados no mercado financeiro.

A SOMMA Investimentos efetua testes regulares visando garantir a devida segurança das informações e segurança cibernética em sua dependência e disponibiliza relatório anual com os resultados dos testes realizados. Além disso, a SOMMA Investimentos também atua na capacitação de Colaboradores e demais envolvidos no tratamento das informações.

É de responsabilidade das áreas de TI e de *Compliance* o cumprimento desta Política.

10. DISPOSIÇÕES GERAIS

A SOMMA Investimentos frisa o cuidado especial que todos os seus Colaboradores devem possuir com informações confidenciais e restritas em lugares públicos e/ou telefones. Recomenda-se, ainda, a destruição de qualquer lixo produzido que possa ser fonte de informações para pessoas mal-intencionadas. Todos os papéis com informações que não possam ser divulgadas devem ser triturados.

Solicita-se a adoção de comportamento seguro entre os Colaboradores da SOMMA Investimentos, ao não compartilhar nem divulgar senhas a terceiros; não abrir mensagens de origem desconhecida; armazenar corretamente documentos físicos e arquivos virtuais cujo conteúdo sejam informações confidenciais; não transportar informações confidenciais em qualquer meio (CD, DVD, pendrive, HD externo, papel, etc) sem autorização; não discutir assuntos referente à SOMMA Investimentos em lugares públicos ou áreas expostas, como restaurantes, aviões ou encontros sociais; e seguir corretamente esta Política.

Por fim, quaisquer dúvidas decorrentes desta Política poderão ser dirimidas pela área de Compliance da SOMMA Investimentos, ou através do correio eletrônico compliance@sommainvestimentos.com.br.

11. VIGÊNCIA E ATUALIZAÇÃO

Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.