Política de Segurança da Informação e Cyber Security

1. Objetivo: Formalizar os conceitos e as diretrizes da Segurança da Informação e Cyber Security da SOCOPA que visam à proteção dos ativos de informação com eficiência e eficácia, de modo seguro e transparente, garantindo a confidencialidade, integridade e disponibilidade das informações.

2. Público-alvo: Órgãos integrantes do sistema financeiro nacional, instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, entidades de classe, público em geral, especialmente clientes e parceiros, administradores, gestores, colaboradores, prestadores ou fornecedores de serviços, estagiários e usuários externos das informações pertencentes/custodiadas à/pela SOCOPA.

3. Diretrizes Gerais:

a) Deve ser assegurado pelo Departamento de Compliance que esta Política, normas complementares e as responsabilidades quanto à Segurança da Informação estejam amplamente divulgadas ao público-alvo, visando à sua disponibilidade para todos que se relacionam com a SOCOPA e que, direta ou indiretamente, são impactados.

b) Esta Política e suas normas complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, no qual os usuários têm acesso somente aos ativos de informação imprescindíveis para o pleno desempenho de suas atividades. Ou seja, tudo que não estiver expressamente permitido só poderá ser realizado após prévia autorização, devendo ser levado em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

c) A informação deve ser utilizada de forma transparente e apenas para execução de sua atividade profissional. A gestão da informação e dos ativos deve ser assegurada por meio de medidas efetivas que proporcionem acesso e divulgação devidamente autorizados e de acordo com a legislação vigente e com o seu nível de classificação (**v. item 5.2**).

d) A SOCOPA é a detentora de todos os direitos patrimoniais relativos às suas marcas, nomes comerciais e qualquer informação produzida através do uso dos Recursos de Tecnologia da Informação e Comunicação (RTICs), portanto, deve proibir o uso não autorizado de suas logomarcas, identidade visual e quaisquer outros sinais distintivos, atuais e futuros, em qualquer forma ou mídia, inclusive na Internet.

e) Sempre que considere necessário, o Departamento de Compliance ou o Departamento de Segurança da Informação podem inspecionar quaisquer RTICs (**v. item 4.2.a**) que porventura interajam com seus ambientes, lógicos ou físicos e/ou suas informações, incluindo aqueles de propriedade de terceiros, serviços de computação e nuvem quando autorizada a sua vinculação à SOCOPA, independentemente da interação com seus ambientes e informações.

f) O Departamento de Segurança da Informação deve manter a segurança dos ativos de informação provendo ferramentas que permitam aplicar as melhores práticas de segurança no ambiente físico ou lógico, para garantir o sigilo e a integridade no ciclo de vida da informação, desde a sua recepção, produção, registro, classificação, controle, acesso, manuseio, reprodução, transmissão, guarda e descarte com vistas a prevenir, detectar e reduzir a vulnerabilidade a ataques cibernéticos;

g) O Diretor responsável pela política de segurança cibernética nomeado junto aos órgãos reguladores, além dos departamentos de Segurança da Informação, TI são os responsáveis por definir, zelar, aperfeiçoar e garantir a aderência da SOCOPA às diretrizes de Segurança da Informação e Cyber Security com o apoio das demais linhas de defesa da organização (Compliance Corporativo, Controles Internos e Auditoria Interna);

h) As ocorrências que podem ser consideradas violações desta Política de Segurança da Informação e Cyber Security devem ser avaliadas pelas linhas de defesa da organização principalmente, Segurança e Tecnologia da Informação e, constatado como um incidente (**v. item 4.5**), este deve ser registrado nas ferramentas de registro definidas pela organização, dependendo de sua gravidade, deverá ser encaminhada para os Comitês e Comissões Internas (ex.: Comitê de Compliance e Governança, Comitê de Riscos e Controles e Comissão de Segurança da Informação) para deliberação quanto ao curso de ação a ser tomada.

i) As situações não previstas nesta política serão arbitradas pelo Diretor responsável desta Política, com assessoria dos Departamentos de Compliance Corporativo e de TI;

j) Cabe ao Conselho de Administração aprovar esta Política e suas diretrizes, assim como, avaliar sua efetividade a qualquer tempo.

4. Conceitos e Regras Básicas de Segurança da Informação

4.1. Conceito de Informação: Segundo a ISO/IEC 27002:2005(2005), Informação é o conhecimento produzido como resultado do processamento de um conjunto de dados (representações de fatos, medidas, valores, ideias ou conceitos), por exemplo, mas não se limitando: ***(a)*** Informações pertencentes ou relacionadas aos clientes; ***(b)*** Informações relacionadas à SOCOPA, inclusive contábeis; ***(c)*** Estratégias e decisões da alta administração; ***(d)*** Processos e metodologias internos da SOCOPA; ***(e)*** Informações disponibilizadas na Intranet da SOCOPA, entre outras.

4.2. Intervenientes da Segurança da Informação e Responsabilidades: Para efeitos desta política, é algo ou alguém que faz parte dos processos de Segurança da Informação ou pode afetá-los. São classificados em:

a) **Proprietário da Informação**: administrador ou gestor da área de negócio que possui a responsabilidade de classificar a informação quanto à sua necessidade de sigilo e definir os perfis de acesso.

b) **Custodiante da Informação:** indicado pelo Proprietário da Informação, é o colaborador, a unidade organizacional ou o fornecedor contratado responsável pela guarda, proteção e defesa das informações produzidas, adquiridas ou custodiadas pela SOCOPA e deve observar os critérios e controles definidos no tratamento e classificação da informação.

c) **Usuário da Informação:** é a pessoa, a unidade organizacional, a entidade ou o recurso computacional (por exemplo, programas computacionais ou dispositivos) que está autorizado(a) a acessar e fazer uso da informação.

d) **Gestor da Segurança da Informação:** o Departamento de Compliance Corporativo é a área responsável pelo Sistema de Gestão da Segurança da Informação **(v. item 5)**.

4.3. Ativos de Informação: Entende-se por Ativos de Informação qualquer componente de sustentação de processos de negócio capaz de criar, atualizar, alterar, processar, armazenar, transmitir e até excluir a informação.

Os Ativos de Informação podem ser classificados como Recursos de Tecnologia da Informação e de Comunicação (**RTICs**), que incluem, mas não se limitam a: estações de trabalho, sistema de telefonia, acessos à Internet, sistemas aplicativos de processamento de dados, computação em nuvem, Softwares, que englobam também pacotes aplicativos, extensões e complementos, dentre outros.

Os Ativos de Informação são de propriedade e direito de uso exclusivo da SOCOPA e devem ser empregados unicamente para fins profissionais, limitado às atribuições de cargo e/ou função desempenhadas pelo colaborador, que deve cumpri-las dentro do padrão de conduta ética estabelecida pela SOCOPA e em observância a sua obrigação legal de sigilo profissional, sendo que o mesmo responde diretamente por qualquer dano causado, por ação ou omissão, resultante de sua postura e/ou comportamento, mediante apuração de responsabilidade em processo administrativo disciplinar devidamente instaurado.

4.4. Princípios da Segurança da Informação:

a) **Confidencialidade**: garantir que a informação não estará disponível ou divulgada a indivíduos, entidades ou aplicativos (sistemas e ferramentas do pacote *Office*, como por exemplo *Excel)* sem autorização. Em outras palavras, é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra a sua revelação não autorizada.

b) **Integridade:** garantir que a informação não tenha sido alterada em seu conteúdo e, portanto, é íntegra, autêntica, procedente e fidedigna. Uma informação íntegra é uma informação que não foi alterada de forma indevida ou não autorizada.

c) **Disponibilidade**: permite que a informação seja utilizada quando necessária, portanto, esteja ao alcance de seus usuários e destinatários e possa ser acessada no momento em que for necessário utilizá-la.

4.5. Ciclo de Vida da Informação: Para efeito desta política, será considerado o seguinte ciclo de vida da informação:

a) **Manuseio**: é a etapa onde a informação é criada e manipulada.

b) **Armazenamento**: consiste na guarda da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.

c) **Transporte**: ocorre quando a informação é transportada para algum local, não importando o meio no qual ela está armazenada.

d) **Descarte**: essa fase refere-se à eliminação de documento impresso (depositado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

4.6. Classificação da Informação: A classificação das informações deve ser avaliada em razão do teor do conteúdo, relevância do conhecimento externo e pelos elementos intrínsecos do documento. O acesso, divulgação e tratamento de documento (físico ou digitalizado), dado ou informação da SOCOPA são restritos aos colaboradores que tenham necessidade de conhecê-los em razão de suas atividades profissionais, pautados pela regulamentação existente e pelos princípios de pertinência, utilidade e relevância.

Toda informação de uso corporativo deve ser classificada de acordo com o grau de sigilo para o negócio da empresa, considerando-se os três níveis descritos a seguir:

a) **Confidencial:** É o mais alto grau de sigilo, aplicadas às informações de caráter estratégico e que devem ser manuseadas por um grupo restrito de usuários. O acesso não autorizado a essas informações pode ter consequências críticas para o negócio, causando danos estratégicos à imagem da empresa.

b) **Restrito**: São informações específicas para uso interno, com circulação exclusiva e irrestrita dentro da empresa. Estas informações podem estar disponíveis a todas os colaboradores e prestadores de serviços e devem ser utilizadas somente para as atividades da SOCOPA. Essas informações, mesmo sendo de circulação

livre dentro das empresas, não devem ser divulgadas para entidades externas sem os devidos cuidados, incluindo, quando necessário, a assinatura de acordos de confidencialidade ou de autorização formal previamente avaliada pela alçada responsável pela informação ou documento em questão.

c) **Público:** São informações de circulação livre e domínio público. Esse tipo de informação não exige controles ou restrições de segurança para seu acesso ou guarda.

d) **Uso Interno:** São informações de nível reduzido de confidencialidade onde qualquer informação que possa ser divulgada a toda a empresa, bem como pessoas vinculadas. Geralmente tais informações ficam disponíveis na intranet.

4.7. Incidentes de Segurança da Informação: Para efeito desta política, um incidente de segurança é definido como qualquer evento adverso, decorrente da ação de uma ameaça que explora uma ou mais vulnerabilidades, relacionado à segurança de um ativo que pode prejudicar quaisquer princípios da Segurança da Informação, descritos no **item 4.3**.

5. Sistema de Gestão da Segurança da Informação: O Sistema de Gestão da Segurança da Informação (SGSI) é um conjunto de disciplinas, deveres e boas práticas para estabelecer, implementar, operar, monitorar, revisar, manter e aprimorar a Segurança da Informação visando a coordenação de ações em quatro grandes frentes de atuação: ***(a)*** Governança das políticas e procedimentos de segurança da informação; ***(b)*** Recursos e componentes de segurança da informação; ***(c)*** Monitoramento contínuo do ambiente de tecnologia da informação; e ***(d)*** Gestão de crises e continuidade de negócios.

Visando à estruturação e coordenação das ações de atendimento das necessidades de segurança da informação nas visões dos órgãos reguladores (normas e regulamentos), público-alvo (modelo comportamental, conscientização de pessoas no tratamento e uso seguro das informações), ambientes (acessos físicos e proteção ao ambiente de trabalho) e processos de negócios, foram considerados nesta Política os seguintes componentes do ambiente de tecnologia da informação, ordenados dos aspectos mais gerais aos mais específicos: ***(a)*** Órgãos reguladores; ***(b)*** Continuidade de negócios; ***(c)*** Governança e controles de acesso; ***(d)*** Prevenção dos ataques internos, conscientização dos usuários e diálogos com as partes externas; ***(e)*** Gestão de vulnerabilidades e processo de investigação; ***(f)*** Internet; ***(g)*** Dispositivos de rede; ***(h)*** Controles tecnológicos e físicos; ***(i)*** Estação de trabalho e telefonia; ***(j)*** Servidores internos; ***(k)*** Servidores externos; ***(l)*** Dispositivos móveis e BYOD - “Bring Your Own Device”; e ***(m)*** Acesso à informação.

6. Controles Internos de Segurança da Informação e Cyber Security:

6.1. Identificação/Avaliação de Ameaças e Vulnerabilidades: Caberá ao Departamento de Segurança da Informação da SOCOPA a identificação e avaliação dos riscos residuais a que os processos e ativos relevantes das instituições estejam sujeitos em virtude das vulnerabilidades e possíveis cenários de ameaça atribuídos a cada processo ou ativo.

No que tange às empresas prestadoras de serviços e fornecedores que manuseiem dados ou informações sensíveis, as quais sejam relevantes para a condução de suas atividades operacionais, a SOCOPA revisou a relação de cláusulas contratuais obrigatórias para a contratação de fornecedores e prestadores de serviços prevista na norma interna, de forma a obrigar seus novos fornecedores e prestadores de serviços a se adequarem ao disposto na Resolução CMN 4658/2018, gerando ainda ações revisionais dos contratos em vigor com seus fornecedores e prestadores de serviços, de forma a considerar a obrigatoriedade do enquadramento à essa Resolução.

6.2. Ações de Prevenção e Proteção: Sem prejuízo de ações específicas para proteção e prevenção de riscos identificados e avaliados pela área responsável, serão adotadas pela SOCOPA, por meio do Departamento de

Segurança da informação, rotinas padronizadas de prevenção e proteção dos processos e ativos relevantes das referidas instituições, conforme previstas na norma interna, realizando análises de vulnerabilidade, testes de intrusão e outras avaliações específicas que certifiquem o cumprimento dos requisitos de segurança e as responsabilidades previamente estabelecidas.

Destacando a execução periódica de testes de ataque e invasão, visando monitorar a eficiência de seu sistema de proteção a vulnerabilidades cibernéticas, a SOCOPA realiza testes, tanto em ambiente interno (na modalidade *Gray Box*) como no externo (na modalidade *Black Box*).

6.3. Monitoramento e Testes: Devem ser implementados controles internos efetivos para proteção dos RTICs da SOCOPA, garantindo a sua confidencialidade, integridade, disponibilidade e norteado por esta política, com as melhores práticas de mercado e regulamentações vigentes.

A SOCOPA deve comunicar aos intervenientes **(v. item 4.1)** sobre o monitoramento, inclusive de forma remota, de todo acesso e uso de suas informações, seus RTICs, além de seus ambientes, físicos e lógicos, para verificação da eficácia dos controles implantados e proteção de seu patrimônio e reputação, mantendo os acessos gravados e passíveis de monitoração, portanto, não há expectativas de privacidade em sua utilização.

Os aplicativos críticos devem implementar a geração/manutenção de trilhas de auditoria, controle de versionamento do código fonte e segregação entre os ambientes de produção, homologação e teste. As ameaças cibernéticas devem ser analisadas em conjunto com as vulnerabilidades detectadas pelo SGSI nos ativos de informação e devem possuir monitoramento proativo.

6.4. Plano de Ação e de Resposta a Incidentes: Os incidentes de Segurança da Informação **(v. item 4.7)** devem ser identificados e registrados para acompanhamento dos planos de ação e análise das vulnerabilidades da instituição respeitando o nível de exposição a risco aceito e definido pela SOCOPA.

a) **Comunicação de incidentes:** Os intervenientes **(v. Item 4.1)** devem comunicar imediatamente os casos de incidentes ao Gestor do Sistema de Segurança da Informação. Os incidentes deverão ser avaliados e investigados de forma a construir uma análise consistente de causas-consequências, riscos envolvidos, partes envolvidas e planos de respostas. A avaliação deverá ser direcionada ao Diretor responsável pela Política de Segurança Cibernética para decisão das ações iniciais a serem tomadas. Classificada a relevância do incidente, a SOCOPA deverá emitir com adequada tempestividade comunicado às partes envolvidas, informando a situação ocorrida e ações definidas, ao menos, de forma preliminar, informando/notificando as atividades posteriores pertinentes. O Gestor do Sistema de Segurança da Informação deve elaborar e divulgar ao Conselho de administração relatório anual sobre os planos de ação e de resposta aos incidentes.

b) **Tentativa de burlar:** A mera tentativa de burlar às diretrizes e controles estabelecidos pela SOCOPA, quando constatada, deve ser tratada como uma violação.

c) **Tratamento de vulnerabilidade identificadas:** O tratamento e correções proativas das principais fragilidades ou fraquezas dos ativos de informação a serem utilizados devem estar registrados, sendo necessário avaliar o risco residual e ser sustentado pelos intervenientes indicados no plano.
d) **Conflitos de interesse:** A SOCOPA deve possuir um processo de concessão de acessos que utiliza critérios claros e objetivos para identificar os conflitos de interesse os quais decorrem de limitações técnicas ou de situações devidamente autorizadas. Deverá haver monitoramento das atividades dos intervenientes e das ameaças cibernéticas.

e) **Elaboração de plano de ação:** O Plano de Ação deverá ser elaborado pelos Departamentos de Segurança da Informação e Compliance Corporativo, podendo ser envolvidos outros departamentos caso necessários para implementação das soluções para administração de eventuais contingências. Tal plano deve contar com

definição expressa dos papéis e responsabilidades na solução do impasse, prevendo acionamento dos colaboradores-chaves e contatos externos relevantes, caso aplicáveis. Deverão ser levados em consideração os cenários de ameaças previstos na avaliação de risco, havendo critérios para classificação dos incidentes, por severidade. O Plano de Ação deverá prever os casos de necessidade de utilização das instalações de contingências nos casos mais severos, assim como o processo de retorno às instalações originais após o término do incidente. A documentação relacionada ao gerenciamento dos incidentes deverá ser arquivada para fins de auditoria.

f) **Comunicação aos Órgãos Reguladores:** Conforme determinado na Resolução CMN 4658/18, a SOCOPA efetuará comunicação tempestiva das ocorrências de incidentes relevantes e interrupções de serviços relevantes que configurem uma situação de crise, bem como as providências adotadas para o reinício dessas atividades.

g) **Compartilhamento de informações de ocorrências:** A SOCOPA, de forma a incentivar a troca de informações e o maior conhecimento dos integrantes do sistema financeiro nacional, promoverá o compartilhamento das ocorrências de segurança cibernética, inclusive envolvendo situações relacionadas a prestadores de serviços e fornecedores, cujos registros estarão centralizados em sistema corporativo de gerenciamento de riscos. De maneira similar, as ciências de ocorrências compartilhadas junto à SOCOPA serão apresentadas nos Comitês e Comissões internas, buscando definir eventuais ações preventivas.

h) **Seguro de Riscos Cibernéticos:** A SOCOPA possui seguro de riscos cibernéticos contratado, assegurando cobertura adicional ao tema. Este seguro visa cobrir, especificamente, despesas decorrentes de reclamações e ocorrências originadas pelo vazamento de dados ou informações de terceiros (ex.: clientes, fornecedores, colaboradores etc.), por meio de sistemas computadorizados.

7. Programa de Capacitação, Conscientização e Revisão dos Normativos: A SOCOPA deve possuir e manter um programa de revisão/atualização que vise garantir que todos os requisitos de segurança técnicos e legais implementados estão sendo cumpridos, atualizados e em conformidade com a legislação vigente, incluindo também a revisão periódica dos planos de ação, incluindo sua adesão a iniciativas de compartilhamento de informações sobre incidentes cibernéticos com outras instituições financeiras e/ou entidades de classe em que haja foros de tratamento do tema.

A SOCOPA promove através da plataforma de Educação Corporativa Paulista E-Learning, um curso de conscientização sobre a importância da Segurança da Informação e Cyber Security voltada a todo público-alvo, além de um resumo de segurança divulgado nos sítios de internet da SOCOPA.

A SOCOPA também divulga informações nos sítios de internet da SOCOPA acerca das precauções na utilização de produtos e serviços financeiros e sua Política de Privacidade.

8. Responsabilidades: As questões de segurança de informação e segurança cibernética, deverão ser endereçadas ao Diretor responsável pela Política de Segurança Cibernética (Resolução CMN 4.658/18 e Circular 3909/18).