SOCINAL
FINANCEIRA

POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVOS

Estabelecer critérios e procedimentos para contemplar a segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pela Socinal Financeira, conforme determinado pela Resolução do Banco Central nº 4.658, de 26 de abril de 2018.

2. ABRANGÊNCIA

A presente politica se aplica a Socinal Financeira, sendo de responsabilidade de todos os funcionários e ou colaboradores internos ou externos, devendo ser dado amplo conhecimento de seu teor a todas as pessoas ou correspondentes bancários que utilizam os meios físicos ou lógicos desta instituição, por serem todos responsáveis por garantir a segurança das informações a que tenham acesso. Será dividida em duas partes principais:

✓ A segurança cibernética, subdividida entre implementação, divulgação e plano de ação e resposta a incidentes;e
✓ Serviços de processamento e armazenamento de dados e de computação em nuvem.

3. CONCEITOS E DEFINIÇÕES

Para os efeitos desta normativa, são estabalecidos os seguintes conceitos e definições:

✓ ***Acesso*:**Ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação da desta instituiçãol;
✓ ***Ameaça:*** Qualquer evento que explore vulnerabilidades ou seja causa potencial de um incidente indesejado, que pode resultar em dano para o sistema da Socinal;
✓ ***Análise de riscos:***Uso sistemático de informações para identificar fontes e avaliar riscos;
✓ ***Ativo:***Qualquer componente (seja humano, tecnológico,software ou outros) que sustente uma ou mais atividades e que tenha valor;
✓ ***Bens de informação:***Os meios de armazenamento, transmissão e processamento; os sistemas de informação; além das informações em si, bem como os locais em que se encontram esses meios e os colaboradores que têm acesso a eles;
✓ ***Autenticidade:*** Propriedade de que a informação foi produzida, expedida, modificada ou destruída por determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
✓ ***Celeridade:*** As ações de segurança devem oferecer respostas rápidas a incidentes e falhas;
✓ ***Classificação da informação:***Identificação dos níveis de proteção que as informações demandam; atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas;
✓ ***Confidencialidade:*** Propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada ou não credenciada pela Socinal;
✓ ***Controle de acesso:*** Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
✓ ***Desastre:*** Evento repentino e não planejado que causa perda para toda ou parte da Socinal, com sérios impactos em sua capacidade de prestar serviços essências ou críticos, por um período de tempo superior ao prazo de recuperação;

✓ ***Descarte:*** Eliminação correta de informações, documentos, mídias e acervos digitais;
✓ ***Disponibilidade:***Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
✓ ***Evento de segurança da informação:*** Ocorrência identificada de procedimento, sistema, serviço ou rede que indica possível perda de controle ou violação da política de segurança da informação, ou situação desconhecida que possa ser relevante para a segurança da informação;
✓ ***Gestão de continuidade os negócios:*** Processo de gestão que identifica ameaças potenciais para Socinal, bem como os possíveis impactos nas operações de negócios, caso essas ameaças se concretizem. Esse processo prevê a definição de estrutura para o aprimoramento da resiliência organizacional, de modo a se responder efetivamente as ameaças e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, assim como suas atividades de valor agregado; e
✓ ***Gestão de Risco Segurança da Informação:*** Conjunto de processos que permiem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

4. PRINCÍPIOS

Esta Política e suas ações serão norteadas pelos seguintes princípios:

✓ ***Celeridade:*** As ações de segurança devem oferecer respostas rápidas a incidentes e falhas;
✓ ***Ética:***Os direitos e interesses legítimos dos usuários devem ser preservados, sem comprometimento da segurança;
✓ ***Clareza:***As regras de segurança devem ser precisas, concisas e de fácil entendimento;
✓ ***Legalidade:*** As ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais da Socinal;e
✓ ***Publicidade:*** Transparência no trato da informação, observados os critérios legais.

5. DIRETRIZES GERAIS

As diretrizes de segurança da informação estabelecidas nesta política, aplicam-se aos ***Bens de Informação***, ou seja: Os meios de armazenamento, transmissão e processamento; os sistemas de informação; além das informações em si, bem como os locais em que se encontram esses meios, as informações armazenadas, acessadas, produzidas e transmitidas pela Socinal, e que devem ser seguidas pelos usuários, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Independente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada deverá ser sempre protegida adequadamente, de acordo com está política. Os recursos de tecnologia da informação disponibilizados pela Socinal serão utilizados estritamente propósito da instituição.

Obs.: É vedado a qualquer usuário e ou colaborador da financeira o uso de quaisquer "***Bens de Informação***" e dos recursos para fins pessoais (próprios ou de terceiros).

6. DIRETRIZES ESPECÍFICAS

6.1. GESTÃO DA SEGURANÇA DA INFORMAÇÃO

✓ Todos os mecanismos de proteção utilizados para a segurança devem ser mantidos com o objetivo de garantir a continuidade dos negócios da Socinal;
✓ As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido;
✓ Os requisitos de segurança da Socinal devem ser explicitamente citados em todos os termos de compromissos celebrados entre a instituição e terceiros, por meio de cláusulas específica sobre a obrigatoriedade de atendimento as diretrizes desta política, devendo também ser exigido termo de confidencialidade.

6.2. GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDECOMPUTACIONAL

A Diretoria responsável pela Gestão de Processos e Tecnologia da Informação, devera criar e manter equipe de tratamento de resposta a incidentes em redes computacionais, instituída pelo gestor de segurança da informação, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em redes de computadores. Os eventos e incidentes devem ser comunicados, registrados e tratados de acordo com um plano de gerenciamento de incidentes especificada nos normativos internos.

7. SEGURANÇA CIBERNÉTICA

Os procedimentos de segurança cibernética, deverão estar adequados aos fatores como porte e modelo de negócio da Socinal, natureza das operações, complexidade dos produtos e a sensibilidade dos dados em questão. E tem como um de seus objetivos a capacidade de prevenir,detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético. É necessário, portanto, estabelecer a combinação de conhecimento do risco cibernético com a avaliação do impacto,desta forma, esta instituição considera três fatores: plano de ação aos incidentes, implementação edivulgação.

- **Minimizando o número dos incidentes ->** Quando houver um incidente de segurança, o setor de T. I da Socinal precisará assegurar que seu impacto seja minimizado e deverá:

✓ Estabelecer claramente e aplicar todas as diretivas e procedimentos, que devem ser testados integralmente para garantir que eles sejam práticos e claros e, assim, ofereçam o nível apropriado de segurança;
✓ Obter o suporte da gerência a respeito das diretivas de segurança e do tratamento de incidentes;
✓ Avaliar regularmente as vulnerabilidades do seu ambiente;
✓ Verificar regularmente todos os sistemas de computadores e dispositivos de rede para garantir que todos eles tenham os *patches* mais recentes instalados;
✓ Estabelecer programas de treinamento em segurança para a equipe de TI e os usuários finais;
✓ Postar faixas de segurança que lembrem os usuários de suas responsabilidades e restrições;
✓ Desenvolver, implementar e aplicar uma diretiva que exija senhas fortes;
✓ Monitorar e analisar regularmente o tráfego da rede e o desempenho do sistema;
✓ Verificar regularmente todos os logs e mecanismos de registro, inclusive logs de eventos do sistema operacional, logs de aplicativos específicos e logs do sistema de detecção de instruções;
✓ Verificar seus procedimentos de backup e restauração;
✓ Monitorar os sistemas em busca de violações de segurança;

✓ Funcionar como um ponto central de comunicação, tanto para receber relatórios dos incidentes de segurança quanto para disseminar informações vitais a respeito do incidente para as entidades adequadas;
✓ Documentar e catalogar os incidentes de segurança;
✓ Promover a percepção da segurança dentro da Socinal para ajudar a impedir que os incidentes ocorram;
✓ Oferecer suporte à auditoria do sistema e da rede por meio de processos como, por exemplo, a avaliação da vulnerabilidade e o teste de penetração;
✓ Pesquisar novos patches de software;
✓ Analisar e desenvolver novas tecnologias para minimizar vulnerabilidades e riscos de segurança;e
✓ Refinar e atualizar sempre os sistemas e os procedimentos atuais.

8. RESPONSABILIDADES

8.1 DIRETORIA

✓ É responsável por avaliar e aprovar esta política quanto à adequação aos riscos à segurança cibernética da Socinal e supervisionar a sua observância e implementação.
✓ Aprovar o plano de ação e resposta a incidentes e supervisionar sua implementação.

8.2 GERÊNCIA DE TI

✓ É responsável por elaborar e manter periodicamente revisada a política de segurança cibernética.
✓ Conceder e controlar os acessos aos sistemas e informações.
✓ Sugerir a alocação dos recursos financeiros, humanos e tecnológicos para atender os objetivos desta política.
✓ Implementar e manter o Plano de Ação e resposta a incidentes e recomendar a adoção de procedimentos para proteção dos dados.
✓ Promover treinamentos e esclarecimentos para toda à organização.

8.3 ÁREA DE CONTROLE INTERNO E COMPLIANCE

✓ É responsável por contribuir com a identificação de riscos à segurança cibernética que porventura tenham sido identificados através do processo de gerenciamento de riscos integrados da instituição.
✓ Compartilhar os dados de incidentes relevantes de segurança cibernética comoutras instituições financeiras, quando for aplicável.

8.4 TODOS OS COLABORADORES

✓ São responsáveis por participar ativamente do processo de segurança cibernética.
✓ Coletar, tratar e utilizar as informações e dados de acordo com as diretrizes desta política.
✓ Participar dos treinamentos relativos à segurança cibernética.
✓ Manter sua senha em sigilo e de usoindividual.
✓ Reportar a área de Controle Interno e Compliance os riscos à segurança cibernética identificados durante a execução das rotinas da instituição
✓ Classificação dos dados e informações sob seu controle quanto ao sigilo.

9. DISPOSIÇÕES GERAIS

9.1. PRAZO

✓ O prazo de atualização desta Política é de 01 (um) ano, sendo passivel de alteração ou atualização sempre que constatada sua necessidade.

9.2. APROVAÇÃO

✓ Está política foi aprovada pela Diretoria executiva e pelo Comitê de Controles Internos e passa a fazer efeito a partir desta data.

10. DIVULGAÇÃO DO CONTEÚDO

Esta versão deve ser utilizada para publicidade nos veículos de comunicação externa da Socinal, alinhada com a sua Política de Segurança da Informação oficial interna da instituição.

Araruama, 31 de outubro de 2018