I. OBJETIVO

Os objetivos da Política de Segurança Cibernética da Kredilig S/A CFI, considerando o porte, o perfil de risco e o modelo de negócio da instituição, é garantir os três pilares fundamentais da segurança, que são confidencialidade, integridade e disponibilidade, através dos seguintes controles:

- Estabelecer procedimentos e controles para reduzir a vulnerabilidade da instituição a incidentes;
- Constituir controles específicos para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
- Garantir o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para a instituição.

II. ALCANCE

Esta política aplica-se a todas as áreas da Instituição.

III. DIRETRIZES

A instituição possui como diretrizes da segurança cibernética:

- A classificação dos dados e informações ocorre conforme definido no item XXIII CLASSIFICAÇÃO DAS INFORMAÇÕES, da Política de Segurança da Informação.
- Manter a capacidade de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, utilizando-se de registros de rastreabilidade da manipulação de dados de seus clientes;
- Assegurar que os dados da instituição e de seus clientes sejam acessados e manipulados apenas por pessoas autorizadas e de forma segura;
- Proteger ativos tecnológicos e estabelecer procedimentos de monitoramento das redes da instituição e das máquinas de funcionários para detecção de intrusões
- Conduzir monitoramento e resposta de incidentes, seguindo as etapas de detecção, mitigação emergencial e análise de causa raiz;
- Elaborar cenários de incidentes para realização periódica de testes de continuidade;
- Garantir a conscientização da equipe através de programas de capacitação e avaliações periódicas.
- Garantir o compartilhamento de informações sobre os incidentes relevantes com as demais instituições autorizadas a funcionar pelo Banco Central.

IV. CENÁRIOS

Os cenários de incidentes identificados devem considerar testes de continuidade de negócios, sendo eles:

- Vazamento de Informação por invasão ao ambiente da Kredilig;
- Vazamento de Informação por intervenção de Colaborador;
- Acesso indevido à informação;
- Indisponibilidade de serviço de Prestador de Serviço;
- Indisponibilidade de serviço da Instituição;
- Ataque por malware / vírus;
- Sequestro de dados;
- Ataque por engenharia social;

- Vulnerabilidade sistêmica;
- Falhas no Backup;
- Ataque de serviço.

V. PLANOS DE RESPOSTAS

A Instituição possui o documento Plano de Contingência, no qual consta a definição dos planos de respostas voltados aos cenários identificados.
Além de estabelecer o documento Plano de Ação e de Respostas a Incidentes, onde estabelece a implementação da política de segurança cibernética.

VI. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZANAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, devem-se seguir as diretrizes da Resolução CMN nº 4.893/21 e a Política de Compras e Contratações.

CLÁUSULA CONTRATUAL

Os contratos de prestação de serviços de terceiros devem conter cláusulas específicas quanto à proteção dos dados, conforme descrito na Política de Compras e Contratações.

VII. TREINAMENTOS

A instituição compromete-se a incluir em seu planejamento anual treinamentos quanto à segurança cibernética a todos os funcionários e Diretores da Instituição.

VIII. RESPONSABILIDADES

As atribuições e responsabilidades dos usuários em dados confidencias, referente à segurança cibernética, serão detalhadas em termos de responsabilidades próprios.
Os termos irão abordar:

- Acessos ao Banco de Dados;
- Gerenciamento de Dados (B.I.);
- Acessos Privilegiados a Servidores;
- Backups.

IX. RELATÓRIO

A Instituição realiza o monitoramento referente à segurança cibernética e detalha em relatório anualmente, submetidos à auditoria interna.

X. AUDITORIA INTERNA

Os mecanismos de acompanhamento e controle implementados pela instituição deverão ser submetidos a testes realizados anualmente pela auditoria interna.

XI. COMUNICAÇÃO AO BANCO CENTRAL

Na ocorrência de incidentes relevantes e/ou na interrupção de serviços relevantes, caracterizando situação de crise na instituição, será comunicado ao Banco Central conforme

normativo da Resolução n° 4.893/21. A comunicação será realizada de acordo com os critérios que configuram uma situação de crise com classificação Grave.

XII. COMPARTILHAMENTO DE INCIDENTES

A instituição se compromete a compartilhar as informações de incidentes relevantes do que trata o art. 3, inc. IV. A divulgação será feita através de ferramenta exclusiva para fins de compartilhamento de incidente cibernético, considerando os critérios adotados pela Instituição, conforme descrito no item XVII.

XIII. MONITORAMENTO DE DADOS

A Instituição realiza o monitoramento de vazamento de dados através de uma ferramenta para a identificação de seus dados.

XIV. DIVULGAÇÃO

A Instituição valoriza a transparência no relacionamento entre as partes interessadas, desta forma, a divulgação desta política ocorre das seguintes formas:

- Colaboradores e usuários internos: por meio de comunicados e publicação na rede interna da Instituição.
- Clientes e usuários externos, fornecedores: divulgada por meio do site da Instituição.

XV. VERIFICAÇÃO DO CUMPRIMENTO DA POLÍTICA

Para fiscalizar o cumprimento das regras estabelecidas nesta Política, a T.I. poderá implantar softwares e sistemas de monitoramento do uso da Internet, rede e estações de trabalho, além de inspecionar arquivos armazenados nas estações de trabalho ou nas pastas da rede, buscando garantir a integridade dos dados e a segurança de seus sistemas de informação.

XVI. DO DESCUMPRIMENTO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

O descumprimento a esta Política de Segurança Cibernética será analisado pela Alta Administração considerando a gravidade, a natureza e os possíveis danos para a Instituição, estando o infrator sujeito a medidas disciplinares, independentemente do nível hierárquico.

Todos que tiverem conhecimento de ato ou fato que indique o descumprimento ao estabelecido nesta política deverão comunicar a seus supervisores ou à Alta Administração.

XVII. REGULAMENTAÇÕES ASSOCIADAS

ORGÃO REGULAMENTADOR	NORMA
Conselho Monetário Nacional	Resolução 4.893/21

XVIII. VIGÊNCIA

Esta política foi aprovada pela Diretoria da KREDILIG S/A CFI, passando a vigorar a partir da data da sua publicação.