I. OBJETIVO

Esta política tem o objetivo de orientar a conduta dos usuários de informática da KREDILIG S/A CFI na utilização dos recursos computacionais, visando proteger a integridade, confidencialidade e disponibilidade dos dados e dos sistemas de informações, além de manter a continuidade operacional e reduzir a vulnerabilidade a incidentes de segurança cibernética.

II. ALCANCE

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

III. AMPLITUDE DA SEGURANÇA DA INFORMAÇÃO

A Instituição preza pela integridade, disponibilidade e confidencialidade das informações, assim a instituição garante que a informação armazenada ou transferida se mantém integra e disponível a todos os usuários que necessitarem, seguindo os padrões de confidencialidade de tais informações, conforme regras estabelecidas no Código de Conduta e Ética.

IV. SEGURANÇA CIBERNÉTICA

A Segurança Cibernética é um conjunto de ações que tem como objetivo proteger os dados e informações provendo a disponibilidade, a integridade e autenticidade.

Os riscos podem ter origem interna e externa, intencional ou não, através de malware, ataque a serviços e servidores para parar ou degrada-lo, engenharia social, invasões entre outros, que tem como objetivo causar falha na disponibilidade, alteração da integridade, fraudar a autenticidade, ou roubo e/ou vazamento de informação.

V. ESTRUTURA DE GERENCIAMENTO

São definidos procedimentos para identificar falhas e possíveis ataques, com o objetivo de minimizar e restabelecer serviços afetados com o menos tempo de inoperância, com o objetivo de proteger os dados e serviços.

As autorizações de acessos às informações são controladas de acordo com as alçadas dos usuários e há um monitoramento anual.

Os incidentes são registrados em Relatórios de Não Conformidade - RNC, com as análises da ocorrência, ações de correção e mitigação.

VI. CONFIDENCIALIDADE

Todos os contratos firmados com a KREDILIG S/A CFI possuem cláusula de confidencialidade.

VII. PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES

A KREDILIG S/A CFI tem controles e política que previnem o vazamento de informações estabelecendo boas práticas para uso de correio eletrônico, acesso à internet, acesso remoto, comportamento dos funcionários em locais públicos e na troca de informações com fornecedores.

VIII. PLANO DE CONTINUIDADE DE NEGÓCIOS

A Instituição possui o documento Plano de Continuidade de Negócios, no qual consta a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes.

IX. DISSEMINAÇÃO DA CULTURA DE SEGURANÇA

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.