SEGURANÇA DA INFORMAÇÃO

Resumo das linhas gerais

Classificação da informação: Pública

CrediSIS
Sistema de Crédito Cooperativo

www.credisis.com.br

DO OBJETIVO

Art. 1° O objetivo da Segurança da Informação é garantir a continuidade dos negócios da organização frente a ameaças. A Política de Segurança da Informação ("Política") é o documento que estabelece conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança da informação, em especial sobre a segurança cibernética, visando preservar a confidencialidade, integridade e disponibilidade das informações sob responsabilidade do CrediSIS, bem como, zelar pelo dever de sigilo das operações de instituições financeiras conforme Lei Complementar n° 105/01, e a observância à Lei Geral de Proteção de Dados Pessoais (LGPD) e à Resolução n° 4.893/21 - CMN e suas disposições futuras.

Parágrafo único. Este resumo é direcionado ao público geral e também aos prestadores de serviço a terceiros que mantenham relacionamento com as instituições do Sistema CrediSIS.

DA ABRANGÊNCIA

Art. 2° Esta Política tem abrangência corporativa na CrediSIS Central e em todas as suas Cooperativas filiadas, sendo compatível com o porte, o perfil de risco, o modelo de negócio, a natureza das operações, a complexidade dos produtos, serviços, atividades e processos e a sensibilidade dos dados e das informações sob responsabilidade da instituição.

DOS PAPÉIS E RESPONSABILIDADES

Art. 3° O CrediSIS define responsabilidades específicas para todos que se relacionem com as informações sob sua responsabilidade.

DO TRATAMENTO DAS INFORMAÇÕES

Art. 4° Toda informação, que garanta a continuidade das atividades dos integrantes do sistema CrediSIS, é tratada com critérios específicos inclusive no que diz respeito à classificação das informações. A Política de Proteção de Dados Pessoais estabelece as diretrizes para o tratamento das informações referentes à pessoa natural.

Art. 5° O CrediSIS atenta-se para reduzir, dentro das atividades individuais, o risco de violação de segurança, fraude e roubo de informações causadas por documentos deixados desprotegidos sobre as mesas, impressoras ou em locais inadequados, considerando a classificação e o valor da informação ali contida.

DA SEGURANÇA LÓGICA

Art. 6° O controle de acesso dos usuários das estações de trabalho é centralizado através de controlador de domínio, na qual, seguindo as melhores práticas de segurança, para efetivação de acessos possui requisitos mínimos de segurança como complexidade de senhas, renovação periódica de senhas, impossibilidade de cadastramento de senha anterior, dentre outros. As áreas devem gerir a concessão, revogação e os privilégios dos acessos lógicos de sua responsabilidade.

Art. 7° O acesso remoto, tanto interno quanto externo, deverá ser efetuado utilizando tecnologias adequadas e aprovadas para tal finalidade, respeitando os limites de supervisão estabelecidos.

Art. 8° O CrediSIS mantém controles tecnológicos aptos a proteger o acesso à rede, sejam elas locais, públicas, remotas, entre outras.

DA SEGURANÇA FÍSICA

Art. 9° O CrediSIS mantém controles de acesso físico às dependências da cooperativa. Para acesso a áreas restritas são aplicados controles com maior nível

de complexidade. As áreas devem gerir a concessão, revogação e os privilégios dos acessos físicos de sua responsabilidade.

Art. 10° Os equipamentos que atualmente operam os serviços e aplicações críticas para o funcionamento dos negócios, possuem contingência adequada que garanta a continuidade das operações.

DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 11° Os riscos de segurança da informação devem ser devidamente gerenciados, de maneira integrada aos demais riscos inerentes às atividades da cooperativa.

Art. 12° O CrediSIS mantém o Plano de Resposta a Incidentes seguindo as diretrizes da Política de Gestão de Incidentes de Segurança da Informação.

DO LICENCIAMENTO DE SOFTWARES

Art. 13° Todo equipamento deverá ter o seu sistema operacional devidamente licenciado obedecendo os termos de utilização do fabricante.

Art. 14° *Softwares* de uso diário, que não possuírem licenças gratuitas, também deverão obedecer às regras de licenciamento do fabricante.

DA CONSCIENTIZAÇÃO E DIVULGAÇÃO

Art. 15° Programas de conscientização, divulgação e reciclagem do conhecimento desta política devem ser estabelecidos e praticados regularmente para garantir que todos saibam as diretrizes e responsabilidades relacionadas à segurança das informações sob responsabilidade do CrediSIS.

DO REGIME HOME OFFICE

Art. 16° Para adoção de regime home office a CrediSIS segue as diretrizes e recomendações de segurança descritas nesta política.

DO USO DE DISPOSITIVOS MÓVEIS PESSOAIS (BYOD)

Art. 17° O CrediSIS mantém diretrizes de autorização e uso de dispositivos móveis pessoais para utilização adequada nas atividades da cooperativa.

DO USO DE APLICATIVOS DE COMUNICAÇÃO

Art. 18° O uso de *e-mail* corporativo deve ser restrito apenas para assuntos pertinentes à CrediSIS no relacionamento entre colaboradores, cooperativas, cooperados e terceiros.

Art. 19° Todos os colaboradores do CrediSIS devem utilizar preferencialmente os canais de comunicação corporativos como *e-mail* ou telefones da cooperativa para efetuar contato com seus cooperados.

DOS REGISTROS DE AUDITORIA

Art. 20° O CrediSIS mantém registros de eventos em logs de auditoria contendo no mínimo informações de identificação de usuário (quando aplicável), data, hora e as ações do evento.

DA ANÁLISE DE VULNERABILIDADES

Art. 21° O CrediSIS periodicamente realiza testes de vulnerabilidades técnicas em sua rede, serviços e aplicações.

Art. 22° Verificações ou auditorias regulares devem verificar a conformidade com as exigências técnicas dos sistemas e das redes.

DA PREVENÇÃO E DETECÇÃO DE INTRUSÃO

Art. 23° O CrediSIS mantém mecanismos de detecção e prevenção a intrusão aptos a mitigar riscos que possam impactar as atividades do sistema.

DA PROTEÇÃO CONTRA MALWARES

Art. 24° O CrediSIS mantém controles *antimalware*, individuais e atualizados, aptos a proteger os dispositivos que possam acessar informações corporativas do CrediSIS.

DOS CONTROLES CRIPTOGRÁFICOS

Art. 25° O CrediSIS mantém controles criptográficos visando a proteção da informação.

DA AQUISIÇÃO E DESENVOLVIMENTO SEGURO DE SISTEMAS

Art. 26° O CrediSIS mantém processos de segurança, como documentação concisa, controle e versionamento de código, gestão de atualização de versões, visando o desenvolvimento seguro de sistemas, sejam desenvolvidos internamente ou adquiridos.

DO SERVIÇO DE NUVEM

Art. 27° O CrediSIS poderá utilizar serviços de computação e armazenamento em nuvem, considerando o teor das informações. Qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada ao Banco Central do Brasil.

DA GESTÃO DE FORNECEDORES

Art. 28° O CrediSIS mantém processos de avaliação de fornecedores, inclusive avaliação de risco em relação aos serviços prestados.

DA POLÍTICA DE BACKUP

Art. 29° O CrediSIS mantém Política de *Backup* que estabelece as principais diretrizes e responsabilidades com relação aos processos de *backup* da infraestrutura de TI e dados da CrediSIS, visando garantir a sua segurança, disponibilidade, integridade e a continuidade do negócio.

DA POLÍTICA DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 30° O CrediSIS mantém Política de Gestão de Incidentes de Segurança da Informação, que estabelece as diretrizes a serem seguidas para que estes incidentes sejam tratados adequadamente, reduzindo ao máximo os impactos para o negócio.

DAS PENALIDADES

Art. 31° O descumprimento das regras e diretrizes impostas neste documento estão sujeitas às penalidades cabíveis.

DAS DISPOSIÇÕES FINAIS

Art. 32° Esta política deverá ser revista e atualizada, ao menos anualmente, com vistas a se manter em sintonia com as regras de negócios, com as melhores práticas do mercado, leis, regulamentos e demais aspectos.

Art. 33° A política a que se refere este resumo foi aprovada em reunião extraordinária realizada em 26 de outubro de 2022.