CRESOL CONFEDERAÇÃO

POLÍTICA DE SEGURANÇA CIBERNÉTICA E INFORMAÇÃO

V: 1.1 – Validade: 24/11/2020

Histórico de revisões:

Versão	Data	Descrição	Responsável
1.0	15/06/2019	Elaboração	Márcio Falcão
1.1	30/09/2019	Ajustes e revisão	Márcio Falcão
1.1	24/10/2019	Aprovação da Política pelo Conselho de Administração	Leonardo Santana

1. Introdução

A Política de Segurança Cibernética do Sistema CRESOL estabelece princípios, diretrizes e regras para sistematizar o processo de segurança de informação e riscos cibernéticos, demonstrando que proteção privacidade de dados refletem os valores do Sistema CRESOL, reafirmando o seu compromisso com a melhoria contínua da eficácia do processo de proteção de dados.

2. Princípios

- Confidencialidade: as informações tratadas devem ser de conhecimento exclusivo de pessoas especificamente autorizadas ao seu acesso e manuseio;
- Integridade: as informações devem ser mantidas íntegras, sem modificações indevidas (acidentais ou propositais);
- Disponibilidade: as informações devem estar disponíveis a todas as pessoas autorizadas ao seu acesso e manuseio no tempo requerido;

3. Diretrizes

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, privacidade, disponibilidade e integridade;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;
- Selecionar os mecanismos de segurança da informação, considerando fatores de riscos, tecnologia e custo;
- Assegurar que 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;
- Garantir que ocorrências que podem ser consideradas violações desta Política de Segurança da Informação e Cibernética devem ser avaliadas dentro do plano de resposta a incidentes, onde este deve ser registrado nas ferramentas de registro definidas pela Cresol, dependendo de sua gravidade, deverá ser encaminhada para os Comitês e Comissões internas (ex.: Comitê de

Riscos/Compliance e Controles e Comitê de Segurança Cibernética/Informação) para deliberação quanto ao curso de ação a ser tomada.

- Garantir segurança, integridade e disponibilidade dos ambientes computacionais em toda rede corporativa.

4. Esta Política está relacionada com os seguintes documentos institucionais em vigor:

- Estatuto Social da Confederação de Crédito, das Cooperativas Centrais e Filiadas;
- Regimento Interno da Confederação, das Cooperativas Centrais e Filiadas;
- Código de Conduta Ética da Confederação, das Cooperativas Centrais e Filiadas;
- Política de Gerenciamento Contínuo e Integrado de Riscos do Sistema CRESOL;
- Política de Compliance do Sistema CRESOL;
- Política de Prevenção e Combate à Lavagem de Dinheiro e Combate ao Terrorismo do Sistema CRESOL.

5. Público – Alvo

A Política de Segurança de Segurança Cibernética do Sistema CRESOL destina-se a todos os dirigentes e colaboradores da Confederação de Crédito, Cooperativas Centrais e das Cooperativas Filiadas, assim considerados os diretores, conselheiros de administração e fiscal, colaboradores, estagiários e terceiros que compõe o Sistema CRESOL.

6. Responsabilidades

6.1 Confederação de Crédito e Cooperativas Centrais

6.1.1 Conselho de Administração

- Avaliar e Aprovar a Política de Segurança da Informação e Segurança Cibernética do Sistema CRESOL e as propostas de atualizações e/ou alterações desta Política;
- Cumprir e fazer cumprir a aplicação dos procedimentos descritos nesta Política pela Diretoria da Confederação de Crédito, Cooperativa Central e das Cooperativas Filiadas.

6.1.2 Conselho Fiscal

- Averiguar e fiscalizar o cumprimento da aplicação desta Política pelo Conselho de Administração e pelas Diretorias.

6.1.3 Diretoria de Tecnologia

- Zelar pelo cumprimento desta Política e adequação de melhores práticas, procedimentos e normas relacionadas à Segurança da Informação;
- Revisar esta Política e propor à Diretoria Executiva as alterações quando julgar necessário, a fim de mantê-la atualizada;
- Praticar as ações necessárias para que os procedimentos descritos nesta Política sejam efetivamente implementados, supervisionando e respondendo pelo cumprimento destas, além de manter a Diretoria Executiva e o Conselho de Administração informados acerca dos procedimentos adotados para tanto;
- Garantir a implantação e monitoração do processo de Segurança Cibernética;
- Assegurar a observância das melhores práticas, procedimentos e normas relacionadas à Segurança Cibernética;
- Promover ações de conscientização, treinamento e educação dos usuários quanto à Segurança Cibernética;
- Orientar a adoção de medidas e providências para eliminação ou mitigação de riscos relacionados à Segurança Cibernética;

- Estabelecer as estratégias e demandas das áreas de Negócios e de Tecnologia da Informação, de acordo com as melhores práticas de Segurança Cibernética;
- Gerir os indicadores de Segurança Cibernética reportados pelas áreas gestoras;
- Receber e gerenciar os incidentes de Segurança Cibernética.

6.1.4 Diretoria de Operações

- Zelar pelo cumprimento desta Política e adequação de melhores práticas, procedimentos e normas relacionadas à Segurança Cibernética nos projetos das áreas de negócio, garantindo a confidencialidade, integridade e disponibilidade das informações, envolvendo as áreas de TI para averiguar as escolhas de tecnologias no ínicio dos projetos, a confirmar a completude com as normas relacionadas à Segurança Cibernética e as adequações necessárias em softwares.

6.1.5 Área de Segurança da Informação:

- Prover ao Comitê de Segurança Cibernética/Informação e à Diretoria Executiva todas as informações de gestão de Segurança Cibernética solicitadas;
- Prover ampla divulgação da Política e das Normas de Segurança Cibernética para todos os funcionários, estagiários e prestadores de serviços;
- Promover ações de conscientização sobre Segurança Cibernética para os funcionários, estagiários e prestadores de serviços;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da Segurança Cibernética do Sistema CRESOL;
- Estabelecer procedimentos relacionados à instrumentação da Segurança Cibernética do Sistema CRESOL.

6.1.6 Diretoria de Riscos

- Acompanhar demandas regulatórias relacionadas à Segurança Cibernética e Informação assegurando sua implementação pela Diretoria de Tecnologia;
- Assegurar que os casos de incidentes de Segurança Cibernética e Informação sejam devidamente reportados, encaminhando-os se necessário ao Comitê de Riscos da Cresol Confederação;

- Propor à Diretoria de Tecnologia, pontos de controle e melhorias no processo relacionados à Segurança Cibernética;
- Monitorar a execução dos processos instituídos pela Diretoria de Tecnologia relacionados à Segurança Cibernética.

6.1.7 Diretor de Riscos

- Zelar e responder pelo acompanhamento, supervisão e cumprimento desta Política, em atendimento à regulamentação vigente, adotando as medidas cabíveis para as não conformidades.

6.1.8 Diretoria Executiva

- Zelar e responder pelo acompanhamento, supervisão e cumprimento desta Política, em atendimento à regulamentação vigente, adotando as medidas cabíveis para as não conformidades.

6.2 Cooperativas Filiadas

6.2.1 Conselho de Administração

- Cumprir e fazer cumprir a aplicação dos procedimentos descritos nesta Política pela Diretoria da Cooperativa.

6.2.2 Conselho Fiscal

- Averiguar e fiscalizar o cumprimento da aplicação dos procedimentos descritos nesta Política pela Diretoria e pelo Conselho de Administração da Cooperativa.

6.2.3 Diretoria

- Responder pelo cumprimento desta Política, além de manter o Conselho de Administração informado acerca dos procedimentos adotados para tanto;
- Propor melhorias relativas à Política e Normas de Segurança Cibernética do Sistema CRESOL para a Diretoria de Tecnologia da Cresol Confederação.

6.3 Usuário da Informação

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança Cibernética;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pelo Sistema CRESOL;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Sistema CRESOL;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual:
- Evitar discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Assegurar que informações confidenciais de qualquer tipo não serão compartilhadas, com exceção de exigências por conformidade de lei.

- Comunicar imediatamente à área de Operações de TI setor de Segurança Cibernética/Informação da Confederação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

7 – Glossários/Definições

Segurança Cibernética: constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento de informações de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

Malwares: a) Vírus: software que causa danos a máquina, rede, softwares e banco de dados; b) Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador; c) Spyware: software malicioso para coletar e monitorar o uso de informações; d) Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja restabelecido;

Engenharia Social: a) Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento; b) Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais; c) Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais; d) Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e) Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes Externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

Usuário da informação: Todos os indivíduos que acessam as informações da organização são usuários, seja funcionário,seja contratado da empresa, seja contratante.

8 – Regras

Seção 1 Fundamentação Legal

1. **Resolução nº 4.658, de 26 de abril de 2018, do Conselho Monetário Nacional.**

Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeira e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

2. **ABNT NBR ISO 27.001:2013 – Tecnologia Cibernética– Técnicas de Segurança – Sistemas de gestão da segurança Cibernética– Requisitos.**

Dispõe sobre os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança Cibernética dentro do contexto da organização.

3. **Norma ABNT NBR ISO 27.002:2013 Tecnologia Cibernética– Técnicas de Segurança – Código de Prática para controles de segurança da informação.**

Dispõe sobre práticas de gestão de segurança Cibernética e normas de segurança Cibernética para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança Cibernética da organização.

Seção II Disposições

O gerenciamento de procedimentos e controles de Segurança Cibernética objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos:

Gestão de acesso às informações	Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente com a aprovação do gestor do responsável e o da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.
Proteção do ambiente	São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, através de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.
Segurança física e lógica	Os equipamentos e instalações de processamento de informação críticas ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais. Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, integridade e disponibilidade. Os colaboradores e terceiros são treinados sobre os conceitos de Segurança Cibernética, através de um programa efetivo de conscientização.
Continuidade dos negócios	O processo de gestão de continuidade de negócios relativo a segurança cibernética, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através da combinação de requisitos como operações,

	colaboradores chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados de nuvem e os testes previstos para os cenários de ataques cibernéticos.
Processamento, armazenamento de dados e computação em nuvem	Para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, a Cresol, assegura-se um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

8 – Medidas Disciplinares/Penalidades

O cumprimento das diretrizes previstas nestas Política, serão monitoradas e fiscalizadas periodicamente pela área de Compliance, e em casos de descumprimento será acionado o Código de Ética e Conduta do Sistema CRESOL, aplicando-se às medidas necessárias cabíveis.