7.7. POLÍTICA DE RISCO CIBERNÉTICO E SEGURANÇA DA INFORMAÇÃO

SUMÁRIO

7.7. POLÍTICA DE RISCO CIBERNÉTICO E SEGURANÇA DA INFORMAÇÃO

7.7.1. Objetivo

A presente Política de Risco Cibernético e Segurança da Informação estabelece os padrões de comportamento e valores que devem nortear as atividades na **Cooperativa de Economia e Crédito Mútuo dos Funcionários Públicos Municipais de Itapira - CREDITA,** fundamentando-se em normas legais, princípios éticos, morais e nos bons costumes.

7.7.2. Introdução

A presente política estabelece as diretrizes e os controles adotados pela, visando assegurar a proteção das informações institucionais e dos ativos tecnológicos, bem como a prevenção e resposta a riscos cibernéticos que possam comprometer a confidencialidade, integridade, disponibilidade e autenticidade dos dados.

Como cooperativa independente do Segmento S5, autorizada pelo Banco Central do Brasil, a **CREDITA** adota práticas proporcionais ao seu porte e complexidade, observando os requisitos mínimos previstos na Resolução do Conselho Monetário Nacional - CMN nº 4.893/2017, que regula o gerenciamento de segurança cibernética nas instituições financeiras.

Esta política contempla:

a) A definição de controles e procedimentos para proteção dos dados e dos sistemas;

b) A classificação e tratamento de incidentes cibernéticos;

c) A elaboração de plano de ação e de resposta a eventos de segurança;

d) A definição de diretrizes de continuidade operacional frente a riscos tecnológicos;

e) A promoção da cultura de segurança entre colaboradores, terceiros e associados.

Ao implementar esta política, a **CREDITA** reforça seu compromisso com a governança digital segura, a conformidade regulatória e a proteção da confiança dos seus cooperados frente aos desafios tecnológicos e às ameaças cibernéticas atuais.

7.7.3. Responsabilidades

7.7.3.1. Todos os Colaboradores

Todos os colaboradores da **CREDITA** são responsáveis por garantir o cumprimento das diretrizes de segurança da informação e zelar pelos ativos tecnológicos sob sua responsabilidade. Para isso, devem:

a) Cumprir integralmente a Política de Segurança da Informação;

b) Acessar apenas as informações da instituição para as quais tenham autorização expressa;

c) Proteger e preservar os recursos computacionais disponibilizados para o trabalho;

d) Notificar imediatamente à Gerência qualquer ocorrência ou indício de ameaça à segurança, como:
- **i.** Vulnerabilidades ou falhas técnicas;
- **ii.** Vírus, malwares ou arquivos suspeitos;
- **iii.** Interceptação de mensagens eletrônicas;
- **iv.** Acessos indevidos a pastas, internet, rede ou softwares não autorizados.

e) Manter o sigilo e a proteção de dados da cooperativa, evitando compartilhamentos ou discussões em ambientes públicos como transportes, restaurantes ou redes sociais;

f) Utilizar seu login e senha de acesso pessoal à rede, e-mail e internet de forma sigilosa e intransferível;

g) É terminantemente proibido compartilhar senhas. O titular será responsabilizado por infrações resultantes do uso indevido por terceiros;

h) Em caso de suspeita de comprometimento da senha, o usuário deve solicitar imediata alteração à Gerência;

i) Nunca abrir arquivos ou anexos de origem desconhecida;

j) Armazenar e proteger adequadamente documentos impressos e arquivos que contenham informações confidenciais;

k) Mensagens eletrônicas e anexos devem ser tratados como material reservado — não podendo ser reproduzidos ou divulgados sem o consentimento formal do remetente.

7.7.3.2. Empresa Prestadora de Serviços de TI

A **CREDITA** mantém contrato com a empresa especializada Rodrigo Mazzer Gracini ME, nome fantasia YeTI, sediada em Itapira/SP, responsável pelo suporte técnico e gerenciamento da infraestrutura de TI da cooperativa.

Serviços Prestados:

a) Suporte aos usuários por chamados técnicos, telefone ou atendimento presencial;

b) Manutenção preventiva e corretiva de equipamentos;

c) Apoio na melhoria da estrutura de TI;

d) Monitoramento de ativos e ambiente de produção;

e) Identificação de vulnerabilidades em sistemas;

f) Administração de servidores, rede e execução de batches;

g) Gestão de backups e operação de ferramentas de segurança (firewall e antivírus);

h) Tratamento de incidentes em múltiplos níveis (usuário, rede e servidores).

Responsabilidades Adicionais:

a) Garantir a **integridade da rede da cooperativa**, com uso de ferramentas atualizadas;

b) Instalar **softwares homologados** pela Diretoria Executiva e desinstalar aplicações consideradas nocivas;

c) Promover a **orientação e capacitação dos colaboradores** sobre boas práticas de Segurança da Informação e Cibernética, visando uso adequado dos sistemas e prevenção de falhas operacionais.

7.7.4. Utilização da Internet e E-mail

7.7.4.1. Uso da Internet

A **CREDITA** disponibiliza acesso à internet aos seus colaboradores como recurso de apoio às atividades profissionais, especialmente para pesquisas e consultas relacionadas aos interesses institucionais.

Todo acesso é realizado exclusivamente através da **rede corporativa**, sendo **monitorado regularmente** pela cooperativa e pela empresa prestadora de serviços de TI (YeTI), com o objetivo de:

a) Preservar a integridade das informações;

b) Identificar vulnerabilidades e falhas de segurança;

c) Garantir o uso adequado da rede e dos recursos digitais.

Caso sejam detectados indícios de quebra de segurança ou ações que possam comprometer a imagem ou os negócios da cooperativa, os serviços de internet poderão ser suspensos sem aviso prévio pela Gerência ou pela YeTI.

É expressamente proibido aos colaboradores:

a) Realizar atividades de interesse pessoal ou negócios particulares;

b) Alterar configurações da rede local ou dos servidores;

c) Comprometer o sigilo das informações da cooperativa;

d) Praticar hostilidade ou ações maliciosas via meio digital;

e) Realizar download de softwares, jogos, arquivos executáveis, músicas ou vídeos não autorizados;

f) Efetuar upload de softwares licenciados ou dados institucionais sem autorização;

g) Propagar vírus, worms, trojans ou qualquer outro software malicioso;

h) Violar leis e acessar conteúdos inapropriados como pornografia, incitação à violência ou manifestações discriminatórias.

7.7.4.2. Uso de E-mail

O e-mail corporativo é fornecido pela **CREDITA** como ferramenta exclusiva de comunicação institucional, sendo seu uso restrito às atividades profissionais do colaborador.

Todas as mensagens enviadas por meio do sistema institucional recebem a assinatura oficial da cooperativa, caracterizando-se como documentação oficial, sujeita às normas éticas e de segurança da informação.

A concessão e permanência do uso do e-mail estão vinculadas aos interesses da cooperativa, podendo ser revogada ou restringida a qualquer tempo.

Regras de uso:

a) O colaborador é responsável pela conta de e-mail sob sua gestão;

b) O e-mail institucional pertence à cooperativa, e não ao colaborador;

c) As mensagens podem ser monitoradas e, se necessário, utilizadas como evidência formal, sem que isso constitua violação de privacidade;

d) A linguagem utilizada nas comunicações deve refletir os valores institucionais, com postura adequada e profissional;

e) As mensagens devem ser removidas sempre que não forem mais úteis às atividades;

f) Impressões de e-mails sensíveis não devem permanecer em impressoras públicas ou compartilhadas.

É vedado aos colaboradores:

a) Configurar ou utilizar contas de e-mail externas (não oficiais);

b) Utilizar o e-mail institucional para envio de propagandas, correntes, conteúdos políticos, religiosos, partidários ou ilegais;

c) Propagar spam, boatos ou conteúdos que não se relacionem com a atividade institucional.

A estrutura de identificação das contas de e-mail seguirá padrão definido pela cooperativa, visando a uniformidade e fácil rastreabilidade das comunicações internas e externas.

7.7.5. Gestão de Acesso aos Sistemas de Informação

Todo acesso às informações e aos ambientes digitais da CREDITA deve ser controlado e restrito a pessoas autorizadas, mediante aprovação do responsável pela informação ou pela sua guarda e integridade.

O **controle de acesso** deve ser formalizado e documentado, contemplando:

a) Solicitação formal da Gerência, tanto para concessão quanto para cancelamento de acesso, realizada:

i. Via sistema de atendimento Mantis (sistemas da Prodaf);

ii. Via chamado técnico à YeTI (serviços de TI) para acesso à rede interna.

b) Verificação da adequação do perfil de acesso ao cargo e função do colaborador;

c) Remoção imediata de autorizações em casos de desligamento, afastamento ou mudança de função.

Todas as criações, remoções e bloqueios de contas de acesso devem ser centralizadas na Gerência.

É responsabilidade individual de cada usuário:

a) Manter a confidencialidade das senhas;

b) Utilizar login e senha de forma segura, conforme diretrizes da política de segurança da cooperativa;

c) Jamais compartilhar credenciais, pois são pessoais e intransferíveis.

A CREDITA adota política de senhas complexas, exigindo:

a) Mínimo de caracteres;

b) Uso de letras maiúsculas e minúsculas;

c) Inclusão de caracteres especiais;

d) Bloqueio automático após 3 tentativas incorretas.

7.7.6. Permissões e Acessos (Rede Interna e Sistema SYSCOOP32 - Prodaf)

Os perfis de acesso aos sistemas e diretórios da cooperativa são individuais e definidos com base nas atribuições de cada colaborador.

Para prevenir conflitos de interesse, o colaborador terá acesso somente às informações e recursos tecnológicos necessários ao desempenho de suas atividades, conforme função e nível de responsabilidade.

Compete à Gerência:

a) Definir os direitos de acesso com base no princípio da essencialidade e limitação;

b) Avaliar solicitações de acesso extraordinárias ou excepcionais, autorizando quando justificadas;

c) Revogar acessos a qualquer tempo, sem aviso prévio, sempre que necessário.

Todos os acessos são controlados por mecanismos de identificação e autenticação, que incluem login e senha, permitindo a rastreabilidade individual das atividades realizadas.

Esses mecanismos devem ser intransferíveis, garantindo a responsabilização individual por todos os acessos e ações executadas nos ambientes digitais da **CREDITA**.

7.7.7. Backup

A **CREDITA** realiza cópias de segurança (backup) como medida fundamental para garantir a proteção e recuperação dos dados e arquivos internos, especialmente aqueles contidos no sistema SYSCOOP32 e nos demais diretórios utilizados pela instituição.

Os procedimentos de backup visam:

a) Proteger a integridade das informações em caso de perda, falha ou incidente tecnológico;

b) Assegurar a disponibilidade de dados em situações de crise ou recuperação de sistemas;

c) Apoiar o plano de continuidade de negócios da cooperativa.

7.7.7.1. Local de Armazenamento dos Backups

A **CREDITA** adota múltiplos ambientes de armazenamento para garantir a integridade e disponibilidade dos dados:

a) Backup local: realizado em dispositivo NAS (Network Attached Storage), acessível à cooperativa e replicável em nuvem (DataSafer);

b) Backup em nuvem (Office 365): armazenado em datacenter externo, com restauração e testes conduzidos pela YeTI, empresa contratada para suporte de TI. Os testes de recuperação são realizados a cada 15 dias;

c) Os colaboradores são orientados a salvar/trabalhar todos os arquivos diretamente da nuvem Office 365, que serve de base para os backups automatizados;

d) Os dados do sistema SYSCOOP32 são armazenados na base Sybase (Amazon Cloud), sob gestão da Prodaf. Restauros devem ser solicitados via sistema Mantis.

7.7.7.2. Conteúdo Abrangido pelos Backups

São incluídos nos backups:

a) Todos os dados e registros gerados e mantidos pelo sistema SYSCOOP32;

b) Arquivos internos da cooperativa, como planilhas, documentos de controle e gestão, entre outros materiais operacionais.

7.7.7.3. Periodicidade dos Backups

A periodicidade dos backups segue o seguinte cronograma:

Tipo de Backup	Frequência	Destino
SYSCOOP32 (banco Sybase)	Diariamente às 21h	Amazon (Prodaf/Sybase)
Sharepoint Office 365 (NAS/Nuvem)	A cada 2 horas	Repositório local e nuvem
Backup completo (NAS/Nuvem)	Mensal	Repositório local e nuvem
Backup incremental (NAS/Nuvem)	A cada 2 horas	Repositório local e nuvem

7.7.7.4. Tempo de Retenção

A política de retenção dos backups é definida conforme a criticidade das informações:

Tipo de Backup	Tempo de Retenção	Local
DUMP do banco SYSCOOP32	7 dias	Sybase
Sharepoint (backup em nuvem)	30 dias	Nuvem
Sharepoint (backup local cada 2h)	30 dias	NAS
Backup completo e incremental	30 dias	NAS/Nuvem

A responsabilidade pelo armazenamento adequado dos arquivos é compartilhada entre todos os colaboradores da cooperativa. Garantir que os documentos estejam salvos no Sharepoint é essencial para a continuidade dos serviços e a recuperação segura das informações em caso de perda ou falha.

7.7.8. Programas e Ferramentas de Segurança da Informação

A **CREDITA** adota um conjunto de ferramentas tecnológicas para proteger seus sistemas e informações contra riscos digitais e operacionais:

a) **Antivírus corporativo:** software Kaspersky com licença ativa por 3 anos, instalado em todas as estações de trabalho e no servidor, para prevenção, detecção e eliminação de ameaças digitais.

b) **Firewall Sophos:** appliance, atua no controle de acessos à internet, bloqueio de páginas maliciosas, inspeção de rede, definição de conteúdos que podem trafegar na rede e rejeição de conexões suspeitas ou invasivas. É monitorado e mantido pela empresa YeTI.

c) **Acronis (DLP – Data Loss Prevention):** ferramenta instalada em terminais para evitar o vazamento de dados sensíveis. Bloqueia ações indevidas ou maliciosas que possam expor informações confidenciais da cooperativa.

d) **Zabbix:** software de monitoramento de redes, servidores e serviços, utilizado para avaliar desempenho, disponibilidade e qualidade dos serviços digitais da instituição.

e) **Nobreaks:** instalados nas estações de trabalho com autonomia de até 20 minutos e no servidor com autonomia de até 40 minutos, garantindo proteção contra quedas de energia e integridade dos dados.

7.7.9. Controles de Acessos Externos

A realização de acessos remotos aos sistemas da **CREDITA** ocorre exclusivamente para fins de manutenção ou suporte técnico, sendo realizados por:

a) YeTI (serviços de TI);

b) Prodaf (sistema SYSCOOP32).

Os acessos são feitos mediante ferramentas seguras como TeamViewer ou AnyDesk, e só são autorizados mediante liberação prévia de ID e senha pela Gerência.

Por questão de segurança, nenhum outro prestador de serviços está autorizado a realizar acessos remotos aos computadores ou servidores da cooperativa. Todos os colaboradores estão cientes dessa restrição.

7.7.10. Monitoramento e Controle da Segurança da Informação

Todos os sistemas, informações e serviços utilizados na **CREDITA** são de propriedade exclusiva da cooperativa e devem ser utilizados apenas para fins profissionais.

i. O uso dos sistemas poderá ser monitorado regularmente. Registros de acesso e atividades podem ser utilizados:
- **a)** Para apuração de descumprimento das normas internas;
- **b)** Como evidência em processos administrativos e legais, quando aplicável.

ii. Serão realizadas avaliações periódicas com os colaboradores, visando:
- **a)** Verificar o grau de conhecimento sobre segurança da informação;
- **b)** Reforçar orientações sobre os princípios e diretrizes desta política;
- **c)** Promover atualizações contínuas e alinhamento com boas práticas.

7.7.11. Registro de Incidentes de Segurança

O monitoramento do ambiente tecnológico da CREDITA é realizado pela empresa YeTI, responsável pela prestação de serviços de TI. O controle é efetuado por meio de um sistema de **chamados (tickets)**, que registra:

a) Ocorrências e atendimentos relacionados ao ambiente computacional;

b) Detecção de falhas, vulnerabilidades ou violações de segurança;

c) Emissão de relatórios periódicos com os resultados das rotinas, procedimentos, controles aplicados e incidentes relevantes identificados.

Caso seja detectado algum incidente relacionado à segurança da informação ou segurança cibernética, seja por um colaborador ou pela equipe técnica, deve-se acionar imediatamente o responsável pela execução do Plano de Continuidade de Negócios (PCN), que adotará os procedimentos definidos nesta política.

7.7.12. Mídias Sociais

A criação de canais oficiais da **CREDITA** em redes sociais é responsabilidade da Gerência, em conjunto com o prestador de serviços de marketing. A publicação de conteúdos, imagens e informações é restrita a esses profissionais autorizados.

Quanto aos demais colaboradores:

a) Têm permissão apenas para acessar os canais oficiais, sendo vedada qualquer publicação ou manifestação em nome da cooperativa sem autorização prévia e formal;

b) Toda menção pública à cooperativa é monitorada pela Gerência e pelo marketing, com foco na preservação da reputação institucional e imagem corporativa;

c) Caso um colaborador identifique algum conteúdo potencialmente prejudicial à cooperativa, como publicações ofensivas, uso indevido da marca ou exposição de dados sigilosos, deverá comunicar imediatamente a Gerência para ação preventiva.

O acesso corporativo às mídias sociais é monitorado via rede institucional, com o objetivo de proteger os ativos, a imagem e os interesses da **CREDITA** e de seus públicos relacionados.

A cooperativa poderá, a seu critério e sem aviso prévio, inspecionar ou suspender o acesso corporativo do colaborador aos perfis oficiais ou a conexões relacionadas, caso entenda necessário para manter a integridade das operações e da comunicação.

Os dados gerados e monitorados são armazenados para fins administrativos e legais, e poderão ser compartilhados com autoridades competentes em caso de investigação.

Todos os colaboradores são responsáveis pela proteção dos ativos tangíveis e intangíveis da cooperativa, devendo cumprir integralmente esta política, a legislação vigente no Brasil e os normativos complementares aplicáveis.

7.7.13. Segurança Física

A segurança física é essencial para proteger os ativos da **CREDITA** contra acesso não autorizado, danos acidentais ou intencionais, e interrupções operacionais causadas por eventos externos.

7.7.14. Perímetro de Segurança Física

As áreas destinadas ao armazenamento e processamento de dados devem ter seu perímetro claramente delimitado, com medidas que dificultem o reconhecimento externo da finalidade dos espaços.

Instalações críticas devem ser localizadas em áreas de acesso restrito, discretas e com o menor número possível de indicações visuais que revelem a natureza dos recursos ali mantidos.

7.7.15. Controles de Acesso Físico

O acesso a ambientes que abrigam informações sensíveis e sistemas críticos da cooperativa deve ser restrito a colaboradores autorizados, mediante validação pela Gerência.

Os terceiros prestadores de serviços só poderão acessar essas áreas mediante necessidade comprovada e autorização formal da Gerência. Toda movimentação em áreas de processamento deve ser controlada, registrada e monitorada.

7.7.16. Proteção contra Ameaças Externas e do Meio Ambiente

A escolha e a manutenção dos locais destinados ao processamento e armazenamento de informações sensíveis devem considerar os riscos físicos e ambientais do entorno, como:

i. Incêndios em edificações vizinhas;

ii. Vazamentos de água em telhados ou pisos inferiores;

iii. Explosões, interferências elétricas ou problemas com o suprimento de energia;

iv. Ações criminosas, vandalismo ou manifestações externas.

Devem ser implantadas medidas de proteção física compatíveis com o nível de risco, incluindo:

a) Sistemas de combate a incêndio e sensores de fumaça;

b) Isolamento contra umidade e sistemas de drenagem;

c) Redundância elétrica e proteção contra quedas de energia;

d) Barreiras contra invasão e controle de acesso físico;

e) Isolamento contra radiação eletromagnética, quando necessário;

f) Planos de contingência e resposta a emergências.

7.7.17. Contratação de Serviços de Processamento, Armazenamento de Dados e Computação em Nuvem

A contratação de serviços de terceiros para processamento e armazenamento de dados — incluindo serviços de computação em nuvem, no Brasil ou no exterior — representa uma fonte significativa de riscos cibernéticos e operacionais.

Diante disso, a **CREDITA** adota cuidados proporcionais à criticidade dos serviços contratados, conforme exigências regulatórias e práticas prudenciais.

7.7.18. Exigências para a Contratação

Antes da contratação, a **CREDITA** deverá verificar se o prestador atende a requisitos mínimos de governança e segurança, tais como:

a) Práticas de Governança e Gestão
- **i.** Política formal de Segurança da Informação;
- **ii.** Plano de Continuidade Operacional;
- **iii.** Processo de Gestão de Mudanças;
- **iv.** Procedimentos formais de Gestão de Incidentes.

b) Requisitos Técnicos e Regulatórios
- **i.** Conformidade com a legislação e regulamentação vigente;
- **ii.** Acesso da cooperativa aos dados processados ou armazenados;
- **iii.** Garantia da confidencialidade, integridade, disponibilidade e recuperação dos dados;
- **iv.** Certificações compatíveis com os serviços contratados;
- **v.** Relatórios auditados por empresa independente especializada;
- **vi.** Transparência nas informações e nos recursos de gestão;

vii. Controles físicos ou lógicos para segregação dos dados;
viii. Efetividade nos controles de acesso aos dados sensíveis dos cooperados.

7.7.19. Avaliação da Relevância dos Serviços

A avaliação dos prestadores deve considerar:

a) Grau de criticidade dos serviços contratados;

b) Sensibilidade dos dados envolvidos;

c) Mecanismos adotados para mitigação de vulnerabilidades, especialmente em versões de aplicativos acessadas via internet.

7.7.20. Comunicação ao Banco Central

A Cooperativa deverá comunicar ao Banco Central do Brasil, em até 10 dias corridos após a contratação ou alteração contratual, os seguintes dados:

a) Nome da empresa contratada;

b) Serviços relevantes contratados;

c) Localização (país e região) onde os dados serão processados ou armazenados.

Para Contratação no Exterior:

A contratação dependerá da observância dos seguintes requisitos:

a) Existência de convênio entre o Banco Central e autoridades supervisoras locais;

b) Garantia de funcionamento regular da cooperativa e não obstrução da supervisão brasileira;

c) Definição prévia das regiões onde os serviços serão prestados;

d) Plano alternativo para continuidade operacional em caso de suspensão contratual.

Caso não haja convênio:

a) A cooperativa deverá solicitar autorização formal ao Banco Central:

b) Prazo mínimo: 60 dias antes da contratação ou alteração contratual.

Além disso, é necessário garantir que legislações locais não restrinjam o acesso do Banco Central e da cooperativa aos dados, informações e registros contratados.

7.7.21. Requisitos Contratuais

Os contratos firmados devem contemplar:

a) Escopo e Localização dos Serviços:
- **i.** Países e regiões onde os serviços serão prestados e os dados armazenados.

b) Segurança e Acesso aos Dados
- **i.** Medidas para transmissão segura e armazenamento protegido;
- **ii.** Segregação e controle de acesso a dados sensíveis enquanto o contrato estiver vigente.

c) Procedimentos em Caso de Extinção do Contrato
- **i.** Transferência segura dos dados à cooperativa ou ao novo prestador;
- **ii.** Exclusão dos dados pela empresa substituída, após confirmação da integridade da transferência.

d) Garantias de Transparência e Monitoramento
- **i.** Acesso da cooperativa a informações técnicas, certificações e relatórios de auditoria;
- **ii.** Compartilhamento de informações de gestão e subcontratações relevantes;
- **iii.** Permissão expressa de acesso do Banco Central a contratos, dados, backup, documentação e códigos de acesso.

e) Responsabilidades Legais e Regulatórias

- **i.** Atendimento às determinações do Banco Central;
- **ii.** Notificação imediata de restrições legais ou operacionais que possam afetar a prestação dos serviços;
- **iii.** Compromissos específicos para o caso de regime de resolução da cooperativa, incluindo:
- **iv.** Acesso irrestrito do responsável pelo regime aos ativos digitais e contratos;
- **v.** Notificação prévia (30 dias) de intenção de interrupção;
- **vi.** Aceitação de prorrogação adicional de 30 dias, quando solicitada.

7.7.22. Prevenção e Proteção ao Risco Cibernético

7.7.22.1. Mitigação de Riscos

A **CREDITA** adota um conjunto de medidas preventivas com o objetivo de mitigar riscos e reduzir a probabilidade de ataques cibernéticos, promovendo um ambiente digital seguro e resiliente.

Todos os colaboradores devem:

a) Zelar pela integridade dos equipamentos utilizados nas atividades profissionais (computadores, notebooks, acesso à internet, e-mail);

b) Utilizar os recursos tecnológicos exclusivamente para fins institucionais legítimos;

c) Solicitar autorização do Diretor responsável pela Segurança Cibernética para instalação de qualquer software ou arquivo externo, observando direitos autorais e licenciamento;

d) Reconhecer que mensagens eletrônicas e navegação na internet podem ser monitoradas pela cooperativa;

e) Manter senhas individuais seguras, não compartilhadas e não armazenadas de forma não criptografada;

f) Evitar senhas baseadas em dados pessoais ou padrões óbvios;

g) Solicitar alteração imediata da senha caso haja suspeita de acesso indevido.

7.7.22.2. Ações de Prevenção

Para garantir a efetividade da segurança cibernética, a cooperativa implementa os seguintes controles:

a) Inventário atualizado de hardware e software, com verificação periódica;

b) Atualização constante dos sistemas operacionais e aplicativos;

c) Monitoramento e testes regulares de backup e de restauração de dados;

d) Análise recorrente de vulnerabilidades tecnológicas;

e) Testes do plano de resposta a incidentes com simulações de cenários adversos.

7.7.22.3. Tratamento de Incidentes

São considerados incidentes cibernéticos relevantes:

a) Queda prolongada de energia elétrica;

b) Falhas de conexão ou indisponibilidade de servidores;

c) Ataques DDOS, sabotagens, acesso não autorizado;

d) Interrupções nos serviços essenciais da cooperativa.

7.7.22.4. Procedimentos:

7.7.22.4.1. Avaliação Inicial

a) Avaliação conjunta com a Diretoria Executiva;

b) Verificação de recorrência, gravidade e impactos;

c) Determinação de medidas corretivas.

7.7.22.4.2. Incidente Caracterizado

a) Adoção imediata de ações de contingência (redirecionamento de serviços, ativação de redundância);

b) Avaliação do impacto com suporte técnico especializado (YeTI);

c) Registro de boletim de ocorrência, quando aplicável;

d) Comunicação aos cooperados afetados;

e) Notificação ao Banco Central do Brasil nos casos de crise, definidos como interrupções superiores a 24 horas.

7.7.22.4.3. Recuperação

a) Após contenção do incidente, inicia-se fase de recuperação de sistemas, restauração de dados e verificação de integridade;

b) Notificação à Diretoria sobre quaisquer dados corrompidos ou ausentes.

7.7.22.4.4. Retomada

a) Retorno gradual às operações normais;

b) Implementação de ajustes, melhorias, reposição de equipamentos e medidas preventivas.

7.7.23. Monitoramento e Testes

O ambiente de TI é monitorado continuamente com foco na:

a) Detecção de usuários, dispositivos ou componentes não autorizados;

b) Identificação de ameaças como invasões, phishing, vazamento de dados ou instalação indevida de softwares.

7.7.23.1. Testes semestrais de cibersegurança devem verificar:

a) Capacidade instalada e desempenho da rede;

b) Tempo de resposta de serviços críticos e internet;

c) Períodos de indisponibilidade;

d) Vulnerabilidades e riscos operacionais.

7.7.24. Documentação à Disposição do Banco Central

A **CREDITA** manterá os seguintes documentos à disposição do Banco Central por, no mínimo, 5 (cinco) anos:

a) Política de Segurança Cibernética vigente;

b) Ata de aprovação pela Diretoria Executiva;

c) Plano de Ação e Resposta a Incidentes;

d) Relatórios anuais de incidentes de segurança da informação e segurança cibernética;

e) Documentos relativos à contratação de serviços relevantes de tecnologia;

f) Contratos de serviços prestados no Brasil e no exterior (se aplicável);

g) Registros de monitoramento da efetividade da política;

h) Critérios internos que configuram situação de crise.

7.7.25. Compartilhamento de Informações sobre Incidentes Relevantes

Em atendimento à Resolução CMN nº 4.893/2017, a **CREDITA** compartilhará informações sobre incidentes cibernéticos relevantes por meio da Federação Nacional das Cooperativas de Crédito – FNCC.

Esse compartilhamento será feito de forma técnica e sigilosa, com o objetivo de:

a) Alertar outras instituições sobre riscos emergentes;

b) Fortalecer a segurança coletiva do setor cooperativo;

c) Contribuir para ações coordenadas de resposta e prevenção.

A identidade dos envolvidos será preservada e as comunicações seguirão diretrizes acordadas entre a cooperativa e a FNCC.

7.7.26. Relatório sobre os Incidentes de Segurança Cibernética e Segurança da Informação

A **CREDITA** emitirá, anualmente, com data-base de 31 de dezembro, o Relatório de Incidentes de Segurança da Informação e Segurança Cibernética, em conformidade com os requisitos da Resolução CMN nº 4.893/2017.

Esse relatório tem como objetivo demonstrar a eficácia da Política de Segurança Cibernética e a capacidade da instituição em prevenir, detectar e responder a incidentes relevantes, garantindo a continuidade dos negócios e a proteção dos ativos digitais.

O relatório deverá conter, no mínimo:

a) Avaliação da efetividade das ações implementadas no âmbito da Política de Segurança Cibernética;

b) Resumo dos resultados das rotinas, procedimentos, controles e tecnologias adotadas;

c) Registro dos incidentes cibernéticos relevantes ocorridos no período, com classificação e tratamento aplicado;

d) Resultados dos testes de continuidade operacional, considerando cenários de indisponibilidade causados por incidentes.

O documento será elaborado até 31 de março do ano seguinte ao da data-base e deverá ser formalmente aprovado pelo Diretor responsável pela Segurança Cibernética, com registro em ata e arquivamento conforme os prazos legais aplicáveis.

7.7.27. Atendimento à Política de Privacidade e Proteção de Dados - LGPD

Todos os procedimentos e diretrizes desta política são realizados em conformidade com a Política de Privacidade e proteção de dados da Cooperativa, a qual dispõe sobre o tratamento de dados em observância da Lei nº 13.709/18.

7.7.28. Disposições Finais

A Política de Risco Cibernético e Segurança Cibernética será aprovada e revisada a cada 2 (dois) anos, ou quando houver exigências / alterações dos órgãos normativos, pela Diretoria Executiva da que deverá assegurar sua divulgação, bem como manter documentação relativa à disposição do Banco Central do Brasil.

Este documento é parte integrante da estrutura de controles internos e gerenciamento de riscos. Conheça a estrutura completa no item **1.1 – ESTRUTURA DE CONTROLES INTERNOS E GERENCIAMENTO DE RISCOS.**

7.7.29. Controle de Atualizações

Data da atualização	Instrumento de atualização	Atualizações
30/09/2025	Atualização periódica	Revisão geral e atualização do layout.

		Unificação das políticas anteriormente vigentes: 7.11 – Política de Segurança da Informação e 7.13 – Política de Segurança Cibernética.

Raquel Cássia de Campos
Diretora Presidente

Luciano Donisete Couto
Diretor Administrativo

Renata Delalana Figueredo
Diretora Operacional