POLÍTICA
DE SEGURANÇA CIBERNÉTICA
E DA INFORMAÇÃO

RESOLUÇÃO:	**4.893/2021**
DIRETOR RESPONSÁVEL:	**DIRETOR ADMINISTRATIVO FINANCEIRO**
APROVADA EM REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO EM:	**DEZEMBRO/2021**
RELATÓRIO DAS ATIVIDADES	
PRÓXIMA REVISÃO EM:	**Até DEZEMBRO/2022**

Cooperativa de Economia e Crédito Mútuo dos Colaboradores do Grupo Empresarial A Costa Ltda
Rodovia MG 22, Km 105 – Barra dos Coutos – Visconde do Rio Branco/MG – CEP 36.520-000

SUMÁRIO

Sumário

1. DEFINIÇÃO

A presente política visa atender à resolução 4.893, de 26 de fevereiro de 2021, do Banco Central do Brasil, que estabelece a implementação da Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados de computação em nuvem, bem como assegurar princípios e diretrizes básicas que garantem a integridade, confidencialidade, disponibilidade e autenticidade dos dados, observando o porte, o perfil de risco e os negócios desenvolvidos, a natureza das operações, a complexidade dos produtos, serviços, atividades e processos, assim como a sensibilidade dos dados e das informações sob responsabilidade da cooperativa.

A cooperativa está enquadrada no porte de Singular S5, onde o nível de risco é considerado baixo, com operação de capital/empréstimo com consignação na folha de pagamento.

2. OBJETIVO

Essa política tem como propósito promover uma base comum para as práticas efetivas de gestão de segurança da informação e solidificar a confiança nos relacionamentos entre a Cooper Cred Pif Paf e seus STAKEHOLDERS.

A informação representa um dos bens mais valiosos de uma organização, contribuindo para a continuidade dos negócios, minimizando os riscos de perdas financeiras, melhorando a imagem da empresa no mercado, auxiliando na descobertas de novas oportunidades de negócios, dentre outros.

Pelo seu grau de importância, pois pode ser transmitida pelos mais variados meios e seja qual for esse meio a informação compartilhada ou armazenada deve ser adequadamente protegida.

A segurança da informação é baseada em 03 pilares:

Confidencialidade: garantia de que a informação é acessivel somente a pessoas autorizadas;

Integridade: salvaguarda da exatidão e completude da informação;

Disponibilidade: garantia de acesso a informação sempre que preciso.

O objetivo desta Política é orientar a cooperativa no que diz respeito a gestão de riscos e ao tratamento de incidentes de Segurança Cibernética e da Informação, em conformidade com as disposições constitucionais, legais e regimentais vigentes, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da cooperativa, dos cooperados e envolvidos. A segurança cibernética e da informação, não pode se limitar somente aos ativos físicos e tecnológicos onde transitam os dados ou são armazenados, e sim a proteção desses dados.

2.1 – Princípios:

A segurança da informação está baseada na proteção preventiva de toda a cadeia de dados confidenciais ou não processados que são de responsabilidade da cooperativa e manuseados pelos membros estatutários ou colaboradores, visando a plena confidencialidade desses dados nas diversas formas que são gerados, com ênfase no armazenamento cibernético.

Toda informação produzida ou recebida pelos colaboradores, como resultado da atividade profissional contratada pela Cooper Cred Pif Paf, pertence à cooperativa.

Os equipamentos são usados pelos colaboradores/diretores para atividades profissionais, sendo VEDADO seu uso para atividades particulares.

2.2 - Aspectos da segurança cibernética que irão nortear esta política:

I - Objetivos da Segurança Cibernética: Assegurar a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados.

II - Procedimentos e controles adotados para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos objetivos da segurança cibernética: Esses procedimentos requerem controles, como os níveis de acesso às informações, a contínua vigilância e, principalmente, sistemas adequados e confiáveis contratados para processamentos e armazenamento de dados.

III – Controles específicos que busquem garantir a segurança das informações sensíveis, incluindo os voltados para a rastreabilidade da informação: Esses procedimentos requerem a utilização de equipamentos e programas confiáveis, com a utilização de programas antivírus adequados e capazes de assegurar a confiabilidade da proteção, aliado a uma manutenção preventiva e constante dessas ferramentas. O armazenamento em nuvem deverá ser adotado como princípio de segurança confiável.

IV – O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição: Deve-se estar atento às tentativas de ataques cibernéticos, bem como as apurações em casos de incidentes relevantes ou não, pois qualquer ocorrência demonstrará falhas nas defesas ou prevenções, devendo ser debatidas as ocorrências nos diversos níveis operacionais da cooperativa, buscando aprimorar os mecanismos preventivos.

V- As diretrizes para:

A elaboração de cenários de incidentes considerados nos testes de continuidade de negócios: Deve-se levar em consideração cenários que possam abalar os negócios causando interrupções danosas às operações, acesso e roubos de informações confidenciais, acesso e roubos nas contas de depósitos da Cooperativa, destruição de arquivos e bancos de dados, bloqueio de acessos com a liberação mediante resgates criminosos, entre outros.

A definição de procedimentos e de controles voltados à prevenção e ao tratamento de incidentes a serem adotados por empresas prestadoras de serviços, a terceiros que manuseiam

dados ou informações sensíveis ou que seja relevantes para a condução das atividades operacionais da Cooperativa: Trata-se de uma parte extremamente relevante na política de segurança cibernética, pois a relação da cooperativa e as empresas prestadoras desses serviços deve estar estruturada além da sua capacitação técnica, na confiabilidade recíproca conquistada em anos de relacionamento. Juridicamente deve estar ancorada em contrato, que seja considerado um ato jurídico perfeito, com cláusulas pétreas e preventivas de segurança, além dos aspectos técnicos sobre os serviços contratados e outros, devendo ser revisto periodicamente para atualizações, aperfeiçoando essa relação com uma segurança jurídica garantidora da prestação dos serviços.

A classificação dos dados e das informações quanto a relevância: A cooperativa como instituição financeira, opera com informações protegidas por sigilo de acordo com a Legislação em Vigor (Lei Complementar 105/2001), que relaciona essas operações cuja violação é passível de penalizações. Essas operações elencadas terão tratamento prioritário na classificação de dados na política de segurança cibernética tanto pela relevância, quanto pela penalização imposta por sua violação. O seu manuseio e acesso pelas pessoas, que por dever de ofício tem autorização para fazê-lo, deverão ser cientificadas quanto a violações. Outros tipos de dados e informações poderão ter classificação mais abrandada nas atividades da cooperativa.

A definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes: Como está evidenciado no item "c" anterior, os parâmetros levarão em consideração em primeiro lugar, as informações previstas na Lei Complementar 105/2001 e que a cooperativa por sua classificação está autorizada a operar. Atendida essa relevância, as demais informações serão avaliadas por outros critérios, dentro das relevâncias julgadas pertinentes.

VI – Os mecanismos de disseminação da cultura de segurança cibernética na cooperativa incluindo:

A implementação de programas de capacitação e de avaliação periódica de pessoal: Dentro dos programas de treinamento e capacitação de membros estatutários e colaboradores, a cooperativa incluirá a segurança cibernética como programa de capacitação, bem como avaliação do pessoal.

A prestação de informações a clientes e usuários sobre precaução na utilização de produtos e serviços financeiros: Essa é uma parte sensível no relacionamento entre a cooperativa e seus associados, pois a cooperativa não pode negligenciar nas orientações e precauções na utilização desses serviços. Os colaboradores serão orientados sempre na prestação dos atendimentos e as informações e orientações no trato desses serviços, que são protegidos pelo sigilo previstos na Lei complementar 105/2001.

O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética: A diretoria da cooperativa deverá ter comprometimento prioritário com a segurança cibernética, pois além de ter um diretor indicado responsável pela segurança, deverá estar atualizada no que ocorre na área de

segurança cibernética, atuando preventivamente, cobrando informações e providências diuturnas.

VII – As iniciativas para compartilhamento de informações sobre incidentes relevantes mencionados no inciso IV, com outras cooperativas de crédito: Trata-se de uma prática que não é comum, mas que deve ser buscada em função de que diversos incidentes são comuns, tendo como origem fontes idênticas e o mesmo "modus operandi". Uma das formas seria através das empresas de informática contratadas que prestam serviços a diversas cooperativas e serviriam de elo de compartilhamento de incidentes, que para tanto, deveriam ser autorizadas a divulgarem incidentes ocorridos para ações preventivas. Cabe ressaltar que deverá ser mantido o sigilo das informações no compartilhamento com outras cooperativas.

Deverá ser contemplada a capacidade da cooperativa para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, situação esta, que está ligada aos operadores do sistema de informática (equipamentos e programas), com sistemas adequados de detecção.

Os procedimentos e controles devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção da vulnerabilidade, a proteção contra programas maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, devendo também ser aplicado no desenvolvimento ou contratação de sistemas de informação seguros e na adoção de novas tecnologias empregadas na atividade cooperativa.

O registro, a análise da causa, o impacto, bem como o controle dos efeitos de incidentes devem abranger inclusive informações recebidas das empresas de prestação de serviços de informática contratadas.

As diretrizes devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão, compatíveis com os utilizados pela cooperativa.

A cooperativa está em consonância com a legislação vigente, principalmente em relação a Lei Geral de Proteção de Dados Pessoais – LGPD, Lei 13.709, que tem por finalidade a proteção dos dados, dividindo em:

Dados Pessoais: São aqueles dados que identificam uma pessoa, como nome, sobrenome, RG, CPF, data de nascimento, idade, telefone, e-mail, endereço residencial, etc;

Dados Sensíveis: São aqueles dados que podem levar a discriminação de uma pessoa, como raça ou etnia, opção sexual, religiosidade, opção política, filiação sindical, dados genéticos e biométricos, saúde, entre outros.

A cooperativa tem por princípio, NÃO coletar nenhum dado sensível de seus cooperados.

3. RESPONSABILIDADE E REVISÃO

Função	Responsabilidades
Conselho de Administração	• Deliberar sobre a Política de Segurança Cibernética e da Informação; • Acompanhar a implementação das estratégias referente a política supra citada; • Revisar essa política anualmente.
Diretor Administrativo Financeiro (Responsável indicado no UNICAD)	• Avaliar os riscos da Segurança Cibernética e da Informação; • Assegurar a correção tempestiva das deficiências das estruturas de gerenciamento de Segurança Cibernética e da Informação; • Propor alterações que visem maximizar a segurança cibernética e da informação; • Supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento da Segurança Cibernética e da Informação.
Conselho Fiscal	• Fiscalizar o cumprimento da aplicação dessa Política; • Orientar em caso de descumprimento.
Gerente Executivo	• Assegurar o cumprimento e a aderência de todos os envolvidos na cooperativa com esta política; • Assessorar o Conselho de Administração no aprimoramento, revisão e atualização da política de segurança cibernética e da informação; • Realizar orçamentos para a implementação das ações e estratégias que visem contribuir para a segurança cibernética e da informação; • Capacitar o quadro de colaboradores para a prevenção na segurança cibernética e da informação, seja por meio de capacitações contratadas ou participação em treinamentos oferecidos pelo SESCOOP-MG; • Avaliar e orientar a conduta dos colaboradores;

Analista Administrativa e Estagiárias.	• Cumprir os dispositivos presentes nesta política; • Comunicar ao Gerente Executivo ações suspeitas que comprometem a segurança cibernética ou da informação;
Analista de Controles Internos e Governança Cooperativa	• Propor capacitações ao Gerente Executivo sobre assuntos referentes a Segurança Cibernética e da Informação; • Capacitar anualmente a equipe sobre as definições da presente política; • Promover a disseminação da cultura de Gerenciamento de Segurança Cibernética e da Informação na Cooperativa; • Cumprir os dispositivos presentes nesta política; • Comunicar ao Gerente Executivo ações suspeitas que comprometem a segurança cibernética ou da informação;

4. REGRAS PARA USO DOS RECURSOS DE TECNOLOGIA

A Cooper Cred Pif Paf, possui atualmente 06 notebooks que são disponibilizados a seus funcionários e estagiários, para serem utilizados EXCLUSIVAMENTE, em suas tarefas a serviço da Cooperativa.

Os recursos tecnológicos que são de propriedade da cooperativa, são autorizados e disponibilizados exclusivamente para os usuários desempenharem suas funções a serviço da cooperativa.

A comunicação através dos recursos tecnológicos deve ser formal e profissional, dentro da ética, de modo a preservar a imagem institucional da cooperativa.

Os conteúdos acessados e transmitidos através dos recursos de tecnologia devem ser legais, bem como a utilização de equipamentos e programas, de modo a contribuir para atividades profissionais dentro da ética.

Cada usuário é responsável pelo uso dos recursos tecnológicos que lhe for confiado e autorizado, que estarão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas instalados, sendo vedado o uso de programas ilegais nos equipamentos.

Os recursos de tecnologia da cooperativa disponibilizados para os usuários, não podem ser repassados para terceiros, estranhos à cooperativa, salvo em caso de autorização expressa.

Qualquer anormalidade ou irregularidade nos recursos de tecnologia, devem ser comunicados de imediato aos superiores hierárquicos.

4.1 – Regras para uso do notebook:

Os computadores disponibilizados para os usuários são de propriedade da cooperativa, e devem ser utilizados com zelo e os cuidados necessários para assegurar seu pleno funcionamento dentro da vida útil estimada do equipamento.

A utilização dos equipamentos poderá implicar/exigir a utilização de senha específica e login de acesso, bem como limites de acesso, de modo a que se possa identificar a qualquer

tempo, o usuário na realização de tarefas, pois a senha e o login serão assinatura digital do usuário.

É vedada a cessão de senha pelo usuário, sendo de sua inteira responsabilidade tal ocorrência, pois ela é pessoal e intransferível.

Os programas básicos, operacionais e aplicativos instalados nos computadores são de responsabilidade da cooperativa, cabendo ao usuário a sua correta utilização.

Bloqueios de acesso podem ser implantados como formas preventivas de incidentes, devendo o usuário estar sempre atento a atualizações de programas de proteção antivírus, tentativas de ataques, programas maliciosos e outras situações que possam redundar em incidentes, devendo estar sempre atento a realizar cópias de segurança dos programas e arquivos, armazenando-as em local seguro.

O usuário está ciente de que a instalação ou utilização de programas não autorizados, constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/1998, sujeitando os infratores a pena de detenção e multa.

A cooperativa não se responsabiliza por qualquer ação individual que esteja em desacordo com a lei mencionada, sendo considerada sua prática, uma ameaça à segurança da informação e será tratada com aplicação de ações disciplinares.

4.2 - Regras para uso da internet:

As regras visam basicamente o desenvolvimento de um comportamento ético e profissional na instituição.

O uso da internet para fins pessoais será permitido, COM MODERAÇÃO, e desde que não prejudique o andamento dos trabalhos nas unidades. Sites pornográficos, jogos, apostas e similares são proibidos.

É proibida a divulgação e/ou compartilhamento indevido de informações da área administrativa em listas de discussões, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha a surgir na internet.

Os colaboradores estão proibidos de realizar download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

4.3 – Regras para uso do Correio Eletrônico:

O uso do correio eletrônico é para fins corporativos e relacionados a atividade do colaborador dentro da instituição. A utilização deste serviço para fins pessoais é permitida desde que seja feita com muito bom senso e que não prejudique a cooperativa e não atrapalhe o tráfego da rede.

No caso de endereço eletrônico individual para usuário, este é intransferível e pertence à cooperativa, sendo o mesmo enquanto permanecer o vínculo com a cooperativa.

O usuário que utiliza o endereço individual do correio eletrônico da cooperativa, é responsável por todo o acesso, conteúdo de mensagens e uso relativo ao seu e-mail, podendo enviar mensagens necessárias ao seu desempenho profissional e a sua atuação na cooperativa.

O usuário deve estar ciente que o correio eletrônico da cooperativa deve ser utilizado para os serviços da instituição em todos os seus aspectos formais e profissionais, devendo abster-se

de uso particular ou em benefício de terceiros não autorizados, salvo se previamente autorizado.

4.4 – Regras da Estação de Trabalho:

Cada colaborador possui sua própria estação de trabalho. Tudo o que venha a ser executado de sua estação, acarretará responsabilidades do próprio.

Nenhum software/hardware poderá ser instalado sem autorização.

É proibido manter filmes, músicas, fotos pessoais na estação de trabalho.

É obrigatório que o usuário quando não estiver utilizando a estação efetue o Logoff na mesma.

4.5 – Regras para Uso do Telefone:

A cooperativa disponibiliza telefone fixo e celular para utilização dos colaboradores/diretores, liberados para prestarem serviço na instituição, para atendimento ao quadro social e ao público em geral.

Os atendimentos devem ser formais e objetivos aos usuários e clientes, fornecedores e ao público em geral.

Os telefones poderão ser usados para recebimento ou chamadas particulares, em casos estritamente necessários e urgentes, mas sempre com objetividade de brevidade de modo que as linhas estejam prontamente liberadas.

O uso racional das linhas telefônicas pressupõe economia no custo mensal com telefone, devendo ser buscado e implementado por todos.

4.6 – Regras Gerais do Comportamento Seguro:

O acesso à cooperativa é vedado para aqueles que não são membros estatutários, colaboradores e/ou prestadores de serviço.

Os dados confidenciais não podem ser acessados de maneira alguma por quem não é permitido. O atendimento ao quadro social e ao público em geral, deve ser de forma destacada, sem acesso ao local de trabalho da equipe.

Todo o lixo de informações confidenciais deve ser descartado utilizando a fragmentadora de papéis.

O colaborador ou os diretores liberados para prestarem serviço na cooperativa devem adotar um comportamento seguro quanto a não compartilhar e nem divulgar sua senha a terceiros, não transportar informações confidenciais sem o conhecimento e/ou devida autorização, não discutir assuntos confidenciais em ambiente público, não abrir e-mails com mensagens de origem desconhecida ou suspeita, armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos com informações confidenciais, e por fim, seguir corretamente a política de segurança cibernética para uso da internet e correio eletrônico ou outras formas de comunicação.

5. SEGURANÇA NO ARMAZENAMENTO DO BANCO DE DADOS DA COOPERATIVA

A Cooper Cred Pif Paf, contratou a PRODAF INFORMÁTICA, amesma empresa fornecedora do seu sistema operacional, SYSCOOP 32, para gerenciamento do seu Banco de Dados

Serviços contratados, conforme contrato assinado entre as partes, para direito de uso dos seguintes programas ou serviços:

I. Syscoop 32;
II. Sycoop Web e App;
III. Prodaf CLOUD;
IV. Prodaf HOST.

Documentos complementares dessa política:

I. Prodaf Informática – Condições Gerais de Contratação de Direito de Uso e Prestação de Serviços;
II. Prodaf Informática – Política de Segurança da Informação;
III. Prodaf Informática – Plano de Resposta a Incidentes de Segurança da Informação.

6. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação da cooperativa estabelece os principais controles, denominados diretrizes:

I. As informações da Cooperativa, dos cooperados e de todos os envolvidos devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida;
II. A informação deve ser utilizada de forma transparente e apenas para finalidade para a qual foi coletada;
III. Todo processo, durante o seu ciclo de vida, deve garantir a segregação de funções por meio da participação de mais de um colaborador, para que a atividade não seja executada e controlada por uma única pessoa;
IV. O acesso às informações e recursos só deve ser feito se devidamente autorizado;
V. A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-a como responsável pelas ações realizadas;
VI. A concessão de acessos deve obedecer a critérios de menor privilégio, no qual os usuários têm acesso somente aos recursos e informações imprescindíveis para o pleno desempenho de suas atividades;
VII. A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;
VIII. Os riscos às informações da cooperativa devem ser reportados ao Gerente, e esse, ao Diretor Responsável pela área de Segurança da Informação;

As responsabilidades quanto à Segurança Cibernética e da Informação devem ser amplamente divulgadas aos colaboradores e estagiários, que devem entender e assegurar estas diretrizes.

7. TRATAMENTO DA INFORMAÇÃO, PROCEDIMENTOS E CONTROLE

A informação deve receber proteção adequada em observância aos princípios e diretrizes

de Segurança da Informação da cooperativa em todo seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

No intuito de registrar procedimentos e controles para reduzir a vulnerabilidade da cooperativa a incidentes e atender aos demais objetivos de Segurança Cibernética, e através disso prover controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis, apresentamos a seguir as principais orientações para manter seu computador seguro:

I - Mantenha o sistema operacional do seu computador e seus programas sempre atualizados para protegê-los contra as falhas de segurança;

II - Somente instale programas com a permissão da área de TI da empresa;

III – Não abra e-mails de arquivos enviados de fontes desconhecidas;

IV – Ao compartilhar recursos de seu computador, estabeleça senhas para os compartilhamentos e permissões de acesso adequadas;

V - Fique atento aos endereços acessados no seu navegador;

VI – Na utilização de internet banking procure pelos sinais de segurança;

VII – Troque suas senhas com frequência, ela é pessoal e intransferível e criada de acordo com as funções permitidas para o exercício das suas atividades;

VIII – A maioria das redes sem fio usa algum tipo de configurações de segurança. Essas configurações de segurança definem a autenticação (como o dispositivo se identifica para a rede) e a criptografia (como os dados são criptografados à medida que são enviados através da rede). Procure sempre acessar redes seguras;

IX – Ao detectar algum erro é importante que seja rastreado, através de tecnologias disponíveis todo o caminho do processo, para corrigir o ponto onde o erro aconteceu ou iniciou.

Ressaltamos que a simples aplicação destas recomendações auxilia, porém não garante a segurança da informação. Orientamos que no caso de dúvidas, não seja executado nenhum procedimento sem o conhecimento e orientação de pessoas regularmente habilitadas para sanar quaisquer dúvidas e executar procedimentos de segurança, procure a área de TI da empresa.

Os procedimentos acima descritos buscam abranger no mínimo a autenticação, criptografia, prevenção, detecção e possíveis vazamentos de informação, a realização periódica de testes e varreduras para detecção de vulnerabilidade, bem como a proteção contra software maliciosos, e o estabelecimento de mecanismos de rastreabilidade. Buscam prover ainda, o controle de acesso e segmentação da rede, a manutenção de cópias de segurança dos dados e das informações e o desenvolvimento de sistemas seguros.

8. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Cooper Cred Pif Paf adota os seguintes processos:

a) Gestão de ativos da informação.

Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos (“software” e “hardware”) e não tecnológicos (pessoas, processos e dependências físicas).

Os ativos da informação devem ser identificados de forma individual, inventariado e

protegido de acesso indevido, fisicamente e logicamente, ter documentos e planos de manutenção.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

c) Gestão de acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da cooperativa.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o usuário do computador, para que seja devidamente responsabilizado por suas ações.

d) Gestão de riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os ativos da informação da cooperativa, para que sejam recomendadas as proteções adequadas.

Os cenários de riscos de segurança da informação são escalonados nos setores apropriados, para decisão.

e) Tratamentos de incidentes de Segurança da Informação e Cyber Security

Os incidentes de Segurança da Informação e cibernéticos da cooperativa devem ser reportados à Diretoria Executiva.

f) Conscientização em Segurança da Informação e Cyber Security

A cooperativa promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de Segurança da Informação.

g) Segurança Física do Ambiente

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas.

h) Programa Cyber Security

O programa de Cyber Security da Cooperativa é norteado pelos seguintes fatores:

- Regulamentações vigentes;
- Melhores Práticas;
- Cenário Mundial.

Conforme sua criticidade, o programa divide-se em:

AÇÕES CRÍTICAS: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;

AÇÕES DE SUSTENTAÇÃO: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o nível de risco da cooperativa e permitindo que ações estruturantes de longo prazo possam ser realizadas;

AÇÕES ESTRUTURANTES: Iniciativas de médio/longo prazo que tratam a raiz dos riscos e que preparam a cooperativa para o futuro.

i) Descarte seguro dos dados

Os descartes serão feitos das seguintes formas:

DESCARTE DE DOCUMENTOS FÍSICOS

Verificação no arquivo dos documentos que a área possui armazenados.

Os documentos serão descartados de acordo com os prazos de retenção constantes no "Mapa de Dados Pessoais x Tempo de Retenção", de acordo com a legislação vigente.

Os documentos cujo prazo de retenção já tenham expirado serão descartados, com exceção de documentos que a área entenda que a guarda é necessária por razão específica. Nestes casos a guarda destes documentos será justificada.

DESCARTE DE DOCUMENTOS ELETRÔNICOS

Análise e verificação de todas as pastas constantes no arquivo Y da cooperativa, conferindo os prazos de retenção constantes no "Mapa de Dados Pessoais x Tempo de Retenção" e havendo documentos cujo prazo tenha expirado, estes serão expurgados, mediante a inserção dos arquivos na lixeira e posteriormente deletados.

Eventuais documentos que a área entenda pela necessidade de manutenção, mesmo após o prazo de retenção, serão justificados.

9. GERENCIAMENTO DE INCIDENTES

Tem o objetivo de assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os sistemas de Informação da cooperativa.

O procedimento padronizado para o tratamento de incidentes de segurança compreende as seguintes etapas:

I – Recepção da denúncia ou notificação interna de atividade suspeita: serão aceitas denúncias e a cooperativa colaborará plenamente com a polícia e entidades legalmente competentes na investigação de atividades presumidamente ilícitas provenientes da rede da Cooper Cred Pif Paf, e serão investigados os alertas provenientes dos sistemas de monitoramento da rede, iniciando o processo de tratamento de incidentes de segurança quando for observada atividade em desacordo com os procedimentos éticos de padrões estabelecidos.

II - Medidas de contenção imediatas ao incidente: a contenção imediata ocorrerá por meio de bloqueio de acesso ao host envolvido à rede até o término da investigação.

III – Coleta de Informações e evidências: serão coletadas informações e evidências sobre as atividades denunciadas através dos logs dos diversos sistemas e serviços disponíveis na rede da Cooperativa.

IV – Análise de informações e evidências: todas as informações e evidências serão analisadas para investigar o host que gerou o incidente denunciado. A identificação do host compreenderá a determinação do seu endereço de IP e endereço MAC da interface de rede, nome, switch, porta de acesso, usuário e todas as outras informações possíveis.

O tipo de atividade será determinado pelas informações evidenciadas em logs de serviço. As evidências necessárias serão compiladas para a formalização da notificação dos envolvidos.

V – Notificação dos envolvidos: Será encaminhada notificação por escrito da atividade denunciada ou sob investigação à direção da cooperativa. Cabe ao responsável pelos usuários da máquina alvo de investigação a determinação da origem da atividade, com sua adequada comprovação.

Como origem das atividades pode considerar:

a) Atividade realizada pelo usuário;
b) Atividade realizada por terceiro com autorização do usuário;
c) Atividade realizada por invasor, sem autorização ou conhecimento do usuário.

Como evidência da origem da atividade pode-se considerar:

a) Logs de acesso local ou remoto na máquina;
b) Logs de detecção de vírus, spyware, malware, etc.
c) Outras informações que possam identificar claramente a origem da atividade.

A Diretoria notificada, com auxílio do responsável pela tecnologia da Empresa, avaliará a resposta e determinará as medidas corretivas no host identificado. Nos casos comprovados de invasão e de atividades maliciosas por parte do usuário, o host permanecerá bloqueado até a implantação das medidas corretivas apresentadas.

Qualquer reclamação em relação à utilização ilícita ou questões de segurança do sistema ou da rede, uso indevido de correio eletrônico, violação de direitos autorais ou qualquer atividade em desacordo com a política, devem ser enviadas para o e-mail oficial da Cooper Cred Pif Paf (cooperativa@pifpaf.com.br), com a devida comprovação da atividade.

10. CONTINUIDADE DOS NEGÓCIOS

A Cooper Cred Pif Paf procurará investigar os eventos e incidentes de forma a não influenciar a continuidade dos negócios, principalmente no caso de ocorrer interrupção de serviços relevantes, primando assim pela execução normal das atividades da instituição o mais breve possível, de forma que a interrupção não ultrapasse 24 (vinte e quatro) horas.

Alguns cenários de incidentes que podem influenciar a continuidade dos negócios são: vazamento de dados/informações, indisponibilidade de recursos computacionais, quebra da integridade dos dados, via alteração ou injeção fraudulenta de dados/informações em sistemas e/ou bases de dados, fraudes eletrônicas, incluindo a realização de transações fraudulentas em sistemas de informação da instituição.

A cooperativa deverá comunicar ao Banco Central do Brasil os procedimentos adotados para continuidade dos negócios em caso de ocorrências de incidentes relevantes e das interrupções dos seus serviços, que venha a afetar o funcionamento normal de suas atividades que configurem uma situação de crise pela instituição financeira.

Posteriormente, deverá ser feito um plano de ação em resposta aos incidentes ocorridos, com ações a serem desenvolvidas pela cooperativa, visando adequar suas estruturas, em consonância a Segurança Cibernética e da Informação, sendo o Gerente Executivo o responsável, reportando diretamente ao Diretor responsável por essa política.