



POLÍTICA DE SEGURANÇA CIBERNÉTICA

SUMÁRIO

1. Política de Segurança Cibernética.....	3
2. Princípios da Segurança da Informação.....	3
3. Papéis e Responsabilidades	4
4. Objetivos	5
5. Controles da Segurança da Informação	5
6. Registros de Incidentes Relevantes	6
7. Divulgação da Política de Segurança Cibernética	7
8. Plano de Ação e de Resposta a Incidentes.....	7
9. Avaliação e Contratação de Serviços de TI e de Processamento e Armazenamento de Dados e de Computação em Nuvem	8
10. Comunicações ao Banco Central do Brasil	9
11. Aplicação	10
12. Serviços de Rede	10
13. Armazenamento de Dados.....	10
13.1. FAC – Fácil Informática.....	10
14. Relatório de Testes de Segurança das Informações	11
15. Continuidade dos Negócios	12
16. Considerações Finais.....	13
17. ANEXO I - Relatório de Incidente de Segurança da Informação	14

1. Política de Segurança Cibernética

A política de segurança cibernética tem como objetivo atender a resolução do Conselho Monetário Nacional - CMN nº 4.893/21 e estabelecer os princípios, conceitos, valores e práticas, sobre os requisitos da contratação de serviços de processamentos e armazenamento de dados e de computação em nuvem que devem ser adotados pelos administradores, colaboradores da **Cooperativa de Economia e Crédito Mútuo dos Funcionários da Tetra Pak - COOPERPAK**.

A Diretoria é responsável pela implementação de um sistema de supervisão que demonstre que os controles de segurança da informação estão sendo devidamente executados e alinhados, conforme as exigências do Banco Central do Brasil, considerando o porte e complexidade das operações da **COOPERPAK**, destacando o fato da **COOPERPAK** ter sua sede fora das instalações da empresa mantenedora já há longa data.

2. Princípios da Segurança da Informação

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações, acesso controlado e riscos cibernéticos. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

- i. **Confidencialidade:** proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas, voluntária ou involuntariamente, dados restritos que deveriam ser acessíveis apenas por um determinado grupo de usuários;
- ii. **Integridade:** garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação;
- iii. **Disponibilidade:** prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela;

- iv. **Acesso controlado:** O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. A ameaça à segurança acontece quando há descuido ou possível quebra da confidencialidade das senhas de acesso à rede;
- v. **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.

3. Papéis e Responsabilidades

i. Diretoria

- a) implementar sistema de supervisão que demonstre que os controles de segurança da informação estão sendo devidamente executados e alinhados, conforme as exigências do Banco Central do Brasil.

ii. Coordenador Financeiro

- a) Prover todas as informações de gestão de segurança da informação solicitadas pela Diretoria com o apoio da empresa que presta serviços de T.I. e demais técnicos e consultores quando necessário;
- b) Prover ampla divulgação sobre a Segurança da Informação;
- c) Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da **COOPERPAK**;
- d) Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso da **COOPERPAK**, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- e) Analisar os riscos relacionados à segurança da informação da **COOPERPAK** e propor a alçadas competentes, o aperfeiçoamento do ambiente de controle.

iii. Dos Colaboradores em Geral

- a) Cumprir essa política;
- b) Assegurar que os recursos tecnológicos à sua disposição, sejam utilizados apenas para as finalidades aprovadas pela **COOPERPAK**;
- c) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela **COOPERPAK**;

- d) Garantir que as informações e dados de propriedade da **COOPERPAK** não sejam disponibilizados a terceiros e nem discutidos em ambientes públicos ou em áreas expostas como avião, restaurantes, encontros sociais etc.;
- e) Comunicar imediatamente qualquer fato ou ameaça à segurança dos recursos, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, interceptação de mensagens eletrônicas, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet entre outros.

4. Objetivos

A **COOPERPAK** estabelece as diretrizes para compor um programa completo e consistente de segurança da informação e riscos cibernéticos, visando:

- i. Proteger o valor e a reputação da cooperativa;
- ii. Garantir a confidencialidade, integridade e disponibilidade das informações da **COOPERPAK** contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
- iii. Identificar violações de segurança cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos, dentre outros;
- iv. Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
- v. Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
- vi. Conscientizar, educar e treinar os colaboradores por meio dessa política, normas e procedimentos internos aplicáveis às suas atividades diárias;
- vii. Estabelecer e melhorar continuamente um processo de gestão de riscos de segurança cibernética.

5. Controles da Segurança da Informação

São exigidos alguns controles básicos de segurança da informação:

- i. Plano de ação que precisa ser aprovado pela Diretoria;
- ii. Confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados;
- iii. Controles que considerem o porte da instituição, seu perfil de risco, seu modelo de negócio, seus produtos e a sensibilidade dos dados;

- iv. Controles e procedimentos com rastreabilidade para a garantia da proteção de informações sensíveis. e. classificação de dados ou de informações;
- v. Diretor responsável pela política de segurança cibernética, pela execução do plano de ação e pela gestão de incidentes;
- vi. Implementação de programas de capacitação em segurança;
- vii. Comunicação para clientes e usuários;
- viii. Comprometimento da alta administração.

6. Registros de Incidentes Relevantes

O registro de incidentes **ANEXO I - Relatório de Incidente de Segurança da Informação** toma uma importância muito grande nas normatizações relativas a esse assunto. É exigido a existência e formalização dos seguintes controles relacionados ao registro de incidentes:

- i. Identificação da causa e impactos dos incidentes;
- ii. Planos de ação e planos de resposta para incidentes;
- iii. Área específica para os registros de incidentes;
- iv. Plano de continuidade de negócio e relatório anual – Andamento do plano de ação e resposta para incidentes;
- v. Revisão anual pela Diretoria;
- vi. Tem que ser adotada por empresas prestadoras de serviços para a instituição, que manuseiem informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição.

A cooperativa deve informar ao Banco Central do Brasil (BCB) os incidentes relevantes conforme demais instruções publicadas na resolução CMN nº 4.893/21.

São considerados como incidentes cibernéticos relevantes para este comunicado as interrupções de sistema não planejadas que ocorrem de várias naturezas, que causam danos e afetem os negócios da cooperativa, como por exemplo:

- i. queda de energia elétrica (tempo razoavelmente considerável);
- ii. falha de um elemento de conexão;
- iii. servidor fora do ar, ausência de conexão com internet;
- iv. sabotagem / terrorismo;
- v. indisponibilidade de acesso a cooperativa;
- vi. ataques DDOS, entre outros.

7. Divulgação da Política de Segurança Cibernética

A política de segurança cibernética será divulgada aos funcionários da **COOPERPAK** e às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, podendo a seu critério, considerar tais informações no contrato de prestação de serviço, quando necessário.

A **COOPERPAK** divulgará ao público resumo contendo as linhas gerais da política de segurança cibernética.

Os mecanismos para disseminação da cultura de segurança cibernética na **COOPERPAK** são descritos a seguir:

- a) a implementação de programas de capacitação e de avaliação periódica de pessoal;
- b) a prestação de informações aos associados e usuários sobre precauções na utilização de produtos e serviços financeiros; e
- c) o comprometimento da Diretoria com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

8. Plano de Ação e de Resposta a Incidentes

Fica estabelecido plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética que abrange:

- I. as ações a serem desenvolvidas pela **COOPERPAK** para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;
- II. as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e
- III. a área responsável pelo registro e controle dos efeitos de incidentes relevantes.

Será elaborado relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, que deverá abordar, no mínimo:

- I. a efetividade da implementação das ações a serem desenvolvidas para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética

-
- II. o resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;
 - III. os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e
 - IV. os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório será apresentado à Diretoria até 31 de março do ano seguinte ao da data-base. A política de segurança cibernética e o plano de ação e de resposta a incidentes mencionado devem ser aprovados pela Diretoria.

9. Avaliação e Contratação de Serviços de TI e de Processamento e Armazenamento de Dados e de Computação em Nuvem

A **COOPERPAK** previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, adotará os seguintes procedimentos:

- I. a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e
- II. a verificação da capacidade do potencial prestador de serviço de assegurar:
 - a. o cumprimento da legislação e da regulamentação em vigor;
 - b. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
 - c. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
 - d. a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;
 - e. o acesso da **COOPERPAK** aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
 - f. o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
 - g. a identificação e a segregação dos dados dos clientes da **COOPERPAK** por meio de controles físicos ou lógicos; e
 - h. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados da **COOPERPAK**.

A **COOPERPAK** deve proceder a uma avaliação da relevância contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem considerando:

- i. Criticidade dos serviços a serem prestados, e quando relevantes, aprovadas pela Diretoria depois de avaliação do potencial prestador de serviço candidato no atendimento à cooperativa, sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada;
- ii. Verificação quanto a adoção, por parte do prestador de serviços de controles que mitiguem efeitos de eventuais vulnerabilidades na liberação de novas versões de aplicativos no caso de serem executados através de internet;
- iii. A **COOPERPAK** deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados;
- iv. A **COOPERPAK** é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

Os serviços de computação em nuvem, se contratados, abrangem a disponibilidade à **COOPERPAK**, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- I. processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
- II. implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou
- III. execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

10. Comunicações ao Banco Central do Brasil

A **COOPERPAK** informará previamente o Banco Central do Brasil quando da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, inclusive quando de alterações contratuais. Essa comunicação deverá ser realizada até 10 (dez) dias após a contratação dos serviços e conter as informações:

-
- I. Denominação da empresa a ser contratada;
 - II. Os serviços relevantes a ser contratados;
 - III. A indicação de países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, nos casos de contratação no exterior.

11. Aplicação

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

12. Serviços de Rede

A **COOPERPAK** utiliza os drivers da rede cedidos pela empresa mantenedora que são segmentadas para garantir a segurança e desempenho entre elas. Está implantado um sistema de prevenção de invasão na rede, para garantir a segurança da informação e disponibilidade de serviços.

13. Armazenamento de Dados

A **COOPERPAK** utiliza em parte a rede da empresa mantenedora - as informações administrativas e de Recursos Humanos e pela FAC – Fácil Informática armazenadas as informações do sistema operacional em sistema de nuvem disponibilizado pela **Tetra Pak** – Outlook, Microsoft Office entre outros.

As informações operacionais, financeiras, contábeis, fiscais e indicadores são gerenciadas através do **Sistema FAC – Fácil Informática**.

Com isso seu armazenamento de dados (backup) é realizado de forma segregada a ser apresentada nos itens a seguir descritos.

13.1. FAC – Fácil Informática

A FAC – Fácil Informática, através de seu sistema, realiza o gerenciamento sistêmico e o armazenamento de dados (financeiros, cadastrais, contábeis, fiscais, indicadores e operacionais), através de 17 (dezesete) módulos integrados.

As informações armazenadas em nuvem (cloud) estão protegidas conforme as regras de segurança estabelecidas no contrato firmado com a empresa FAC – Fácil Informática. Esse contrato inclui as empresas subcontratadas, como a Amazon Web

Comentado [MG1]: Valide esse texto com a Facil.

Services (AWS), responsável pela hospedagem e guarda dos dados gerados pela COOPERPAK.

As principais qualidades que o sistema de gestão e a tecnologia Cloud, desenvolvidas pela FAC - Fácil Informática, agregam aos serviços oferecidos para **COOPERPAK** são: praticidade, agilidade e segurança. Com relação a política de Backup, a empresa Fácil Informática realiza Backup diário (1 Backup por dia) de todo o Banco de Dados, utilizando ambiente redundante (replicado) e de alta disponibilidade (99,999999999% de durabilidade e 99,99% de disponibilidade). Os backups serão testados semanalmente (restauração em ambiente de homologação) para garantir sua integridade.

Além dos procedimentos de segurança dos dados descritos acima, a Fácil Informática disponibiliza, diariamente, um arquivo contendo o backup lógico do banco de dados da **COOPERPAK** disponível dentro do ambiente da Amazon, podendo a **COOPERPAK**, mediante senha de acesso, realizar a transferência (download) para sua máquina local utilizando-se do recurso de copiar e colar (Ctrl+C e Ctrl+V).

A Hospedagem é feita no Data Center da Amazon (99.95% de disponibilidade em um período de 365 dias) / (rede de servidores em cluster distribuídos em regiões geográficas diferentes).

Todo contato de suporte é centralizado na FAC – Fácil Informática, não sendo necessário, em nenhum momento, contato direto com Data Center Amazon.

A **COOPERPAK** que está hospedada no cloud, nuvem da FAC – Fácil Informática, ambiente Amazon. O nível de segurança ainda possui ferramentas de firewall, antivírus, ambos atualizados e monitorados diariamente, e análises constantes para detecção de possíveis ataques cibernéticos.

14. Relatório de Testes de Segurança das Informações

Sempre que solicitado pela **COOPERPAK**, o departamento de TI da Fácil Informática, realizará testes dos seus sistemas de segurança de informações, bem como de todos os preceitos contidos na presente política, incluindo, mas não se limitando apenas aos procedimentos de descarte de informações pelos colaboradores, individualização dos usuários, dentre outros.

Estes testes serão realizados pela equipe de suporte de TI contratada, e buscará cobrir os seguintes pontos:

-
- i. Identificação e avaliação de potenciais riscos cibernéticos, envolvendo ativos de hardware e software, além de processos que necessitem de proteção. Importante estimar impactos financeiros, operacionais e reputacionais em caso de evento;
 - ii. Estabelecimento de medidas de prevenção e mitigação de riscos identificados na atividade de identificação de riscos, de forma buscar evitar eventuais ataques cibernéticos aos dados e equipamentos da empresa;
 - iii. Detecção de possíveis anomalias e/ ou fragilidades no ambiente tecnológico, incluindo acessos não permitidos, usuários não cadastrados, e dispositivos não autorizados;
 - iv. Criação de plano de resposta e recuperação de incidentes que contenha comunicação interna e externa, se necessário. Serão realizados testes anuais para validar sua eficiência. O plano identificará papéis e responsabilidades, com previsão de acionamento de colaboradores e contatos externos;
 - v. Manter tal programa de segurança cibernética atualizado, identificando novos e potenciais riscos, ativos e processos.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes, deverão ser mantidas na **COOPERPAK** como evidência em eventuais questionamentos internos ou de órgãos reguladores.

15. Continuidade dos Negócios

O processo de gestão de continuidade de negócios relativo à segurança da informação, é implementado para minimizar os impactos, e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, através de: combinação de requisitos como operações, funcionários 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.



16. Considerações Finais

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

Monte Mor, 26 de maio de 2025.

Helton Cesar Bertini
Diretor Presidente

Carlos Augusto Brischi Cavallaro
Diretor Administrativo

Walter Augusto Gabaldo
Diretor Operacional

Ana Paula de Siqueira Melo
Diretora

17. ANEXO I - Relatório de Incidente de Segurança da Informação

Descrição	Identificar resumidamente sobre o incidente			
Período em que ocorreu o incidente				
Data/hora início: Data/hora fim:				
Severidade do incidente	<table><tr><td>Alta ()</td><td>Média ()</td><td>Baixa ()</td></tr></table>	Alta ()	Média ()	Baixa ()
Alta ()	Média ()	Baixa ()		
Tipo de Impacto	() Confidencialidade () Integridade () Disponibilidade			
Origem do alerta	Informar quem ou qual sistema alertou do incidente			
Comunicação do incidente	Informar a quem ou a quais setores o incidente foi informado.			
Detalhamento do Incidente	Descrição do ocorrido, o que foi impactado (ex. sistema), informações do prestador de serviço, o que foi afetado e demais informações importantes.			
Tratamento do Incidente	Descrever ações executadas para contenção e/ou contorno do problema/incidente, equipes/pessoas envolvidas, sistemas/ferramentas utilizadas para controle do incidente.			
Análise e Encerramento do Incidente	Descrever se necessárias outras ações e recursos necessários para finalizar o tratamento do incidente e/ou para evitar que o incidente volte a ocorrer.			