coopreckitt

POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. Introdução

A Política de Segurança Cibernética tem como objetivo atender a Resolução CMN nº 4.893/2021 e estabelecer os princípios, conceitos, valores e práticas sobre os requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, que devem ser adotados pelos administradores e colaboradores da **Cooperativa de Economia e Crédito Mútuo dos Empregados da Reckitt Benckiser – Coopreckitt.**

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 **Coopreckitt**.

2. Objetivo

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

a) Proteger o valor e a reputação da empresa;
b) Garantir a confidencialidade, integridade e disponibilidade das informações da **Coopreckitt** contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;
c) 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;
d) Garantir a continuidade de seus negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;
e) Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes a atividade da empresa;
f) Conscientizar, educar e treinar os colaboradores por meio de política de Risco Cibernético, normas e procedimentos internos aplicáveis as suas atividades diárias;
g) Estabelecer e melhorar continuamente o processo de gestão de riscos de segurança cibernética.

RS
RS

EF

3. Princípios

Os princípios básicos da segurança da informação são confidencialidade, integridade
e disponibilidade das informações.

NB
NB

A política descreve fatores de reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

4. Abrangência

A Política de Segurança Cibernética tem abrangência corporativa nas dependências da **Coopreckitt**, ou seja, afeta todas as suas áreas de negócio, atendimento, administração e demais operações no que se refere a ocorrência de incidentes relativos ao risco cibernético de segurança da informação.

5. Representatividade

5.1 Diretoria

a) Definir diretrizes para implementação e aprovar a Política de Segurança Cibernética;
b) Acompanhar se as diretrizes definidas na Política estão sendo cumpridas;
c) Acompanhar as alterações na legislação de forma a manter a Política sempre em conformidade com os normativos;
d) Garantir os recursos, inclusive tecnológicos, necessários para o desempenho das atividades da Instituição;
e) Desenvolver a Política de Segurança Cibernética que atenda ao porte e complexidade da **Coopreckitt**;
f) 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;
g) Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação;
h) Prover comprometimento e apoio à aderência a política de segurança cibernética e da informação de acordo com os objetivos e estratégias de negócios estabelecidas para a organização;
i) Prover e garantir a divulgação dessa política aos funcionários da **COOPRECKITT** e às empresas prestadoras de serviços terceirizados, mediante linguagem clara, acessível, inclusive fornecendo treinamentos em nível de detalhamento compatível com as funções desempenhadas e sensibilidade das informações;
j) Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da **Coopreckitt**;
k) Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso da **Coopreckitt**, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
l) Analisar os riscos relacionados à segurança da informação da **Coopreckitt** e propor a alçadas competentes, o aperfeiçoamento do ambiente de controle;
m) Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

RS
RS

EF
EF

NB
NB

n) Conduzir a definição de controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de segurança da informação;
o) Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;
p) Autorizar acesso de seus colaboradores e terceiros apenas quando forem realmente necessários;
q) Garantir a adoção de cláusulas pertinentes à segurança das informações nos contratos estabelecidos com a **Coopreckitt**.

5.2 Colaboradores e Prestadores de Serviços

a) Tomar conhecimento e seguir ao conteúdo desta Política e se comprometer a cumprir com o **Termo de Compromisso da Segurança da Informação** para uso da rede e de ativos da informação;
b) Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI e assegurar que os recursos tecnológicos à sua disposição, sejam utilizados apenas para as finalidades aprovadas pela **Coopreckitt**;
c) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela **Coopreckitt**;
d) Garantir que as informações e dados de propriedade da **Coopreckitt** não sejam disponibilizados a terceiros e nem discutidos em ambientes públicos;
e) Comunicar imediatamente a Diretoria qualquer fato ou ameaça à segurança dos recursos, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, intercepção de mensagens eletrônicas, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet entre outros;
f) Ter atenção quando do manuseio de informações confidenciais, a fim de evitar modificação, perdas ou divulgação não autorizada;
g) Utilizar somente os recursos tecnológicos disponibilizados e permitidos pela Cooperativa.

5.3 Conselho Fiscal

Acompanhar o plano de ação e de resposta a incidentes e verificar se o documento se encontra aprovado e se existem situações identificadas.

5.3 Associados

RS

a) Manter seus dados cadastrais junto a **Coopreckitt** atualizados;
b) Atualizar senha de acesso, quando necessário.

EF

6. Privacidade dos Dados

NB

Os funcionários de empresas empregadoras também adotam Políticas de Segurança rígidas como forma de garantir a proteção e privacidade dos seus dados.

Na Cooperativa é seguida a mesma diretriz, tratando as Informações e os dados relacionados aos assoados com sigilo.

A administração da **Coopreckitt** precisa apenas de estrutura de internet para acessar as
informações em nuvem, o plano de contingência da instituição neste aspecto consiste em utilizar, na falta de acesso à rede fornecida pela **Coopreckitt**, a rede de internet do próprio colaborador em sua residência.

Os associados poderão entrar em contato com a **Coopreckitt** por diversos canais de comunicações, tais como: e-mail, telefone, site, fale conosco, WhatsApp e Teams, de forma que o atendimento aos associados será sempre garantido, estando além do atendimento físico.

7. Controle da Segurança da Informação

A **Coopreckitt** estabeleceu plano de ação e de resposta a incidentes visando implantação da Política de Segurança Cibernética

O Plano de ação é exigido alguns controles básicos de segurança da informação:

a) Política de Segurança Cibernética e respectivo plano de ação que precisam ser aprovados pela Diretoria;
b) Confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados;
c) Controles que considerem o porte da instituição, seu perfil de risco, seu modelo de negócio, seus produtos e a sensibilidade dos dados;
d) Controles e procedimentos com rastreabilidade para a garantia da proteção de informações sensíveis e classificação de dados ou de informações;
e) Diretor responsável pela política de segurança cibernética, pela execução do plano de ação e pela gestão de incidentes;
f) Implementação de programas de capacitação em segurança;
g) Comunicação para clientes e usuários;
h) Comprometimento da alta administração.

Em 14 de novembro de 2022 a Federação Nacional das Cooperativa de Crédito – FNCC emitiu o comunicado nº 014/2022 em atendimento ao inciso VII, art. 3º da Resolução CMNº nº 4.893/2021, em que a **Cooprekitt** poderá compartilhar as informações referentes as ocorrências de incidentes cibernéticos relevantes com as demais cooperativas por meio da FNCC, conforme instruções apresentadas naquele comunicado.

RS
RS

EF

Cabe ressaltar que a comunicação de incidentes também deve ser apresentada ao Banco Central do Brasil, conforme item 2.8.17. - Comunicações ao Banco Central do Brasil.

NB
NB

8. Formas de incidências

São considerados como incidentes cibernéticos relevantes, de acordo com o comunicado, as interrupções de sistema não planejadas que podem ocorrer por ações diversas, que causam danos e afetem os negócios da cooperativa, como por exemplo:

a) queda de energia elétrica de grande escala de tempo;
b) falha de um elemento de conexão;
c) servidor fora do ar, ausência de conexão com internet;
d) sabotagem
e) terrorismo;
f) indisponibilidade de acesso a Cooperativa;
g) ataques DDOS, entre outros.

Atentar para que sejam seguidas as instruções e demais procedimentos contidos no Comunicado 041/2022 – FNCC.

9. Plano de Ação e de Resposta a Incidentes

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

a) as ações a serem desenvolvidas pela **Coopreckitt** para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;
b) as rotinas, os procedimentos, os controles e as tecnologias a serem utilizadas na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e
c) 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:

RS
RS

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;

EF
EF

b) 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;
c) os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período; e

NB
NB

d) os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionadas por incidentes.

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

A **Cooprekitt**, tendo em vista o seu porte, o perfil de risco que se encontra exposta, bem como o modelo de negócio adotado e previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, adotará os seguintes procedimentos:

a) Verificará se a empresa contratada adota práticas de governança corporativa e de gestão, proporcionais à relevância do serviço contratado e aos riscos a que estejam expostas; e
b) Verificação da capacidade do potencial prestador de serviço de assegurar o cumprimento da legislação e da regulamentação em vigor, o acesso da instituição aos dados e às informações a serem processados e armazenados pelo prestador de serviço, a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço e a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado.

11. Contrato de Serviços Relevantes

A **Coopreckitt** deve proceder a uma avaliação criteriosa quanto à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, considerando:

a) 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;
b) 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;
c) A Cooperativa deve possuir recursos e competências necessários para a adequada gestão dos serviços a serem contratados;
d) A Cooperativa 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.

RS
RS

12. Serviços em Nuvem

EF

A **Coopreckitt**, tendo em vista a necessidade de otimizar o atendimento de seus cooperados e visando maior segurança e celeridade, e baseado nas premissas citadas anteriormente, fez a contratação do Serviço de Computação em Nuvem.

NB
NB

O contrato foi firmado com a empresa PRODAF INFORMÁTICA que, é a responsável pelos serviços de processamento e armazenamento de dados conforme disposto na Resolução CMN nº 4.893/2021. Esta, por sua vez, possui

contrato regular de Serviços junto a DEDALUS que, é detentora do espaço utilizado pela **Coopreckitt** para armazenar seus dados.

Por sua vez, o espaço objeto do contrato entre a DEDALUS x PRODAF INFORMÁTICA pertence à AMAZON WEB SERVICES, conforme Termo de Adesão de Proposta Comercial 2850A.14, datado de 15/08/2014, onde foram escolhidas as seguintes opções de serviços: Serviços de Hospedagem AWS – Franquia Mensal e Serviço de Suporte DEDALUS – Nível de Serviços Enterprise.

O backup das máquinas da **Coopreckitt** está em nuvem através da Microsoft - OneDrive, de forma que, permite o acesso às informações de qualquer lugar do mundo que contemple acesso à internet. As informações estão protegidas em nuvem e, trimestralmente é realizado um backup local por segurança adicional, através de HD externo.

13. Responsabilidade da Cooperativa com a Empresa Empregadora

A **Coopreckitt** poderá obter dados cadastrais de seus associados, em algumas situações específicas, tal como via importação cadastral (realizada mensalmente através do sistema nuvem Prodaf Informática e das empresas conveniadas) possibilitando atualização de dados cadastrais dos associados. Os dados fornecidos pelos associados e/ou empresas conveniadas serão mantidos em absoluto sigilo e, por esta razão, a **Coopreckitt** assegura que eles não serão, sob nenhuma hipótese, vendidos, alugados, cedidos, nem de outra forma repassados a terceiros.

14. Relatório de Testes

Sempre que solicitado pela **Coopreckitt**, o departamento de TI da Prodaf, 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. Todas as informações são prestadas pela empresa em relatório anual.

15. Comunicações ao Banco Central do Brasil

A **Coopreckitt** informará previamente ao 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 dez dias antes da contratação dos serviços.

RS
RS

EF

16. Considerações Finais

NB
NB

A Política de Segurança Cibernética será aprovada e revisada a cada 2 (dois) anos pela Diretoria, ou quando houver exigências e alterações dos órgãos normativos.

A divulgação da política deverá ser no site da Cooperativa.

São Paulo – SP, 30 de abril de 2025.

Electronically signed by: Rosa Herminia Storoli
Reason: I approve this document.
Date: May 19, 2025 15:21 ADT

Rosa Hermínia Storoli dos Santos
Diretora Presidente

Electronically signed by: Eliana Fazzio
Reason: I approve this document.
Date: May 21, 2025 16:20 ADT

Eliana Aparecida Fazzio
Diretora Administrativa

Electronically signed by: Nivia Belopede
Reason: I approve this document.
Date: May 23, 2025 08:50 ADT

Nivia Salmazo Belopede Massonetto
Diretora Operacional

CI -Política de Segurança Cibernética 2025

Final Audit Report 2025-05-23

Created:	2025-05-15
By:	Maria de Lourdes Jorge (Mariadelourdes.Jorge@reckitt.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAJcWeC6ACzGN6dNnHiqtnkc04OwHfjrnh

"CI -Política de Segurança Cibernética 2025" History

Document created by Maria de Lourdes Jorge (Mariadelourdes.Jorge@reckitt.com)
2025-05-15 - 17:30:57 GMT- IP address: 165.225.9.76

Document emailed to Rosa Herminia Storoli (Rosa.Storoli@reckitt.com) for signature
2025-05-15 - 17:33:27 GMT

Email viewed by Rosa Herminia Storoli (Rosa.Storoli@reckitt.com)
2025-05-15 - 21:01:27 GMT- IP address: 165.225.214.133

Rosa Herminia Storoli (Rosa.Storoli@reckitt.com) authenticated with Adobe Acrobat Sign.
2025-05-19 - 18:21:26 GMT

Document e-signed by Rosa Herminia Storoli (Rosa.Storoli@reckitt.com)
Signing reason: I approve this document.
Signature Date: 2025-05-19 - 18:21:28 GMT - Time Source: server- IP address: 165.225.214.133

Document emailed to Eliana Fazzio (Eliana.Fazzio@reckitt.com) for signature
2025-05-19 - 18:21:29 GMT

Eliana Fazzio (Eliana.Fazzio@reckitt.com) authenticated with Adobe Acrobat Sign.
2025-05-21 - 19:20:18 GMT

Document e-signed by Eliana Fazzio (Eliana.Fazzio@reckitt.com)
Signing reason: I approve this document.
Signature Date: 2025-05-21 - 19:20:19 GMT - Time Source: server- IP address: 165.225.214.160

Document emailed to Nivia Belopede (Nivia.Belopede@reckitt.com) for signature
2025-05-21 - 19:20:20 GMT

Email viewed by Nivia Belopede (Nivia.Belopede@reckitt.com)
2025-05-21 - 20:22:28 GMT- IP address: 136.226.63.20

Nivia Belopede (Nivia.Belopede@reckitt.com) authenticated with Adobe Acrobat Sign.

2025-05-23 - 11:50:35 GMT

Document e-signed by Nivia Belopede (Nivia.Belopede@reckitt.com)

Signing reason: I approve this document.

Signature Date: 2025-05-23 - 11:50:36 GMT - Time Source: server- IP address: 165.225.214.126

Agreement completed.

2025-05-23 - 11:50:36 GMT