

Área temática: **Finanças**

**RISCOS CIBERNÉTICOS NAS COOPERATIVAS DE CRÉDITO: ANÁLISE
BASEADA NA RESOLUÇÃO nº4.893 DO BACEN**

RESUMO: O trabalho aborda a criação das cooperativas com ênfase na ação mútua e investimento compartilhado, mas destaca que elas não estão imunes aos riscos cibernéticos. Com o avanço tecnológico, as operações via Internet Banking e aplicativos de smartphones se tornam vulneráveis a ataques cibernéticos. As cooperativas, reguladas pelo BACEN, são fiscalizadas para garantir consistência. O objetivo do estudo é analisar a segurança cibernética dos principais sistemas de cooperativismo de crédito no Brasil, baseando-se na resolução nº 4.893 do Banco Central. A avaliação revelou que duas das cinco instituições estão em conformidade, divulgando suas políticas em ambientes externos, enquanto as outras três têm aderência parcial.

Palavras-chave: Cooperativas de crédito, Riscos Cibernéticos, Banco Central do Brasil, Política de Segurança da informação.

ABSTRACT: The work addresses the creation of cooperatives with an emphasis on mutual action and shared investment but highlights that they are not immune to cyber risks. With technological advances, operations via Internet Banking and smartphone applications become vulnerable to cyber-attacks. Cooperatives, regulated by BACEN, are inspected to ensure consistency. The objective of the study is to analyze the cybersecurity of the main credit union systems in Brazil, based on Resolution No. 4,893 of the Central Bank. The assessment revealed that two of the five institutions are in compliance, disclosing their policies in external environments, while the other three have partial adherence.

Keywords: Credit unions, Cyber Risks, Central Bank of Brazil, Information Security Policy.

1. INTRODUÇÃO

Ao longo dos anos, as mudanças no acesso à internet têm influenciado a forma como os humanos se comunicam e interagem com ela. O que costumava ser seguro no passado agora requer medidas de proteção para salvaguardar informações e dados pessoais. A presença de riscos é inerente a todas as atividades, inclusive no contexto das instituições financeiras. Conforme essas organizações evoluem para abranger diversos serviços, a gestão de riscos torna-se vital para a identificação, minimização e administração eficaz dessas potenciais ameaças.

O cooperativismo cresce à medida que as pessoas reconhecem a necessidade de unir esforços para alcançar objetivos comuns, em contraposição às ações individuais. Este modelo surgiu quando indivíduos perceberam que a colaboração poderia levar a resultados mais satisfatórios do que ações isoladas. (SOARES; SOBRINHO, 2008).

Cooperativas de crédito estão crescendo e se tornando competitivas ao oferecerem taxas de juros mais baixas em empréstimos comparadas aos bancos. Além disso, proporcionam taxas de juros mais atrativas em depósitos aplicados nas cooperativas (BRESSAN, V. G. F., BRAGA, M. J., BRESSAN, A. A., E DE ANDRADE RESENDE FILHO, M. 2010). Com a ampliação de novas agências de cooperativas de crédito, houve o fortalecimento de pequenas empresas, geração de empregos, mobilidade social e conseqüentemente competitividade e eficiência econômica.

Segundo Barbosa, Silva, Oliveira, Jesus e Miranda (2021) registro da Polícia Civil do Distrito Federal, identificou um crescimento na tentativa de várias modalidades de fraudes financeiras contra os brasileiros durante a crise da Covid-19. Além disso, no período de quarentena, as instituições registraram um aumento de 80% nas tentativas de ataques de *phishing* que iniciam por meios de recebimentos de e-mails que carregam vírus ou *links* e direcionam o usuário a sites falsos, que, normalmente, possuem remetentes desconhecidos ou falsos. (FEBRABAN, 2020)

CAIADO; CAIADO, (2008, p.32) concluem que:

... as instituições financeiras e, em particular, os bancos, têm de enfrentar novos desafios, mercê do aparecimento de vários fenômenos que há pouco mais de meio século eram praticamente inexistentes, como a internacionalização financeira, a globalização de mercados, a proliferação de novos concorrentes e dos respetivos produtos e serviços e o surto galopante de novas tecnologias.

O presente estudo tem como objetivo buscar a resposta para a seguinte questão: as políticas de segurança cibernética das cooperativas de crédito estão de acordo com o que está previsto na resolução nº 4.893 do BACEN? Para responder a essa pergunta foi feita uma pesquisa exploratória, com abordagem qualitativa, onde pretendeu-se analisar os sistemas de 5 cooperativas de crédito brasileiras.

2. REFERENCIAL TEÓRICO

2.1 GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

Segurança cibernética ou *cybersecurity* é a prática de defender computadores, servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques de procedências duvidosas (KASPERSKY, 2016). A Segurança da informação também

pode ser definida como “uma área do conhecimento dedicada à proteção de ativos da informação contra acesso não autorizado, alterações indevidas ou sua indisponibilidade.” (SÊMOLA, 2014, p. 41).

Diante disso a segurança da informação tem três principais conceitos, segundo Sêmola, (2014. p. 43) são eles:

- Confidencialidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso às pessoas a quem é destinada.
- Integridade – Toda informação deve ser mantida na mesma condição em que foi disponibilizada por seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
- Disponibilidade – Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível para seus usuários, no momento em que eles necessitam delas para qualquer finalidade.

Organizações têm a responsabilidade de gerenciar riscos através de planejamento e organização, visando reduzir perdas e vazamentos de dados. A norma ISO 27005 se destaca como um guia para construir metodologias que ajudam a mitigar riscos contínuos.(KONZEN, 2013).

Segundo Assaf Neto (2018), é importante que a instituição financeira planeje uma boa administração de seus riscos desde que não seja possível ou, muitas vezes, desejável eliminar totalmente o risco. Para Oliveira e Pinheiro (2018), diversos tipos de risco estão envolvidos na atividade econômica, que começam antes das operações serem fechadas e continuam após seu fechamento.

Sendo uma disciplina associada a gestão de risco, a segurança da informação é um conjunto de controles que inclui políticas, procedimentos, controles que precisam ser estabelecidos, monitorados e melhorados continuamente para garantir o atendimento aos objetivos das organizações.

Segundo Caiçara Júnior (2012), ao longo dos anos a informação tornou-se cada vez mais um dos principais ativos empresariais, principalmente a nível estratégico, e isso, fez as empresas preocuparem-se ainda mais com a proteção das informações.

2.2 RISCOS CIBERNÉTICOS

Riscos cibernéticos envolvem tentativas criminosas de prejudicar, roubar ou destruir dados, servidores e sites. Isso resulta em perdas financeiras, operacionais ou danos à reputação, originados de falhas nos sistemas digitais, processos de apoio ou uso indevido das informações. Para Doneda (2006), os dados devem ser protegidos contra o extravio, destruição, modificação, transmissão ou acesso de pessoas não autorizadas.

§ 3º As instituições que não constituírem política de segurança cibernética própria em decorrência do disposto no § 2º devem formalizar a opção por essa faculdade em reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição. (Bacen, 2021. p. 1)

2.2.1 Ataques Cibernéticos

Ataques cibernéticos são ações de agentes maliciosos que utilizam vírus para destruir, espionar, interceptar dados e roubar informações de dispositivos ou redes.

Segundo BAPTISTA; DIAN (2021, P.51) afirma,

De modo geral, estes ataques cibernéticos são uma tentativa de invadir sistemas e computadores para adquirir, roubar, criptografar ou bloquear o acesso de usuários às informações. Estes ataques cibernéticos podem ser realizados de maneiras diferentes e cada uma dessas maneiras tem suas peculiaridades e formas de ação para atingir o seu objetivo, passando a serem classificados de acordo com o modo como agem e estando entre os principais os *exploits* e os malwares.

2.3 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Campos (2007) afirma que as políticas de segurança da informação são o conjunto de políticas emitidas para garantir que todos os usuários de tecnologia da informação conheçam as regras e diretrizes relacionadas à segurança das informações armazenadas em qualquer ponto da rede ou dentro dos limites das organizações.

Em geral os requisitos para uma política são definidos por um *framework*. Os padrões (*frameworks*) podem ser usados para avaliar o estado de um programa de segurança, construir um programa de segurança abrangente, medir a segurança do programa e simplificar a comunicação entre a equipe de segurança e os líderes de negócios (SAXENA e GAYATHRI, 2021). Ainda segundo Rashi e Gayathri (2021), a ISO 27.001, o PCI e o CIS encontram-se entre os *frameworks* que são usados pelos especialistas do setor nos dias de hoje.

A ISO 27001 é uma norma para o Sistema de Gestão da Segurança da Informação (SGSI), de referência internacional, que no Brasil é representada pela ABNT (Associação Brasileira de Normas Técnicas), que tem como objetivo assegurar a adequação contínua, suficiência, efetividade da direção de gestão e suporte à segurança da informação de acordo com os requisitos comerciais, legais, estatutários, regulatórios e contratuais.

O PCI DSS (Payment Card Industry Data Security Standard) é um conjunto de normas de segurança criado por empresas de cartões de crédito, para proteger informações de pagamentos. Ele exige medidas como criptografia de dados, controle de acesso e monitoramento constante para evitar fraudes e garantir a segurança de dados de cartões de pagamento.

Outro padrão internacional conhecido é o CIS – Os "CIS Controls" (Controles do Center for Internet Security) são um conjunto de 20 diretrizes de segurança cibernética desenvolvidas pelo Center for Internet Security. Esses controles são projetados para ajudar organizações a proteger seus sistemas e dados contra ameaças cibernéticas.

As políticas de segurança da informação são parte do escopo de gerenciamento de riscos de segurança cibernética para tomada de decisão organizacional (SULISTYOWATI, HANDAYANI e SURYANTO, 2020). Conforme a ISO 27.002, uma política de segurança da informação deve: (1) preservar confidencialidade, integridade e disponibilidade de dados e ativos de infraestrutura; (2) gerenciar riscos de exposição ou comprometimento; (3) manter ambiente de TI seguro e estável; (4) identificar e reagir a eventos de uso inadequado ou divulgação não autorizada; (5) monitorar sistemas em busca de anomalias indicativas de comprometimento; e (6) promover conscientização sobre segurança da informação.

2.4 RESOLUÇÃO 4.893/2021 BACEN

A Resolução nº 4.658/2018, criada em 26 de abril de 2018, estabelece a política de segurança cibernética para instituições comerciais e financeiras autorizadas pelo Banco Central do Brasil. A resolução foi editada em 26 de fevereiro de 2021 e entrou em vigor em 01 de julho de 2021. Ela define requisitos para a contratação de serviços de processamento, armazenamento de dados e computação em nuvem, permitindo o acesso a arquivos digitais remotamente de qualquer dispositivo em qualquer lugar do mundo. (BRASIL, 2021).

A Resolução 4.893/2021 promove a governança cibernética, protegendo dados e privacidade. Requer a prevenção, detecção e redução de incidentes cibernéticos, com relatórios ao Banco Central sobre serviços de processamento, armazenamento de dados e computação em nuvem, incluindo detalhes da empresa e localização dos dados no exterior.

A Resolução nº 4.893/2021 do BACEN tem como definição:

Art. 1º Esta Resolução dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. (BACEN, 2021 p. 1)

Os itens extraídos da resolução 4.893/2021 tem as seguintes diretrizes a serem seguidas pelas instituições financeiras:

1) Conscientização em segurança: Planejar melhorias para capacitar os colaboradores usando diversos meios de divulgação de informações. 2) Gestão de ativos: Identificar e listar os ativos da organização, garantindo manutenção conforme necessidade. 3) Gestão de Conformidade: Implementar padrões de melhoria contínua, enviando informações ao Bacen e arquivando registros por 5 anos. 4) Gestão de continuidade de negócio: Definir política de continuidade, estabelecer métricas e garantir execução correta dos procedimentos. 5) Gestão de controles criptográficos: Avaliar recursos criptografados para aderência às normas da resolução. 6) Gestão de desenvolvimento seguro: Garantir testes sem dados reais, estabelecer acesso restrito e metodologia segura. 7) Gestão de identidades e acessos: Estabelecer políticas, métricas e proteção de senhas para manter a confiabilidade. 8) Gestão de incidentes: Definir política de resposta a incidentes, mapear riscos e comunicar o Bacen prontamente. 9) Gestão de riscos: Identificar, mapear e mitigar riscos internos e externos para proteger ativos. 10) Gestão de terceiros: Verificar conformidade de terceiros com exigências do Bacen antes de contratar os seus serviços, incluindo autoridades de países envolvidos. 11) Gestão de vulnerabilidades: Analisar, avaliar e corrigir vulnerabilidades, incluindo testes e monitoramento. 12) Governança de segurança da informação: Classificar informações, promover conscientização e estabelecer normas. 13) Segurança de redes: Segmentar redes, realizar testes de invasão, usar detectores de malware e centralizar logs para rastreamento e monitoramento.

Estes itens apresentam uma coerência com os *frameworks* de segurança da informação já discutidos conforme pode ser visto no Quadro 1.

Quadro 1- Análise da Resolução BACEN 4.893/2021. vs frameworks de gestão de segurança da informação

Resolução BACEN 4.893/2021	ISO 27.002	CIS	PCI - DSS
Conscientização em Segurança	X	X	X
Gestão de Ativos	X	X	*
Gestão de Conformidade	X		
Gestão de Continuidade de Negócio	X	X	X
Gestão de Controles Criptográficos	X	X	X
Gestão de Desenvolvimento Seguro	X	X	X
Gestão de Identidades e Acessos	X	X	X
Gestão de Incidentes de Segurança da Informação	X	X	X
Gestão de Riscos	X		*
Gestão de Terceiros	X	X	X
Gestão de Vulnerabilidades	X	X	X
Governança de Segurança da Informação	X		
Segurança de Redes	X	X	X

Fonte: Elaborado pelo autor (2023)

Nota: * corresponde ao assunto ser tratado no framework, mas não de forma específica.

2.5 COOPERATIVAS

No norte da Inglaterra, por volta de meados de 1844, operários que sofriam exploração em seus empregos criaram cooperativas como resposta às más condições de trabalho (SINGER, 2002). Com a industrialização e a substituição gradual da mão de obra artesanal por máquinas, a escassez de empregos resultou em condições precárias para a população, com muitos enfrentando a falta de moradia e alimentos. Diante dessa situação, figuras como Robert Owen e William King lideraram o movimento cooperativista, fundamentado nos princípios de cooperação e igualdade, eliminando a distinção entre patrões e empregados, com os próprios membros da cooperativa atuando como proprietários (OCB/ES, 2018).

A definição de cooperativa segundo Réus *et al* (2016, p. 5, *apud* VEIGA E FONSECA, 2002, p.39)

“Cooperativa é uma associação voluntária de no mínimo 20 pessoas, sem fins lucrativos porém com fins econômicos que exercem uma mesma atividade para realizar objetivos comuns que para tanto contribuem equitativamente para a formação do capital necessário por meio da aquisição de quota-partes e aceitam assumir de forma igualitária os riscos e benefícios do empreendimento. É regida pelo princípio democrático de cada pessoa um voto. Os excedentes ou sobras são distribuídas na proporção do trabalho de cada cooperado”.

Segundo Silva (2018) o cooperativismo culminou em um sistema reconhecido por seus benefícios para a sociedade que tem como propósito propagar a sua cultura.

“Sob o prisma social, a OCB (2017) estima que, atualmente, o movimento cooperativo agrega cerca de 25,4% do total de brasileiros, o que representa mais de 52 milhões de pessoas atingidas por este modelo próprio de negócio que, pela sua origem e natureza, se revela um poderoso instrumento de desenvolvimento e inclusão social, já que promove uma economia baseada

em valores estruturais como os da solidariedade, da democracia e da autoajuda. (SOUZA, 2019. p.2)”

O Cooperativismo tem como base 7 princípios que são interpretados pela 7 cores do arco-íris, que direcionam as cooperativas a praticarem os seus valores.

Para Réus et al. (2016, p. 5) são eles:

1º – Princípio da adesão voluntária e livre: Aberta a todas as pessoas, sem discriminações de sexo, sociais, raciais, políticas e religiosas.

2º-Princípio do controle democrático pelos membros: Os membros são responsáveis por controlar, participar e formular políticas; tomar decisões, definir metas e eleger (cada membro tem direito a um voto) nas assembleias seus dirigentes (VEIGA; FONSECA, 2002).

3º – Princípio da participação econômica dos membros: Os associados contribuem equitativamente e ajudam a controlar democraticamente o capital da cooperativa. As sobras poderão ser divididas para cada membro ou ainda utilizadas para ajudar no desenvolvimento da cooperativa, por exemplo, ou sustentar outras atividades aprovadas pelos sócios (FARIA, 2009).

4º – Princípio da autonomia e independência: Esse princípio tem como base assegurar a autonomia da cooperativa, sendo elas controladas por seus membros. Ainda que mantenha relações com outras organizações assim como com o governo ou se obterem capital de fontes externas, devem garantir o controle democrático pelos seus associados (FARIA, 2009).

5º – Princípio da educação, formação e informação: É dever da cooperativa a promoção da educação e formação de seus membros, dirigentes eleitos e administradores para que estes contribuam para o desenvolvimento da cooperativa. Fica definido que cada cooperativa deve aplicar no mínimo 5% das sobras do exercício financeiro em educação, assistência técnica e social dos associados e seus familiares (VEIGA; FONSECA, 2002).

6º – Princípio da cooperação entre cooperativas: As cooperativas devem trabalhar pelos seus cooperados, assim como trabalhar em conjunto com outras cooperativas no âmbito local, regional, nacional e internacional (OCB, c2008).

7º – Princípio da preocupação com a comunidade: as cooperativas trabalham para o desenvolvimento sustentável e bem-estar da sua localidade por meio de políticas aprovadas pelos membros (OCB, c2008).

2.5.1 Cooperativas de Crédito

A primeira cooperativa de crédito no Brasil foi fundada em 1902 na cidade de Nova Petrópolis no estado do Rio Grande do Sul sob a liderança do Padre Jesuíta Theodor Amstad, que criou a Cooperativa de Crédito da América Latina, a SICREDI Pioneira RS, atualmente umas das maiores do país e na época conhecida como “Caixa Econômica e Empréstimos Amstad”.

De acordo com a Lei nº 5.764/1971, cooperativas de crédito são formadas por pessoas que contribuem com bens ou serviços para uma atividade econômica de benefício comum, sem fins lucrativos. Com relevância socioeconômica, essas cooperativas reinvestem ativos para financiar seus cooperados, apoiando as comunidades locais. Isso contrasta com os bancos, onde os clientes não participam dos lucros e têm um papel distinto das cooperativas. (ARRUDA, CANASSA, MACIEL, e COSTA, (2020).

Como instrumentos de desenvolvimento local, as cooperativas asseguram a reciclagem dos recursos nas próprias comunidades. Ou seja, o resultado monetário do que se gera é reinvestido ali mesmo, produzindo novas riquezas. Além disso, as entidades têm plena autonomia para ajustar a sua política creditícia e de gestão da poupança à realidade do lugar. Essa liberdade permite acompanhar adequadamente o ciclo econômico de cada região e respeitar as suas aptidões e potencialidades socioeconômico-culturais, com geração e incremento de renda, estimulando, ainda, a fixação dos jovens nas próprias comunidades (MEINEN, PORT, 2012. P.55).

Segundo a Lei 5.764, de 1971, art. 5º, parágrafo único. É vedado às cooperativas o uso da expressão “Banco”, sendo assim não se deve empregar a palavra banco quando referir-se as cooperativas de crédito.

3. PROCEDIMENTOS METODOLÓGICOS

Para Gewandsznajder (1989, p. 3) “o que melhor caracteriza o conhecimento científico não é o que ele estuda, mas como estuda. [...] Assim, não é o objeto de estudo que importa, mas a forma, o método pelo qual estudamos este objeto”.

Esta pesquisa avalia as políticas de segurança cibernética de cooperativas brasileiras (Sicoob, Sicredi, Ailos, Cresol e Unicred) à luz da Resolução nº 4.893 do Banco Central. Utilizando dados secundários dos sites das cooperativas, a abordagem qualitativa e exploratória visa identificar a conformidade com as diretrizes de segurança cibernética. Para Oliveira (2008), a metodologia trata-se de estudo e pesquisas que utilizam técnicas, métodos e discursos, formam um conjunto de operações sistematizadas e racionalmente encadeadas.

Este estudo analisou as políticas de segurança cibernética acessíveis publicamente por meio de sites externos. Utilizando diretrizes alinhadas com a Resolução nº 4.893/2021 do Banco Central, o pesquisador identificou e comparou essas diretrizes nas políticas de segurança cibernética de instituições financeiras específicas.

Foram utilizados três níveis de classificação (1-Localizado, 2-Parcialmente, 3-Não localizado) para avaliar as informações nas políticas de segurança cibernética. O nível 1 indicava conformidade com a resolução, o nível 2 refletia entendimento do conceito mesmo sem clareza na resolução, e o nível 3 indicava ausência e não atendimento ao conceito da resolução.

3.1 AMOSTRAGEM DAS COOPERATIVAS

3.1.1. Seleção das cooperativas

A pesquisa escolheu cooperativas de crédito devido ao seu modelo de negócio em ascensão. As cinco maiores cooperativas financeiras de Santa Catarina foram selecionadas para análise.

3.1.2 Cooperativas

Fundado em 1997 em Brasília, o Sicoob é o maior sistema de cooperativas de crédito do Brasil, com 5,9 milhões de cooperados e presença em todos os estados e no Distrito Federal. Possui 366 cooperativas singulares, 16 centrais e o Centro

Cooperativo Sicoob. Com 3.789 pontos de atendimento em 1.934 cidades, é a segunda instituição com mais agências no Brasil.

A Cooperativa Sicredi, criada em 1902 em Nova Petrópolis, RS, é a primeira cooperativa de crédito da América Latina. Hoje chamada Sicredi Pioneira, tem mais de 6 milhões de associados, 2,4 mil agências e 100 cooperativas.

A Unicred, fundada em 1989 em Casca/RS, foi a primeira cooperativa de profissionais da saúde. Com 35 cooperativas, cerca de 253 mil cooperados e unidades em 10 estados, incluindo 4 centrais e uma Confederação Nacional, opera em São Paulo, Porto Alegre e Florianópolis.

A Ailos, estabelecida em 2002, surgiu de uma história que começou em 1951 com a CrediHering. Hoje, com a Central Ailos e 13 cooperativas, forma o Ailos Sistema de Cooperativas, resultado de uma evolução ao longo de 70 anos.

Por fim, a Cresol, criada em 1995 em Dois Vizinhos, Paraná, por agricultores em busca de inclusão financeira, possui mais de 787 mil famílias cooperadas e 712 agências em 18 estados brasileiros.

Quadro 2. Dados coletados dos Sistemas de Cooperativa de Crédito.

Cooperativa	Ano Criação	Quantidade Cooperados	Quantidade P.A(Ponto Atendimento)	Patrimônio Líquido	Ativos (em R\$ mil)	Funcionários(em Mil)	Atualização Dados
AILOS	2002	1,2 mi	267	2.728.945	14,12 bi	4846	Dezembro de 2021
CRESOL	1995	710 mil	687	2.15 bi	17.65 bi	4654	Dezembro de 2021
SICOOB	1997	5,9 mi	3.789	30.3 bi	190.4 bi	53.400	Dezembro de 2021
SICREDI	1902	5,5 mi	2.200	24,9 bi	197,6 bi	30.000	Dezembro de 2021
UNICRED	1989	253 mil	308	2.515.541	19.6 bi	2242	Dezembro de 2021

Fonte: Elaborado pelo autor (2023)

4. RESULTADOS

Os resultados a seguir resumem a análise das informações coletadas dos sites das cooperativas de crédito. É importante observar que a resolução específica que as políticas de segurança cibernética devem estar acessíveis ao público, contendo os princípios gerais da política de segurança cibernética (conforme Seção II, Art. 4º e Art. 5º). Cada item da Resolução nº 4.893 do Bacen foi analisado para verificar a conformidade com a política de segurança cibernética. Cada item valia 1 ponto, e a contagem dos pontos foi representada em um gráfico (Figura 1) para comparação visual entre as quatro cooperativas.

Nos itens conscientização em segurança, gestão de continuidade de negócios, gestão de identidade de acessos e gestão de vulnerabilidade nota-se que as instituições financeiras atenderam o item com o percentual elevado. Nos itens gestão de conformidades e segurança de redes os percentuais variam acima de 50% mostrando que as instituições estão preocupadas com os mesmos. Já no item de gestão de ativos a Cresol e Sicoob atingiram o percentual máximo enquanto Sicredi e Ailos atingiram apenas 33%.

Na Gestão de controles criptográficos e na Gestão de desenvolvimento, com exceção do Sicredi com baixo percentual abaixo de 50%, as outras instituições alcançaram altos percentuais. No que tange à Gestão de incidentes de segurança da informação e Gestão de riscos, Sicredi e Ailos ficaram abaixo de 50%, enquanto as demais obtiveram pontuação máxima. No item de Gestão de terceiros, onde é necessário definir, avaliar e notificar fornecedores de terceiros, o Sicredi não abordou

esse tema em sua política de segurança cibernética, enquanto as outras instituições tiveram percentual acima de 50%.

Na Governança de Segurança da Informação, a Cresol alcançou 100% de conformidade, enquanto Sicoob obteve 75%. Sicredi atingiu 25% e a política da Ailos não apresentou esses itens.

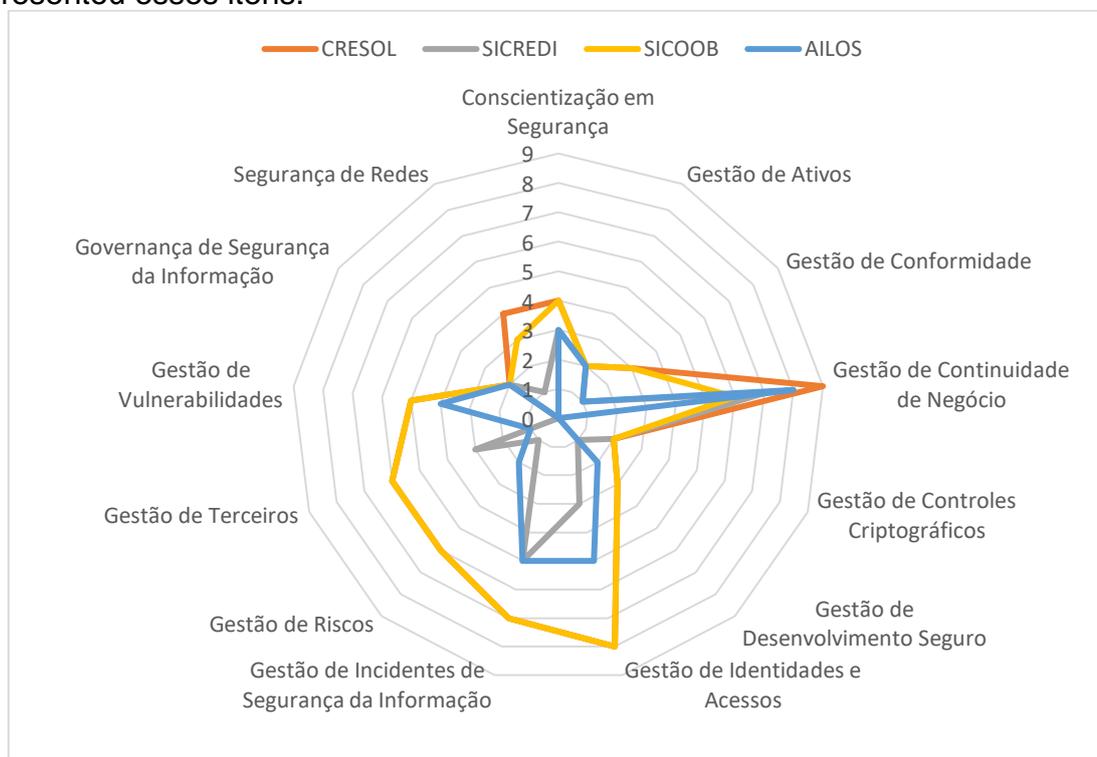


Figura 1. Análise do atendimento aos requisitos da resolução BACEN nº4.893/2021
Fonte: Elaborado pelo autor. (2023)

A Cresol atendeu integralmente os critérios da Resolução 4.893 ao disponibilizar sua política de segurança cibernética publicamente. No caso do Sicoob, sua política foi extraída da Central de Serviços Sicoob, abrangendo todas as cooperativas, mas devido a diferentes políticas em cada cooperativa, alguns itens não foram encontrados. Sicredi e Ailos forneceram políticas resumidas, conforme a recomendação do Bacen. Não foi possível analisar a política da Unicred, pois não foram encontradas versões públicas. A análise considerou arquivos encontrados, representando a perspectiva do autor e não validando nem excluindo todas as informações. Detalhes dos resultados por item estão na Tabela 1.

Quadro 3. Análise do atendimento aos requisitos da resolução. Análise da Resolução BACEN 4.893/2021

Itens da Resolução 4.893/2021	CRESOL	SICREDI	SICOOB	AILOS
Conscientização em Segurança	100%	75%	100%	75%
Gestão de Ativos	100%	33%	100%	33%
Gestão de Conformidade	100%	78%	67%	89%
Gestão de Continuidade de Negócio	100%	100%	100%	0%
Gestão de Controles Criptográficos	100%	33%	100%	67%
Gestão de Desenvolvimento Seguro	100%	38%	100%	63%
Gestão de Identidades e Acessos	100%	71%	100%	71%
Gestão de Incidentes de Segurança da Informação	100%	17%	100%	33%
Gestão de Riscos	100%	50%	100%	17%
Gestão de Terceiros	100%	0%	100%	80%
Gestão de Vulnerabilidades	100%	100%	100%	100%
Governança de Segurança da Informação	100%	25%	75%	0%
Segurança de Redes	100%	51%	93%	57%

Fonte: Elaborado pelo autor.(2023)

5. CONCLUSÃO

Este estudo avaliou se as políticas de segurança cibernética das cooperativas de crédito no Brasil atendem à Resolução nº 4.893/2021 do Banco Central. Algumas cooperativas não disponibilizaram suas políticas completas publicamente, embora seja exigido um resumo. Algumas estão parcialmente em conformidade, apenas uma está totalmente em conformidade.

Os incidentes cibernéticos que afetaram cooperativas como Sicredi, Sicoob e Unicred nos anos de 2018, 2020 e 2021 apontam para a importância de uma análise mais aprofundada das políticas de segurança cibernética. Embora esses incidentes não tenham resultado em vazamentos de dados, a natureza sensível das informações reforça a necessidade de manter rigorosos controles baseados nas políticas de segurança da informação. Isso se mostra crucial para mitigar os riscos associados às operações das cooperativas de crédito.

Para futuros estudos, recomenda-se uma análise mais detalhada das políticas internas das cooperativas para aprimorar a conformidade e eficácia das medidas de segurança cibernéticas adotadas.

6. REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBRISO/IEC27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos**. 3ª edição. ABNT, 2022

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBRISO/IEC27002 - Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação**. 3ª edição. ABNT, 2022

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBRISO/IEC27005 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. 3ª Edição. ABNT, 2019

AILOS SISTEMA DE COOPERATIVAS, c2022. Somos Ailos. **Afinal, como nasceu o nosso Sistema de Cooperativa?**. Disponível em:

<[**AILOS SISTEMA DE COOPERATIVAS, c2022. Pagina Inicial.** Disponível em: <<https://www.ailos.coop.br/sistema-ailos/sobre-o-sistema-ailos/>> . Acesso em: 09 de dez. de 2022.](https://www.ailos.coop.br/releases/como-nasceu-o-nosso-sistema#:~:text=Constitu%C3%Ado%20oficialmente%20como%20sistema%20em,Cr%C3%A9dito%20Organiza%C3%A7%C3%B5es%20Hering%20(CrediHering)>
Acesso em: 23 de jan de 2023.</p></div><div data-bbox=)

AILOS SISTEMA DE COOPERATIVAS, c2022. Resumo público política de segurança cibernética do sistema Ailos. Disponível em: <<https://www.viacredi.coop.br/wp-content/uploads/2019/07/Resumo-Publico-Politica-de-Seguranca-Cibernetica-do-Sistema-Ailos.pdf#:~:text=Pol%C3%Adtica%20de%20Seguran%C3%A7a%20Cibern%C3%A9tica%20do%20Sistema%20Ailos%20estabelece,processos%20de%20neg%C3%B3cios%20das%20Cooperativas%20do%20Sistema%20Ailos>> . Acesso em 23 de Jan. de 2023.

ARRUDA, Alessandro Gustavo Souza, CANASSA, Bruno José, MACIEL, Sirlei De Andrade e COSTA, Davi Rogério De Moura . **Avaliação de Desempenho em Cooperativas de Crédito: Uma Revisão Sistemática.** In: XX USP International Conference in Accounting. São Paulo. 2020.

ASSAF NETO, Alexandre. Mercado financeiro. 14. ed. São Paulo: Atlas, 2018.

BAPTISTA JUNIOR, J. H.; DIAN, M. de O. **A CRESCENTE IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO, SOBRETUDO DURANTE A PANDEMIA.** Revista Interface Tecnológica,[S. l.], v. 18, n. 1, p. 56–67, 2021. DOI: 10.31510/infa.v18i1.1109. Disponível em: <<https://revista.fatectq.edu.br/interfacetecnologica/article/view/1109>>. Acesso em: 27 nov. 2022.

BARBOSA, J. S. .; SILVA, D. B. e .; OLIVEIRA, D. C. de; JESUS, D. C. de .; MIRANDA, W. F. de . **Data protection and information security in the pandemic COVID-19: national context.** Research, Society and Development, [S. l.], v. 10, n. 2, p. e40510212557, 2021. DOI: 10.33448/rsd-v10i2.12557.

BRASIL. **Resolução Nº4.893,de 26 de Fevereiro de 2021.** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cmn-n-4.893-de-26-de-fevereiro-de-2021-305689973>>. Acesso em 11 de Dez. 2022

BRASIL. **Lei Nº 5.764, de 16 de Dezembro de 1971.** Dispõe sobre a política nacional do cooperativismo. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5764.htm>. Acesso em: 11 de dez. de 2022.

BRESSAN, V. G. F., BRAGA, M. J., BRESSAN, A. A., & DE ANDRADE RESENDE FILHO, M. (2010). **UMA PROPOSTA DE INDICADORES CONTÁBEIS APLICADOS ÀS COOPERATIVAS DE CRÉDITO BRASILEIRAS.** Revista de Contabilidade e Controladoria, [S.l.], v. 2, n. 3, dez. 2010. ISSN 1984-6266. Disponível em: <<https://revistas.ufpr.br/rcc/article/view/19625/13784>>. Acesso em: 18 mar. 2023. doi:<http://dx.doi.org/10.5380/rcc.v2i3.19625>.

CAIADO A.C; CAIADO J. **Gestão de Instituições Financeira.** 3.ed. Lisboa: Edições Sílabo, 2008.

CAMPOS, André; **Sistema de Segurança da Informação: Controlando os Riscos**. 2. ed. Florianópolis: Visual Books, 2007. 218 P.

CAIÇARA JÚNIOR, Cícero. **Sistemas integrados de gestão: ERP: uma abordagem gerencial**. Curitiba: Intersaberes, 2012. 207 p. ISBN 9788582124222 (broch.)

Controls, C. I. S. "CIS Controls TM V8." Center for Internet Security (2021).

CISO, 2019. **Hackers alegam invasão do Sicoob BA (em apenas 4 minutos)**. Disponível em: <<https://www.cisoadvisor.com.br/hackers-alegam-invasao-do-sicoob-ba-em-apenas-4-minutos/>>. Acesso em: 22 de Nov.2022.

CRESOL, Instituto de Formação do Cooperativismo Solidário Relatório de sustentabilidade Cresol 2021: transformando relacionamento em resultados / Instituto de Formação do Cooperativismo Solidário. – Francisco Beltrão, PR: Cresol Instituto, 2022. 168 p. Disponível em:< https://cresol.com.br/wp-content/uploads/2022/05/RELATORIO_SUSTENTABILIDADE_CRESOL_2021.pdf>. Acesso em 23 de jan. de 2023.

CRESOL, 2022. **Cresol completa 27 anos de história**. Disponível em:<<https://cresol.com.br/cresol-completa-27-anos-de-historia-e-comemora-em-evento-aos-socios-fundadores/#:~:text=S%C3%A3o%2027%20anos%20da%20primeira,espalhadas%20por%2017%20estados%20brasileiros>>. Acesso em 23 de Jan. de 2023.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. ESCOLA SUPERIOR DE GUERRA (Brasil). **Fundamentos da Escola Superior de Guerra**. Volume I – Elementos Fundamentais. Rio de Janeiro, 2009. 66 pg.

FEBRABAN, **Conheça as tentativas de golpes financeiros mais comuns na pandemia e saiba como evitá-los**, 2020. Disponível em: <<https://portal.febraban.org.br/noticia/3522/pt-br>>. Acesso em: 20 de nov. de 2022.

GAT INFOSEC, Checklist BACEN - Resolução 4.893. Disponível em: <<https://www.gat.digital/checklist-bacen-4893-3909/>>. Acessado em 30 de Jan2023.

GEWANDSZNAJDER, F. **O que é o Método Científico**. 1989. Pioneira Editora, São Paulo. p. 226.

KONZEN, Marcos Paulo et al. **Gestão de riscos de segurança da informação baseada na norma NBR ISO/IEC 27005 usando padrões de segurança**. 2013.

MALWAREBYTES. **Tudo sobre hacking. 2022**. Disponível em: <<https://br.malwarebytes.com/hacker/>>. Acesso em: 27 de nov. 2022. OLIVEIRA, Maria Marly de. **Como fazer projetos, relatórios, monografias, dissertações e teses**. 4. Ed. Rio de Janeiro: Elsevier, 2008.

OLIVEIRA, Virgínia Izabel de e PINHIRO, Juliano Lima. Riscos Financeiros. In: GALVÃO, Alexandre , **Gestão de Risco no Mercado Financeiro: uma abordagem prática e contemporânea para empresas**. 1. ed. São Paulo: Saraiva, 2018. 281 p.

PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 4.0, PCI Security Standards Council, LLC, Wakefield, MA, 2022.

PORTAL DO COOPERATIVISMO FINANCEIRO, 2020, **Sobre o Sicredi**. Disponível em: <https://cooperativismodecredito.coop.br/2020/08/acoes-sociais-do-sicredi-no-dia-c-beneficiaram-43-milhoes-de->

mologado.pdf/16c15436-6745-a6af-6291-81f67b3f1a79?t=1662758034471>. Acesso em 23 de jan. de 2023.

SICOOB, 2021. **Em um ano, Sicoob cresce 37% em sua carteira de crédito. Disponível em: <**

https://www.sicoob.com.br/web/sicoobnossocredito/noticias/-/asset_publisher/xAiolawpOI5S/content/id/58433879?p_r_p_categoryId=1433079 >.

Acesso em 23 de jan. de 2023.

SICOOB, 2020. **Política Institucional de Segurança Cibernética do Sicoob. Disponível em: <**

<https://www.sicoob.com.br/documents/2283876/0/Pol%C3%Adtica+Institucional+de+Seguran%C3%A7a+Cibern%C3%A9tica+do+Sicoob.pdf/564df665-bf24-bb9d-52f3-4153d8717d9e?t=1625077534804> > . Acesso em 23 de jan. de 2023.

SICREDI. 2022, **Relatório de Sustentabilidade ano 2021**. Disponível em: <
https://www.sicredi.com.br/media/produtos/filer_public/2022/04/26/relatorio_sustentabilidade_sicredi_2021_260422.pdf >. Acesso em 23 de jan. de 2023.

SISTEMA OCB, **Somos cooperativismo**, c2022. Disponível em: <
<https://www.somoscooperativismo.coop.br/historia-do-cooperativismo> >. Acesso em: 09 de dez. De 2022.

SOARES, Marden Marques; SOBRINHO, Melo; **MICROFINANÇAS**, A. D. O papel do Banco Central do Brasil e a importância do cooperativismo de crédito. Brasília: BCB, v. 202, 2008.

SOUZA, Leonardo Rafael de. **Composição e atribuições dos conselhos de administração nas cooperativas brasileiras**: visão crítica à luz do plano de ação para uma década cooperativa da aliança cooperativa internacional. In: Revista Eletrônica do Curso de Direito do Centro Universitário UniOpet. Curitiba-PR. Ano XII, n. 21, jul-dez/2019. ISSN 2175-7119.

TECMUNDO, 2018. **Sicredi investiga ataque hacker e vazamento de 1 TB de dados de clientes**. Disponível em:

<**<https://www.tecmundo.com.br/seguranca/137100-sicredi-investiga-ataque-hacker-vazamento-1-tb-dados-de-clientes.htm>**>. Acesso em: 22 de Nov. de 2022.

UOL, 2021. **Ataques Cibernéticos com vírus de resgate explodem durante a pandemia saiba como se proteger?** . Disponível

em:<**<https://noticias.uol.com.br/ultimas-noticias/rfi/2021/04/21/ataques-ciberneticos-com-virus-de-resgate-explodem-durante-a-pandemia-saiba-como-se-proteger.htm?cmpid>** >. Acesso em: 20 de nov. de 2022.

VEIGA, S. M.; FONSECA, I.. **Cooperativismo**: uma revolução pacífica em ação. Rio de Janeiro: DP&A, 2002. 106 p.

ZEFERINO, D. 2022. **ISO 27001**: para que serve e como obter a certificação? . Disponível em:**<https://www.certifiquei.com.br/iso-27001/>**. Acesso em 23 de jan. de 2023.