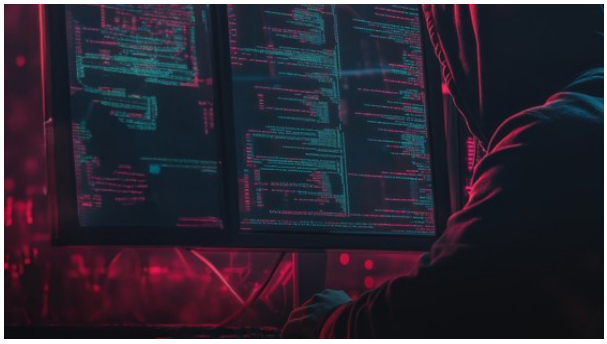
Guerra invisível: sua cooperativa sobreviveria a um ataque hacker hoje?



Ataques digitais crescem contra instituições financeiras no Brasil e atingem o cooperativismo de forma sofisticada

Em um cenário em que a tecnologia avança na mesma velocidade que as ameaças virtuais, as cooperativas de crédito se veem diante de um desafio estratégico: blindar seus sistemas e proteger seus cooperados de ataques cada vez mais sofisticados. Se antes o risco estava apenas no caixa eletrônico ou no golpe telefônico, hoje a vulnerabilidade se esconde em links falsos, aplicativos clonados e invasões silenciosas que podem render prejuízos severos. Diante disso, a pergunta que paira sobre o setor é direta e urgente: como transformar a confiança, essência do cooperativismo, em segurança também no ambiente digital?

Para Paulo Martins, diretor de Segurança da Informação Claro Empresas, deve haver uma preparação mais consistente em relação à segurança cibernética, principalmente pelo aumento da dependência de tecnologias de automação e interconexão. “Com as informações digitalizadas para serem armazenadas e utilizadas por diversas tecnologias, fundamental para a produtividade, a realidade é que as tentativas de ataque continuarão a acontecer. As empresas mais preparadas são as que têm uma boa proteção tecnológica e estão prontas para rapidamente detectar ataques e, assim, contê-los. E justamente o setor financeiro o que mais investe, e o Banco Central é um regulador que exige do setor financeiro um nível de proteção compatível com os desafios”, explica.’

Josias Sales, superintendente de Segurança Cibernética do Sicoob, concorda. Para ele, o ambiente digital é altamente dinâmico e as empresas devem acompanhar as novas tecnologias e ameaças que evoluem constantemente. *“A proteção não é absoluta nem permanente, pois ela varia com o tempo. O verdadeiro desafio da segurança digital é manter uma postura contínua de mitigação de riscos, garantindo que possamos prevenir, detectar e responder rapidamente a qualquer incidente de segurança. Para isso, é essencial implementar uma estratégia integrada, que combine múltiplas camadas de defesa do ambiente cibernético e um plano de resposta eficaz, promovendo uma proteção eficiente e capacidade de contenção ágil”*, afirma.

Panorama Nacional

O cenário da cibersegurança no Brasil é alarmante. Em 2024, os ataques de ransomware contra instituições financeiras cresceram 150%, atingindo desde bancos tradicionais até fintechs em expansão. Casos de invasões e tentativas de sequestro de dados se tornaram mais frequentes e complexos, colocando à prova os sistemas de proteção do setor. Somente entre janeiro e março de 2025, foram registradas mais de 132 mil tentativas de ataques cibernéticos, o que corresponde a 20,18% de todos os incidentes no país, segundo levantamento da ISH Tecnologia. Paralelamente, bancos e empresas de cartões registraram quase 2 milhões de tentativas de fraude no período — um aumento de 21,5% em relação a 2024 — com potencial de prejuízo superior a R$15,7 bilhões, de acordo com a Serasa Experian.

Nem mesmo as cooperativas de crédito ficaram de fora desse mapa de riscos. Embora historicamente vistas como instituições mais próximas e seguras para seus associados, elas também passaram a ser alvo de criminosos digitais, interessados em explorar vulnerabilidades tecnológicas e humanas. É notório que o crescimento acelerado do cooperativismo financeiro, que hoje já reúne mais de 15 milhões de cooperados e movimenta cifras bilionárias, funciona como um atrativo adicional para esses ataques, que vão desde invasões em sistemas internos até golpes de phishing e engenharia social direcionados aos cooperados. Diante de operações cada vez mais digitais, as cooperativas de cré-

dito precisam lidar com a mesma sofisticação de ataques que os grandes bancos já enfrentam.

Casos recentes chamam a atenção. Em São Paulo, uma fintech sofreu um ataque que bloqueou por dias o acesso às contas de clientes, exigindo um resgate milionário em criptomoedas. Em Minas Gerais, cooperados de uma instituição de crédito receberam e-mails falsos, simulando comunicações oficiais, que levaram ao roubo de dados bancários. Já no Sul do país, criminosos clonaram aplicativos de bancos e cooperativas, induzindo usuários a baixar versões fraudulentas, capazes de capturar senhas e autorizar transferências indevidas.

Nesse contexto, a expansão digital, que fortaleceu a competitividade das cooperativas frente aos grandes bancos, trouxe também um novo campo de batalha: a guerra contra os hackers. Para Henrique Carvalho, Diretor de Operações da Vortex Security, empresa de segurança eletrônica, as cooperativas não estão seguras. *"Infelizmente, convivemos num mundo onde a maior fraqueza se encontra justamente nas pessoas, nos operadores dos computadores das empresas, ou seja, no usuário. Hoje o investimento deve ser maior na detecção, para que a ameaça seja identificada a tempo"*, alerta.

Henrique Carvalho
"Um bom serviço gerenciado de Segurança da Informação e campanhas de conscientização dos usuários é o básico, além claro, de uma política de Segurança da informação"– Henrique Carvalho, Diretor de Operações da Vortex Security

Ele diz, ainda, que é necessário estar um passo à frente e vigilante, monitorando o comportamento do negócio, procurando desvios e operações que não são condizentes. *"O conceito é: não confie em ninguém. Faça validações extras com múltiplos fatores de autenticação para cada transação, conceda acessos a cada necessidade de forma única e pontual, e tenha uma monitoria dos seus executivos via serviços de CTI (Cyber Threat Intelligence)"*, define.

Outro ponto que deve ser levado em consideração é que o combate ao cibercrime não é só uma questão de infraestrutura tecnológica, mas um tema estratégico das lideranças das instituições financeiras. *"O ransomware é globalmente rentável para os criminosos, e isso exige uma postura proativa das instituições. O caminho passa por criar uma cultura interna de cibersegurança, com treinamentos contínuos de conscientização, protocolos claros de reação e investimentos constantes em ferramentas de proteção. É indispensável realizar monitoramentos internos das operações realizadas na instituição"*, ensina César Garcia, CEO da OneKey Payments.

Alexandre Murakami, Cybersecurity Sales Director da Logicalis, cita o CIO Report, estudo promovido pela Logicalis que mostra uma alta incidência de ataques cibernéticos: 88% dos CIOs relataram ter sofrido incidentes de segurança nos últimos 12 meses; 43% enfrentaram múltiplos ataques no mesmo período, mesmo com investimentos contínuos em tecnologia de proteção. *"Precisamos sempre pensar em duas etapas: como prevenir um ataque e como agir se formos atacados. Prevenir é sempre melhor do que remediar, mas se ocorrer um ataque, a empresa precisa de backup imutável e segregado, monitoramento avançado com uso de IA e resposta ágil a incidentes. Além disso, é essencial integrar times internos e fornecedores para reduzir o tempo de reação"*, detalha.

Por isso, Paulo Martins, diretor de Segurança da Informação da Claro Empresas, afirma que o crescimento dos ataques cibernéticos é um desafio constante. *"Hoje, criminosos usam tecnologias avançadas, como inteligência artificial, que aceleram o mapeamento dos alvos, tornam os ataques mais precisos e reduzem o tempo de execução. Para enfrentar isso, precisamos da chamada 'IA do Bem': sistemas que detectam ameaças rapidamente, automatizam a resposta a incidentes e nos permitem identificar vulnerabilidades antes que sejam exploradas pelos atacantes."*

Ações das cooperativas

Com o avanço da digitalização e a crescente interconectividade dos sistemas, as cooperativas de crédito passaram a enfrentar riscos cibernéticos mais sofisticados. Para reduzir vulnerabilidades, essas instituições vêm reforçando sua governança, investindo em tecnologia e capacitando equipes, além de apostar em medidas como criptografia de ponta, monitoramento 24 horas por dia com inteligência artificial e iniciativas conjuntas que permitem a criação de protocolos compartilhados.
Josias Sales, superintendente de Segurança Cibernética do Sicoob, explica que o trabalho é contínuo. Segundo ele, avaliações de risco, testes de vulnerabilidade e simulações de incidentes são fundamentais para identificar pontos críticos.

"A vulnerabilidade aumentou nos últimos anos, exigindo que reforcemos governança, investimentos e capacitação para acompanhar a evolução das ameaças e reduzir nossa exposição", afirma.

Josias Sales
"Um dos maiores mitos sobre segurança cibernética no cooperativismo é o de que 'as cooperativas não são as primeiras opções como alvo de ciberataques'. Essa percepção leva à falsa sensação de segurança e à postergação de investimentos e implementação de processos essenciais para a proteção digital". – Josias Sales, superintendente de Segurança Cibernética do Sicoob

Paulo Martins, diretor de Segurança da Informação Claro Empresas, aponta que a defesa cibernética só funciona com estratégia clara e monitoramento constante. *"É preciso identificar tudo que compõe o ambiente digital da empresa, proteger ao máximo e monitorar 24 horas por 7 dias para detectar qualquer possibilidade de incidente, permitindo que ele seja prontamente contido e controlado"*, diz.

Ele ressalta ainda que, no caso das cooperativas de pequeno e médio porte, a prioridade deve ser estruturar uma liderança em segurança. *"É essencial designar um CISO com experiência no mercado financeiro. Esse profissional define a estratégia, estabelece políticas, promove treinamentos e contrata empresas especializadas para operar a segurança da informação com métricas claras."*

Além da proteção individual de cada instituição, a colaboração também tem ganhado espaço. *"Trabalhar em conjunto permite que cada unidade reaproveite experiências das demais. Em segurança não há competição: o objetivo é proteger todo o ramo de negócios"*, reforça Paulo.

Outra opção indicada por Henrique Carvalho, Diretor de Operações da Vortex Security, é recorrer a centros de defesa cibernética, principalmente por conta da escassez de profissionais e dos altos custos de manter equipes próprias. *"Esses centros funcionam 24 horas por 365 dias e têm acesso a informações globais em tempo real, o que aumenta a eficácia e reduz o tempo de resposta a minutos. Para muitas instituições, ter um time próprio é caro e ineficiente"*, observa.

Paulo Martins
"O papel da IA na defesa cibernética será permitir uma detecção mais precisa dos incidentes, por ser uma tecnologia capaz de detectar mudanças de comportamento, seja de tráfego (quantidade e tipo) ou de tipo de uso dos recursos computacionais." – Paulo Martins, diretor de Segurança da Informação Claro Empresas

Na prática, a prevenção e a resposta a incidentes passam por operações em SOCs (Security Operations Centers), integrados a sistemas de detecção, análise e remediação de anomalias. Paulo detalha, ainda, que as medidas mais efetivas envolvem tecnologias como ZTNA (Acesso à Rede com Confiança Zero) e CTEM (Gerenciamento Contínuo de Exposição a Ameaças), além de autenticação forte, segmentação de redes e campanhas de conscientização. *"Também é essencial adotar o conceito de Security by Design, com desenvolvimento seguro (DevSecOps) desde a criação dos sistemas"*, detalha.

O elo mais fraco ainda é o humano

Apesar de investimentos crescentes em tecnologia e protocolos de segurança, as cooperativas de crédito seguem enfrentando uma ameaça que não depende de softwares ou firewalls: o fator humano. Golpes de phishing, engenharia social e fraudes por aplicativos de mensagem, como o WhatsApp, continuam sendo os mais explorados pelos criminosos digitais.

Henrique Carvalho, Diretor de Operações da Vortex Security, lembra que boa parte dos ataques não exige grande sofisticação tecnológica. *"Os maiores ataques ainda são do tipo phishing, que consiste no envio de e-mails falsos que imitam comunicações oficiais, induzindo o usuário a clicar em links que levam a páginas clonadas para capturar credenciais; e de engenharia social, que envolve contatos diretos, muitas vezes por WhatsApp, em que golpistas se passam por alguém de confiança para obter dados sigilosos. Tudo é muito simples, mas extremamente eficaz"*, explica.

Para reduzir a vulnerabilidade (refletida pela busca constante de criminosos por documentos confidenciais, informações pessoais de clientes e funcionários, acessos a recursos da empresa, códigos-fonte e bancos de dados financeiros fechados), muitas cooperativas têm apostado em treinamento de equipes, conscientização de cooperados e programas internos de compliance. Algumas instituições já lançaram aplicativos educativos e campanhas digitais voltadas a mostrar, de forma didática, como identificar tentati-

vas de fraude e reagir diante de situações suspeitas. *"É fundamental fortalecer as defesas básicas, como backups seguros e testados, segmentação de redes e autenticação multifator. Além disso, investir em monitoramento contínuo, com capacidade de detecção rápida, aliado a planos claros de resposta a incidentes, é imprescindível para minimizar impactos"*, diz Josias Sales, superintendente de Segurança Cibernética do Sicoob.

Ele ressalta que, apesar dos avanços tecnológicos, o treinamento contínuo de colaboradores ainda é a principal arma contra os cibercriminosos. *"A conscientização e o preparo constante são essenciais para reduzir o risco de vetores humanos, que continuam sendo a porta de entrada mais comum para esses ataques."*

O problema da segurança cibernética vai além e levanta uma comparação com o setor bancário tradicional. Em 2022, os bancos investiram cerca de R$3,5 bilhões em segurança da informação, valor que representou 10% de todo o orçamento de tecnologia do setor. O movimento foi impulsionado pelo avanço do Open Finance e pela modernização dos sistemas de pagamento.

Para Josias Sales, superintendente de Segurança Cibernética do Sicoob, o crescimento expressivo dos ataques de ransomware exige medidas firmes. *"Nos últimos 12 meses, houve um aumento expressivo nos ataques de engenharia social, com destaque para duas modalidades: o vishing, aplicado por chamadas telefônicas em que fraudadores se passam por representantes da instituição, e o phishing, realizado por meio de sites falsos que reproduzem a identidade visual das cooperativas".*

Ele acrescenta que esses ataques têm se tornado mais sofisticados, explorando dados personalizados para enganar cooperados e realizar transações fraudulentas. *"Além disso, criminosos passaram a combinar múltiplos canais — telefone, e-mail e redes sociais — para ampliar o impacto e dificultar a detecção. Esse cenário reforça a necessidade de investimentos contínuos em treinamento, tecnologias avançadas e uma cultura organizacional voltada à segurança, capaz de proteger tanto os sistemas quanto os cooperados contra ameaças cada vez mais complexas e dinâmicas",* destaca,
Diante disso, como preservar a confiança e a proximidade com os cooperados, essência do cooperativismo de crédito, em meio a uma guerra invisível em que cada clique pode custar milhões? Paulo Martins, diretor de Segurança da Informação Claro Empresas, diz que se trata de um ponto central que deve ser discutido pela organização. *"O risco digital é tão crítico quanto o risco financeiro tradicional. Todo o funcionamento do setor é baseado em tecnologia e conectividade, que trazem eficiência e usabilidade, mas também riscos. Se eles não forem controlados e mitigados, podem comprometer a organização como um todo."*

Henrique Carvalho vai além e alerta que os riscos digitais e financeiros são, na prática, indissociáveis. *"O impacto financeiro de um risco digital pode ser maior que o patrimônio da empresa. Já vimos casos dramáticos, como o da empresa de transportes britânica KNP, que teve toda a operação criptografada e precisou encerrar suas atividades após 158 anos de existência."*

Boas práticas em destaque

Treinamentos contínuos, autenticação multifator, backups seguros e monitoramento em tempo real estão entre as principais recomendações de especialistas para que cooperativas fortaleçam sua proteção digital. Mais do que adotar tecnologia, o desafio é consolidar uma cultura permanente de segurança e boas práticas, capaz de reduzir vulnerabilidades humanas e elevar a resiliência coletiva do setor.

"O mercado em geral investe em treinamentos contínuos para equipes internas, cobrindo desde fundamentos até cenários avançados de ataque", explica Alexandre Murakami, Cybersecurity Sales Director da Logicalis. Simulações de phishing e ransomware devem ser rotineiras, assim como trilhas educacionais segmentadas para diferentes perfis de colaboradores. *"O objetivo é que cada público receba conteúdo no nível adequado de maturidade digital. Além disso, promovemos workshops e campanhas de conscientização em canais digitais e presenciais. A meta final é consolidar uma cultura de segurança sólida e permanente em todo o ecossistema"* completa Josias Sales, superintendente de Segurança Cibernética do Sicoob.

O especialista da cooperativa diz ainda que um dos maiores riscos é a falsa sensação de que cooperativas são alvos menos atrativos para criminosos digitais. *"Esse mito leva à postergação de investimentos. Na prática, o que vemos é exatamente o contrário: atacantes exploram brechas em instituições com menor maturidade de segurança",* alerta. Ele lembra ainda que, no co-

operativismo, a fragilidade de uma entidade pode comprometer todo o sistema. "O risco cibernético não respeita fronteiras organizacionais. Segurança deve ser tratada como responsabilidade coletiva."

Alexandre Murakami
"O pilar mais importante são as pessoas, dado que a engenharia social é um dos meios de ataque. Não existe nenhuma tecnologia que seja realmente efetiva sem que as empresas tenham protocolos sólidos de capacitação de seus usuários". – Alexandre Murakami, Cybersecurity Sales Director da Logicalis

Também deve ser destacado que não há diferença de exigência entre instituições grandes ou pequenas. "As práticas devem incluir controles rigorosos de *acesso, autenticação multifator, monitoramento em tempo real, backups testados e políticas claras de uso e segurança. Também é fundamental proteger os dados dos cooperados e assegurar o cumprimento das normas regulatórias aplicáveis ao setor. Além disso, investir na conscientização das equipes, pois a falha humana continua sendo um dos principais vetores de ataque. Segurança não é uma opção técnica, mas sim um pilar essencial para a sustentabilidade do negócio, independentemente do tamanho da cooperativa"*, observa Sales.

As mudanças mais recentes no cenário de cibersegurança também pedem atenção. *"Antes o foco era na infraestrutura, agora os ataques estão mirando a camada de aplicações, como APIs e códigos de software", ressalta Alexandre. Ele aponta tecnologias priori*tárias: gerenciamento de riscos e exposição, monitoramento em tempo real com inteligência artificial, criptografia avançada e soluções de gestão de identidade. *"Ainda assim, o pilar mais importante são as pessoas. Nenhuma tecnologia funciona sem protocolos de capacitação dos usuários."*
Para cooperativas menores, a estratégia deve equilibrar custo e resiliência. *"Gestão de patches, backups imutáveis, autenticação multifator e monitoramento contínuo, mesmo que simplificado, já elevam bastante a segurança",* recomenda Alexandre. Ele sugere ainda que cooperativas avaliem a contratação de MSSPs (provedores de serviços de segurança gerenciada), que oferecem expertise e ferramentas já consolidadas como forma de incrementar as boas práticas.

No campo da colaboração, o cooperativismo mostra sua força também no ambiente digital e deve ser algo que faça parte das ações em busca de segurança cibernética. *"Compartilhar informações sobre incidentes, criar protocolos comuns de resposta e adquirir tecnologias de forma coletiva pode reduzir custos e ampliar a resiliência do sistema"*, defende o especialista.

Já Henrique Carvalho, Diretor de Operações da Vortex Security, reforça a necessidade de inteligência artificial como aliada estratégica. *"Monitorar o comportamento dos usuários em tempo real, reagir rapidamente e aplicar frameworks de investigação com apoio de IA é a chave. O perímetro já não é suficiente. É preciso olhar o negócio como um todo."*

O que vem por aí
O cenário de segurança cibernética para cooperativas de crédito deve se tornar ainda mais desafiador nos próximos anos, com ataques mais sofisticados, uso crescente de inteligência artificial e exploração de vulnerabilidades em APIs e sistemas de aplicações. Especialistas apontam que deepfakes para golpes, ransomware como serviço (RaaS) e phishing direcionado com dados vazados estão entre as ameaças que devem ganhar força entre 2025 e 2026. Para se proteger, cooperativas precisam combinar tecnologias avançadas, monitoramento em tempo real e capacitação contínua de usuários, reforçando a resiliência coletiva do setor e prevenindo impactos sistêmicos.

Henrique Carvalho, da Vortex Security, alerta que as cooperativas podem sofrer com os vishings, em que os criminosos utilizam chamadas de voz para enganar as vítimas e conseguir informações confidenciais. *"Com a IA ficando cada vez mais poderosa, os deep fakes podem sim fazer um estrago inicial, mas basta implementar um sistema de reconhecimento facial maduro para resolver de forma rápida, dando vida curta a este tipo de ameaça",* ensina.

Para Alexandre Murakami, Cybersecurity Sales Director da Logicalis, uma mudança significativa no mercado é o aumento dos ataques focados na camada de aplicações, como APIs e códigos de software, antes centrados na infraestrutura de rede. Para ele, tecnologias como monitoramento em tempo real baseado em inteligência artificial, criptografia avançada e gestão de identidade e acesso (IAM) são essenciais. "O pilar mais importante são as pessoas. Nenh*uma tecnologia funciona sem protocolos sólidos de*

capacitação dos usuários", alerta.

Outro desafio está na regulamentação de tecnologias emergentes. Blockchain e biometria trazem oportunidades, mas também exigem atenção à LGPD, responsabilidade jurídica e segurança de dados sensíveis. *"O uso de monitoramento em tempo real aliado a inteligência artificial e machine learning permite acompanhar o perfil e o comportamento de cada usuário, detectar desvios de padrão e agir preventivamente. Camadas adicionais de proteção, como autenticação multifator e análise comportamental de transações, reduzem o risco de fraude e aumentam a confiança dos cooperados"*, afirma César Garcia, CEO da OneKey Payments.

Ele acrescenta que o setor também deve investir em seguros cibernéticos, considerados cada vez mais essenciais. "Hoje, entre 30% e 40% das instituições financeiras possuem cobertura específica, mas a tendência é que isso se torne padrão, ao lado de tecnologias e práticas preventivas", diz.

Cesar Garcia
"Devemos ver um aumento significativo no uso de deep fakes para aplicação de golpes de engenharia social com aparência extremamente convincente, inclusive para se passar por cooperados ou gestores." – César Garcia, CEO da OneKey Payments

Por fim, é essencial que a combinação de tecnologia, capacitação e governança seja implementada nas cooperativas de forma efetiva, para que o setor possa enfrentar a crescente sofisticação dos ataques e fortalecer a resiliência coletiva, garantindo proteção aos cooperados e à integridade do sistema financeiro cooperativo. Tudo isso com o auxílio da inteligência artificial. *"O papel da IA na defesa cibernética será permitir uma detecção mais precisa dos incidentes, por ser uma tecnologia capaz de detectar mudanças de comportamento, seja de tráfego (quantidade e tipo) ou de tipo de uso dos recursos computacionais"*, diz Paulo Martins, diretor de Segurança da Informação Claro Empresas.

Além disso, recursos como o Blockchain e a biometria devem estar em foco. *"Na disciplina do blockchain, a completa aderência a LGPD (Controlador e Operador), a Lei Transfronteiriça, que traz à tona a questão judicial no âmbito global e a responsabilidade do status legal de contratos inteligentes deve ser um ponto de atenção. Já na questão biométrica, vejo com preocupação a segurança dos dados biométricos e possíveis vazamentos"*, avalia Henrique Carvalho.

Josias Sales, da Sicoob, concorda e diz estar preocupado com o fato da rápida evolução das ameaças digitais, com ataques cada vez mais sofisticados e automatizados. *"A combinação de engenharia social com tecnologias emergentes, como o deep fake, tende a se intensificar, tornando os golpes mais difíceis de detectar. Além disso, a expansão de modelos de ataque como serviço na nuvem vai facilitar o acesso de criminosos a ferramentas avançadas, ampliando o alcance e a escala dos ataques. Por isso, a segurança não é responsabilidade de uma única entidade e precisa ser encarada como uma responsabilidade sistêmica, com padrões bem definidos, colaboração ativa e estratégia conjunta"*.

César Garcia complementa, afirmando que um dos principais desafios regulatórios será garantir a integração e compatibilidade dessas soluções com o sistema financeiro nacional, preservando a privacidade dos dados sensíveis dos cooperados, alinhados com a LGPD. *"À medida que essas tecnologias ganham escala, tende a aumentar também a exigência de certificações técnicas, trazendo maior segurança operacional por parte"*, finaliza.

Segurança Cibernética no Cooperativismo
Integrar inteligência artificial nas estratégias de defesa será decisivo para acompanhar a evolução das ameaças e proteger a confiança dos cooperados. Há uma integração crescente entre o Centro Cooperativo Sicoob, centrais e cooperativas, com o objetivo de padronizar protocolos de segurança, elevar a maturidade cibernética e criar uma cultura de colaboração frente aos riscos digitais. Um exemplo concreto dessa integração é o Projeto Sistêmico de Riscos e Segurança Cibernéticos, que estabelece diretrizes comuns, define padrões mínimos de proteção e cria mecanismos de governança e acompanhamento para garantir que todas as cooperativas, independentemente do porte, estejam alinhadas aos requisitos atuais de segurança. O projeto também fomenta o compartilhamento de informações sobre incidentes, vulnerabilidades, ameaças emergentes e boas práticas, fortalecendo a capacidade de resposta coletiva.

O Sicoob tem um Centro de Operações de Segurança (SOC) que funciona 24 horas por dia, monitorando redes e sistemas de forma contínua e atuando conforme protocolos rigorosos de resposta a incidentes. Para complementar a estrutura técnica, são promovidos webinars e palestras frequentes

sobre fraudes, incidentes recentes e iniciativas de defesa cibernética, fortalecendo a cultura de segurança em toda a rede e tornando cada membro mais preparado para identificar e reagir a possíveis ataques.

Os programas de capacitação incluem trilhas de aprendizagem, treinamentos obrigatórios, simulações de phishing e campanhas internas regulares, mantendo os colaboradores atualizados diante das ameaças e consolidando a cultura de segurança. Para os cooperados, os canais digitais desempenham papel preventivo e didático. O SuperApp, por exemplo, possui mecanismos de proteção contra golpes como "Falsa Central" e "Mão Fantasma", além de alertas no Pix, bloqueando tentativas de fraude e orientando os usuários a identificar sinais de golpes, promovendo uma experiência segura e intuitiva.

A conscientização dos cooperados é trabalhada de forma segmentada, considerando diferentes idades e níveis de familiaridade digital. As campanhas são contínuas e abrangem múltiplos canais, físicos e digitais. O SuperApp é projetado para oferecer navegação intuitiva e recursos de proteção, combinando educação, tecnologia e comunicação eficaz, criando um ambiente digital mais seguro e confiável. Além disso, o diálogo constante com o Banco Central e outros órgãos reguladores reforça a segurança digital no cooperativismo. O BC apoia iniciativas que elevam a maturidade em segurança, promovem boas práticas e garantem conformidade regulatória, criando um ambiente seguro que protege tanto as cooperativas quanto os cooperados.

Eleva 2026 acontece nesta sexta-feira

Nesta sexta-feira (27), o Sistema OCB realiza o Eleva 2026, um dos principais momentos de alinhamento estratégico da instituição com as 27 Organizações Estaduais (OCEs). O evento será transmitido ao vivo, e a proposta é dar a largada oficial no ciclo de metas, apresentar prioridades para o ano e reforçar a atuação integrada em todo o país.

O presidente do Conselho de Administração do Sistema OCB, Márcio Lopes de Freitas, destaca que o evento vai além do simples cumprimento de metas. "O Eleva é o momento em que reafirmamos nossa unidade e nossa responsabilidade com o futuro do cooperativismo. Trabalhamos com planejamento, método e estratégia, mas, acima de tudo, com propósito".

Com o tema Times de excelência que impulsionam o coop, o evento destaca que a excelência é uma prática construída no dia a dia, com clareza de objetivos, acompanhamento consistente e cooperação entre áreas e unidades estaduais.

Tania Zanella, presidente executiva do Sistema OCB, ressalta que metas bem definidas são fundamentais para esse processo. "Metas claras são instrumentos de alinhamento e de crescimento. Elas ajudam as equipes a entenderem aonde precisamos chegar, organizam a atuação coletiva e fortalecem o senso de propósito. Quando há direção e acompanhamento, conseguimos impulsionar resultados de forma mais consistente e sustentável"

O evento também apresenta o calendário de capacitações presenciais dos times temáticos, previstas para acontecer em Brasília ao longo do ano, e detalha critérios de premiação e recursos suplementares vinculados ao desempenho das OCEs.

Estratégia e integração

O Eleva é o momento em que as lideranças nacionais e estaduais alinham prioridades e consolidam o compromisso com a execução das soluções do Sistema OCB. A iniciativa articula todas as áreas, desde o desenvolvimento de cooperativas até as áreas de operações, gestão e tecnologia.

Para o presidente Márcio, o diferencial do Eleva está na mobilização coletiva. "Somos um sistema. Quando trabalhamos de forma coordenada, compartilhando informações qualificadas e executando bem nossas estratégias, ampliamos nossa capacidade de representar e defender o cooperativismo brasileiro. O Eleva é o ponto de partida dessa jornada", destacou.

EDITAL DE CONVOCAÇÃO – PROVENORTE – COOPERATIVA HABITACIONAL DOS PROFISSIONAIS DA ÁREA DE PROPAGANDA MÉDICA DO NORTE E NOROESTE FLUMINENSE – CONVOCAÇÃO DE AGO – ASSEMBLÉIA GERAL ORDINÁRIA NA MODALIDADE PRESENCIAL – O Diretor Presidente da **PROVENORTE – COOPERATIVA HABITACIONAL DOS PROFISSIONAIS DA ÁREA DE PROPAGANDA MÉDICA DO NORTE E NOROESTE FLUMINENSE**, registrada na JUCERJA sob o NIRE 33.4.0005321-4, e inscrita no CNPJ sob o nº de registro 20.668.288/0001- 84, O Sr. **Carlos Alberto Almeida da Silva**, no exercício das suas atribuições, que lhe são conferidas pelo Estatuto Social, convoca os sócios cooperados para participarem da **AGO – Assembleia Geral Ordinária a ser realizada na modalidade presencial no dia 13/03/2026**, na Rua Visconde de Itaboraí, 620 / casa 34, Pq. Rosário, Cep: 28026-148, Campos dos Goytacazes-RJ, em suas áreas comuns, a fim de dar maior segurança e possibilitar a participação dos sócios. Para tanto, em primeira convocação às 18:00h com a presença mínima de 2/3 (dois terços) dos sócios cooperados; em segunda convocação às 19:00h com a presença mínima de metade mais um do total de sócios cooperados, e em terceira e última convocação às 20:00h com presença mínima de 10 (dez) sócios cooperados. **Na data da presente convocação a cooperativa possui no total de seu quadro social, 29 (vinte e nove) sócios cooperados**. **A Ordem do Dia da AGO é a seguinte**: **1)** Apresentação da Prestação de Contas relativa ao Exercício 2025 para Deliberação da Assembleia, conforme itens a seguir: **a)** Apresentação do Relatório de Gestão da Diretoria; **b)** Apresentação do Balanço Geral e DSPE – Demonstração de Sobras ou Perdas do Exercício; **c)** Apresentação do Parecer do Conselho Fiscal. **2)** Deliberação da Assembléia sobre a Prestação de Contas relativa ao Exercício 2025; **3)** Deliberação da Assembléia sobre a Destinação/Rateio das Sobras ou Perdas do Exercício 2025; **4)** Eleição do Novo Conselho Fiscal para o Mandato de um ano 2026/2027; **5)** Registro da ratificação do pedido de renúncia a cargo da diretoria; **6)** Eleição de nova diretoria para o exercício de mandato do quadriênio 2026 a 2030; **7)** Registro da ratificação de Entrada e Saída de cooperados; **8)** Demais assuntos de interesse social.

Campos dos Goytacazes – RJ, 26 de Fevereiro de 2026.

Carlos Alberto Almeida da Silva
Diretor Presidente

EDITAL DE CONVOCAÇÃO
TELECOOP COOPERATIVA DE TRANSPORTE DE FRETAMENTO, TURISMO, CARGA E TRANSPORTES RODOVIÁRIO DE PASSAGEIROS NO ÂMBITO MUNICIPAL, INTERMUNICIPAL E INTERESTADUAL

AGO – ASSEMBLÉIA GERAL ORDINÁRIA E AGE – ASSEMBLEIA GERAL EXTRAORDINÁRIA NA MODALIDADE PRESENCIAL

O Presidente da **TELECOOP COOPERATIVA DE TRANSPORTE DE FRETAMENTO, TURISMO, CARGA E TRANSPORTES RODOVIÁRIO DE PASSAGEIROS NO ÂMBITO MUNICIPAL, INTERMUNICIPAL E INTERESTADUAL**, registrada na JUCERJA sob o NIRE 33.4.0005004-5 e inscrita no CNPJ sob o nº. de registro 10.813.667/0001-67, Sr. CAIO SOUTO ALVES, no exercício das suas atribuições, convoca os sócios cooperados para participarem da AGO – Assembleia Geral Ordinária e AGE – Assembleia Geral Extraordinária, a serem realizadas em conjunto no dia **08 de março de 2026**, na modalidade presencial, nas dependências do prédio onde a cooperativa está estabelecida, em suas áreas comuns, a fim de dar maior segurança e possibilitar a participação dos sócios. Para tanto, a AGO e AGE serão realizadas na Estrada do Engenho Velho, 840, Taquara, Rio de Janeiro – RJ, CEP: 22723-395, em primeira convocação as 08:00 h com a presença mínima de 2/3 (dois terços) dos sócios cooperados; em segunda convocação as 09:00 h com a presença mínima de metade mais um dos sócios cooperados e em terceira e última convocação as 10:00 h com a presença mínima de 10 (dez) sócios cooperados. **Na data da presente convocação a cooperativa tem no total do seu quadro social 314 (trezentos e quatorze) associados.**

A Ordem do Dia da AGO é a seguinte:

1. Apresentação da Prestação da Contas relativa ao Exercício 2025 para Deliberação da Assembleia conforme itens a seguir:
    a. Apresentação do Relatório de Gestão da Diretoria;
    b. Apresentação do Balanço e DSPE – Demonstração de Sobras ou Perdas do Exercício;
    c. Apresentação do Parecer do Conselho Fiscal.
2. Deliberação da Assembleia sobre a Prestação de Contas relativa ao Exercício 2025;
3. Deliberação da Assembleia sobre a Destinação de Sobras ou Rateio de Perdas do Exercício 2025;
4. Eleição do Novo Conselho Fiscal para o Mandato de um ano – 2025/2026.

A Ordem do Dia da AGE é a seguinte:

1. Apresentação para deliberação da Assembleia do novo projeto de Estatuto Social conforme itens a seguir:
    a. Alteração da Denominação Social;
    b. Atualização e adequações na Redação do Estatuto Social;
    c. Revisão geral e consolidação das mudanças na Redação do Estatuto Social.
2. Apresentação para deliberação da Assembleia do novo projeto de Regimento Interno Disciplinar conforme itens a seguir:
    a. Atualização da Redação do Regimento Interno Disciplinar;
    b. Revisão geral e mudanças na Redação do Regimento Interno Disciplinar.
3. Apresentação para deliberação da Assembleia do projeto de Código de Ética;
4. Demais Assuntos de Interesse Social sem Deliberação.

Rio de Janeiro – RJ, 26 de fevereiro de 2026.

Caio Souto Alves – Diretor Presidente