**1.** Esta Política:

**a)** visa prover diretrizes para a segurança da informação relacionadas ao manuseio, controle, à proteção (contra indisponibilidade, divulgação imprópria, acesso indevido, e modificação não autorizada de informações e de dados) e ao descarte, promovendo a melhoria contínua dos processos relacionados à segurança da informação, mantendo a confidencialidade, integridade e disponibilidade das informações do Sicoob;

**b)** foi elaborada e é revisada, anualmente, por proposta da Superintendência de Controles, por meio da Área de Privacidade de Dados do Centro Cooperativo Sicoob (CCS), a qual considera os resultados dos testes das auditorias interna e independente, as normas vigentes, bem como as sugestões encaminhadas pelas entidades do Sicoob;

**c)** é aprovada pelo Conselho de Administração do CCS – Sicoob Confederação;

**d)** tem aplicação imediata pelas entidades do Sicoob, devendo o conteúdo ser levado ao conhecimento do seu respectivo órgão de administração, mediante registro em ata;

**e)** é aplicável às informações armazenadas ou em trânsito, em meio físico ou digital;

**f)** tem o cumprimento acompanhado pela Diretoria Executiva do CCS (Direx CCS) – Sicoob Confederação e pelas áreas responsáveis pela segurança da informação das entidades do Sicoob;

**g)** é divulgada aos empregados das entidades do Sicoob e a qualquer pessoa que mantenha relação de prestação de serviço com o Sicoob.

**2.** Para fins desta Política, são observados os seguintes conceitos:

**a)** *entidades do Sicoob*: cooperativas centrais e singulares, e entidades do Centro Cooperativo Sicoob (CCS);

**a.1)** *entidades do CCS*: Sicoob Confederação, Banco Sicoob, Sicoob Consórcios Sicoob DTVM, Sicoob Pagamentos, Sicoob Previ, Sicoob Seguradora, Instituto Sicoob e Fundo de Proteção do Sicoob;

**b)** *usuário*: indivíduo que interage com um sistema, aplicativo ou serviço para realizar tarefas específicas de acordo com funções laborais;

**c)** *criador da informação ou gestor da informação*: pessoa ou entidade responsável pela geração ou produção de dados e de informações dentro de um contexto específico;

**d)** *acessos conflitantes ou perfis conflitantes*: situação em que um usuário possui permissões ou privilégios que entram em conflito com as políticas da organização, podendo resultar em vulnerabilidades ou riscos de segurança;

**e)** *ciclo de vida*: criação, recebimento, manuseio, transporte, armazenamento ou descarte das informações;

**f)** *ativo*: qualquer recurso que tenha valor para a organização. Pode ser tangível, ou intangível:

**e.1)** *ativo de informação*: dados ou informações, físicos ou digitais, que possuem valor para a organização. Ativos de informação podem incluir bancos de dados, documentos, *e-mails*, planilhas e qualquer outro meio onde a informação seja armazenada, processada e utilizada;

**e.2)** *ativo de tecnologia*: recursos tecnológicos que suportam o processamento, armazenamento e a comunicação de informações. Inclui componentes físicas (*hardware*), como servidores, computadores, dispositivos móveis, redes e componentes lógicos (*software*), como sistemas operacionais e aplicativos;

**g)** *inventário dos ativos*: registro detalhado de todos os recursos e de todas as propriedades, tanto físicos(as) quanto digitais, de uma entidade, utilizado para gerenciar e manter o controle eficiente dos ativos;

**h)** *recursos corporativos*: ativos e meios disponíveis dentro de uma entidade para auxiliar no alcance dos objetivos, incluindo recursos financeiros, humanos, tecnológicos e materiais;

**i)** *modem de tecnologia móvel*: dispositivo que possibilita a conexão de dispositivos à internet, geralmente utilizando redes móveis (como 3G, 4G ou 5G) para transmitir dados e estabelecer conectividade *online*;

**j)** *pastas funcionais*: diretórios organizacionais designados para armazenar e categorizar os documentos e as informações com base em funções ou departamentos específicos de uma estrutura organizacional;

**k)** *confidencialidade*: atributo que objetiva garantir que a informação é acessível apenas para indivíduos autorizados, e proteger os dados contra acessos não autorizados ou divulgação indevida;

**l)** *integridade*: assegura que a informação é precisa e completa, e que não foi alterada de forma não autorizada;

**m)** *disponibilidade*: assegura que os usuários autorizados possuem acesso aos dados e aos recursos associados a esses dados sempre que necessário e que

os sistemas e aplicativos estejam operacionais e acessíveis quando necessário;

**n)** *rede de dados*: infraestrutura que possibilita a comunicação e troca de informações, abrangendo tanto os componentes físicos (*hardware*) quanto os elementos lógicos (*software*);

**o)** *sistemas corporativos*: conjunto integrado de aplicativos e tecnologias utilizado por uma empresa para suportar suas operações e seus processos de negócios.

**3.** Os atributos básicos para a segurança da informação do Sicoob são: confidencialidade; integridade e disponibilidade.

**4.** As entidades do Sicoob devem seguir as regras e soluções dispostas pelo CCS sobre a segurança da rede de dados e dos ativos de tecnologia para garantir os atributos mínimos necessários para a segurança da informação no Sicoob.

**5.** O Sicoob respeita a privacidade, zelando pela disponibilidade, integridade e confidencialidade dos dados pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte.

**6.** A utilização dos recursos e ativos corporativos pode ser monitorada, não sendo permitido ao usuário o uso desses recursos para atividades que não estejam relacionadas ao exercício das suas funções.

**7.** O inventário dos ativos tecnológicos deve ser realizado sempre que for necessário ou, no mínimo, a cada 2 (dois) anos.

**8.** As informações devem ser classificadas de acordo com os requisitos de proteção esperados em termos de finalidade, sigilo, valor, requisitos legais, sensibilidade e

necessidades do negócio, de modo que busquem assegurar a confidencialidade, a integridade, a disponibilidade dos dados e dos sistemas de informação utilizados.

**9.** Os documentos produzidos no ambiente do Sicoob recebem, do criador da informação, o nível de classificação de acordo com as informações do conteúdo.

**10.** Informações confidenciais não devem ser discutidas em locais públicos ou de circulação de pessoas ligadas ao Sicoob.

**11.** Cada área deve estabelecer a classificação adequada durante todo o ciclo de vida dos ativos de informação, considerando, inclusive, os aspectos legais de cada ativo.

**12.** Os empregados das entidades do Sicoob devem assinar o termo de responsabilidade e de confidencialidade relativo aos ativos de informação a que tiver acesso, o qual fica arquivado nos registros do(a) empregado(a).

**13.** O processo de desligamento dos empregados das entidades do Sicoob exige a devolução dos ativos em seu poder.

**14.** As instalações que abrigam informações, documentos e equipamentos de processamento devem ter perímetros de segurança com controles apropriados à classificação, para assegurar a confidencialidade, a integridade e a disponibilidade.

**15.** O Sicoob possui requisitos de segurança para o controle de acesso à rede, aos sistemas operacionais, às aplicações e às informações. Os sistemas sensíveis são isolados e o acesso à informação restrito.

**16.** Qualquer acesso à informação deve ser previamente autorizado pela área competente, levando em conta, estritamente, as funções desenvolvidas pelo usuário.

**17.** O acesso aos sistemas e às informações é concedido com base no princípio do mínimo privilégio. Cada usuário possui acesso apenas às informações necessárias para o desempenho de suas funções.

**18.** Para acessar os sistemas corporativos disponibilizados pelo Sicoob, o usuário deve estar identificado, autenticado e autorizado. Suas ações podem ser auditadas a qualquer tempo. Os acessos são concedidos à medida que forem solicitados e autorizados pela área responsável.

**19.** Não é concedido acesso a usuários e entidades externas às redes do Sicoob sem a autorização formal dos gestores responsáveis pelas áreas de segurança do Sicoob.

**20.** O Sicoob determina por meio da Área de Privacidade de Dados do CCS, as regras de acesso e de bloqueio a páginas eletrônicas para que não haja comprometimento da segurança lógica nem impacto nas regras de negócio que possam causar danos à imagem da entidade.

**21.** Os recursos providos pelo Sicoob (correio eletrônico, acesso à internet, serviços, computadores etc.) são monitorados e fiscalizados, sendo utilizados para o suporte das atividades desenvolvidas no Sicoob, e seguem as regras de classificação da informação.

**22.** O *e-mail* corporativo e as informações tramitadas por esse meio eletrônico pertencem ao Sicoob e devem ser usados, exclusivamente, para fins de atividades laborais.

**23.** Em conformidade com o disposto no inciso I do § 1º do art. 13 da Lei Complementar nº 130/2009, mediante assinatura de Termo de Responsabilidade e Confidencialidade no Tratamento de Dados, será concedido o acesso aos arquivos de dados para uso na geração das informações e para subsidiar estudos técnicos de lançamento de

produtos e serviços às entidades do Sicoob responsáveis pela gestão de processos sistêmicos.

**24.** A gestão de acessos tem por objetivo estabelecer critérios para o acesso aos sistemas eletrônicos utilizados pelas entidades do Sicoob.

**25.** O Sicoob implementa múltiplo fator de autenticação de forma consistente e conforme necessário para garantir o acesso seguro aos seus sistemas informatizados.

**26.** As rotinas relacionadas à gestão de acesso aos sistemas corporativos do Sicoob deverão ser realizadas pela Área de Privacidade de Dados do CCS ou pelas cooperativas centrais do Sicoob, observando os normativos sistêmicos emitidos pelo CCS.

**27.** As revisões dos acessos devem ser realizadas de forma continuada, a fim de garantir a inativação de usuários indevidos, a revisão das permissões concedidas e a existência de perfis de acesso com privilégio maior do que o necessário para a execução das atividades.

**28.** Deve ser realizada, no mínimo, anualmente, a revisão integral dos acessos de subordinados pelos gestores das áreas, inclusive de usuários corporativos/robôs (Automação Robótica de Processos – RPA).

**29.** São prerrogativas dos gestores de negócio apontar os acessos indevidos, conflitantes ou cumulativos que podem incorrer em riscos, e solicitar ajustes na matriz de acessos ou na concessão à área responsável da gestão de acessos na entidade.

**30.** O CCS define as regras referentes à guarda dos dados e das informações acessadas pelas entidades do Sicoob por meio dos serviços de tecnologia disponibilizados.

**31.** As informações produzidas no ambiente das entidades do Sicoob, com a utilização de recursos próprios ou de serviços contratados, são de propriedade das entidades e somente poderão ser copiadas, divulgadas e publicadas com a autorização da área responsável pela informação.

**32.** As senhas de acesso são individuais, intransferíveis, de responsabilidade única e exclusiva do usuário, e não podem ser compartilhadas ou divulgadas. As senhas respeitarão regras de complexidade mínima definidas, com obrigatoriedade de troca periódica e bloqueio após tentativas falhas de *login*.

**33.** Todos os *softwares* utilizados deverão ser licenciados. Não devem ser instalados, conectados ou utilizados *softwares* não autorizados pelo CCS, independentemente da natureza de uso ou aplicação.

**34.** Deve-se respeitar o direito à propriedade intelectual, na forma da legislação em vigor, não reproduzindo ou divulgando material sem a autorização do autor.

**35.** É vedada a instalação, conexão ou utilização de quaisquer dispositivos de armazenamento e conectividade (modem de tecnologia móvel, HD externo, *pendrive* etc.) em equipamentos pertencentes às entidades Sicoob ou de terceiros – salvo os autorizados pelas áreas responsáveis pela segurança da informação da entidade.

**36.** As cópias de segurança e a restauração de informações são realizadas segundo parâmetros de criticidade, prioridade, bem como observando regras específicas de geração e restauração, conforme a classificação da informação.

**37.** O acesso remoto e o monitoramento dos trabalhos realizados devem respeitar as recomendações de segurança, de forma a garantir a integridade, a disponibilidade, a confidencialidade e a autenticidade das informações manipuladas.

**38.** Para os contratos firmados com terceiros, devem-se incluir cláusulas de cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD), de confidencialidade, de acordo de nível de serviço e em cumprimento ao disposto nesta Política e nos documentos a ela subordinados.

**39.** A utilização e a gestão de sistemas de informação devem estar de acordo com as leis, os contratos e em conformidade com políticas e padrões de segurança sistêmicos fixados pelo CCS.

**40.** As entidades do Sicoob devem definir processos para aquisição, desenvolvimento e manutenção de sistemas de informação que garantam os atributos definidos por esta Política.

**41.** As normas dos órgãos reguladores prevalecem sobre esta Política, sempre que houver divergência ou conflito.

**42.** Complementam a presente Política, e a ela se subordinam, todas as normas internas que regulam a segurança da informação no âmbito do Sicoob.

## Controle de Atualizações

| Data | Link CCS | Link Cooperativas |
|---|---|---|
| Atualizada – RES CCS 348, 2/6/2025 | Acesse | Acesse |
| Atualizada – RES CCS 256, 26/4/2024 | Acesse | Acesse |
| Atualizada – RES CCS 166, 24/4/2023 | Acesse | Acesse |
| Atualizada – RES CCS 097, 24/4/2023 | Acesse | Acesse |
| Atualizada – RES CCS 021, 15/4/2021 | Acesse | Acesse |