1. Esta Política Institucional de Segurança da Informação do Sicoob:

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

   b) é elaborada e revisada, anualmente, por proposta da Área de Segurança da Informação do Centro Cooperativo Sicoob (CCS), a qual considera os resultados dos testes das auditorias interna e externa e as normas vigentes, bem como as sugestões encaminhadas pelas entidades do Sicoob;

   c) é aprovada pelo Conselho de Administração do CCS;

   d) é aplicável às informações armazenadas ou em trânsito;

   e) é observada por todos os componentes da estrutura organizacional das cooperativas centrais e singulares e das entidades do CCS (dirigentes, empregados e estagiários) e pelas demais pessoas com acesso autorizado às informações;

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

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

2. Os atributos básicos para a segurança da informação do Sicoob são: confidencialidade, integridade e disponibilidade.

3. As entidades seguem as regras e soluções dispostas pelo Sicoob que dispõem sobre a segurança da rede de dados e dos ativos de tecnologia, para garantir os atributos básicos para a segurança da informação do Sicoob.

4. 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.

5. Aos ativos da informação são aplicados requisitos de classificação, de acordo com regras institucionalizadas definidas com base nos aspectos legais e necessidades do negócio, as quais estão definidos em manual.

6. Todo o acesso às informações e a utilização dos recursos corporativos poderá ser monitorado, 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 de informação deve ser realizado sempre que 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 e a disponibilidade dos dados e dos sistemas de informação utilizados.

9. Os documentos produzidos no ambiente do Sicoob recebem, do responsável de cada área, o nível de classificação de acordo com as informações do conteúdo.

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

11. A Diretoria Executiva estabelece o ciclo de vida (recebimento, manuseio, transporte, armazenamento e/ou descarte) dos ativos de informação, adequado à classificação e aspectos legais de cada ativo.

12. Os empregados das entidades do Sicoob assinam termo de responsabilidade e de confidencialidade relativos aos ativos de informação a que tiver acesso, o qual fica arquivado nas respectivas pastas funcionais.

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

14. As instalações que abrigam informações, documentos e equipamentos de processamento de informação sensível devem ter perímetros de segurança com controles apropriados que garantem o acesso apenas a pessoas autorizadas, bem como mecanismos de prevenção a incêndios e outros tipos de sinistros.

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 atividades desenvolvidas pelo usuário.

17. Para acessar os sistemas corporativos disponibilizados pelo Sicoob, o usuário deverá estar identificado, autenticado e autorizado. Suas ações poderão ser auditadas a qualquer tempo. Os acessos serão concedidos à medida que solicitados e autorizados pela área responsável.

18. Não é concedido acesso a usuários e entidades externas às redes do Sicoob sem autorização formal do gestor responsável pela área de segurança do Sicoob.

19. O Sicoob determina as regras de acesso e de bloqueio a páginas eletrônicas para que não haja comprometimento da segurança da informação, impacto nas regras de negócio e danos à imagem.

20. Os recursos de correio eletrônico corporativo são monitorados e serão utilizados para suporte das atividades desenvolvidas no Sicoob e seguem as regras de classificação da informação.

21. Em conformidade com o Art. 13, parágrafo único da Lei Complementar 130/2009, mediante assinatura de Termo de Responsabilidade e Confidencialidade no Tratamento de Dados, será concedido às entidades do Sicoob responsáveis pela gestão centralizada de processos sistêmicos em âmbito nacional ou regional, acesso, por meio dos gestores designados pela diretoria da entidade interessada, a arquivos de dados para uso na geração das informações necessárias e também para subsidiar estudos técnicos para lançamento de produtos e desenvolvimento de outras atividades vinculadas ao correspondente objeto social.

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

23. É atribuição do diretor encarregado pela atividade de controles internos das entidades do Sicoob designar formalmente os responsáveis pela gestão de acesso, bem como monitorar e assegurar que as políticas sistêmicas e procedimentos relativos à gestão de acessos sejam adotados e praticados.

24. As rotinas relacionadas à gestão de acesso aos sistemas corporativos do Sicoob deverão, de preferência, ser realizadas pela Área de Segurança da Informação do CCS, adotando matriz única de acessos, ou pelas cooperativas centrais do Sicoob, observando os normativos sistêmicos emitidos pelo CCS.

25. A matriz, grupos e permissões de acesso deverão respeitar a hierarquia de atividades, cargos ou funções, impedindo que ocorram acessos conflitantes e cumulativos, mitigando a possibilidade de riscos operacionais, financeiros e ocorrência de fraudes.

26. As revisões de acesso 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 execução das atividades. No mínimo anualmente, deve ser realizada a revisão integral dos acessos concedidos.

27. É prerrogativa dos gestores de negócio apontar os acessos conflitantes e cumulativos que podem incorrer em riscos e solicitar ajustes na concessão de acessos.

28. O CCS define as regras referentes a guarda dos dados e informações acessadas pelo Sicoob por meio dos serviços de tecnologia disponibilizados.

29. As informações produzidas no ambiente das entidades, por meio de recursos próprios ou de serviços contratados, são de propriedade das entidades e somente poderão ser copiadas, divulgadas e publicadas com autorização da área responsável pela informação.

30. 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.

31. Todos os *softwares* utilizados deverão ser licenciados. Não devem ser instalados, conectados e utilizados *softwares* não autorizados pelo CCS, independentemente da natureza de uso ou aplicação. Deve-se respeitar o direito à propriedade intelectual, na forma da legislação em vigor, não reproduzindo ou divulgando material sem a autorização do autor.

32. Para os contratos firmados com terceiros deve-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 a todas as regras definidas nesta Política e nos documentos a ela subordinados.

33. É vedada a instalação, conexão ou utilização de quaisquer dispositivos de armazenamento e conectividade (modem 3G/4G, HD externo, *pendrive* etc.) em equipamentos pertencentes às entidades Sicoob ou de terceiros, salvo os autorizados pela área responsável pela segurança da entidade.

34. 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.

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

36. A utilização e a gestão de sistemas de informação devem estar de acordo com as leis, contratos e em conformidade com políticas e padrões de segurança sistêmicos do Sicoob.

37. Os registros de *logs* são armazenados em bases segregadas, por período fixado, para registrar acessos a sistemas computacionais e a serviços de rede.

38. O Sicoob define processos para aquisição, desenvolvimento e manutenção de sistemas de informação que garantam os atributos definidos por esta Política.

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

40. Complementam a presente Política, e a ela se subordinam, todas as normas e procedimentos operacionais que regulam a segurança da informação do Sicoob.