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;

   b) é elaborada por proposta do Comitê de Gestão Corporativa do Sicoob;

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

   d) é revisada anualmente pelo Comitê de Gestão Corporativa do Sicoob, considerando também as sugestões encaminhadas pelas entidades do Sicoob;

   e) é aplicável às informações armazenadas ou em trânsito;

   f) é observada por todos os usuários que compõem as estruturas organizacionais (dirigentes, empregados e estagiários) das entidades do Sicoob e pelas demais pessoas com acesso autorizado às informações do Sicoob;

   g) tem o cumprimento acompanhado pelo Comitê de Gestão Corporativa do Sicoob e pelas áreas de segurança das entidades;

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

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

3. As entidades seguem as regras e soluções dispostas pelo Sicoob Confederação que dispõe sobre a segurança da rede de dados e dos ativos de tecnologia, para garantia da confidencialidade, disponibilidade e da integridade das informações.

4. Aos ativos de informação são aplicados requisitos de classificação, de acordo com regras institucionalizadas definidas com base nos aspectos legais e necessidades do negócio.

5. Todo o acesso às informações e a utilização dos recursos corporativos poderão ser monitorados, não sendo permitido ao usuário o uso desses recursos para atividades que não estejam relacionadas ao exercício das suas funções.

6. Qualquer acesso à informação da entidade será previamente autorizado pela área competente, levando em conta estritamente as atividades desenvolvidas pelo usuário dentro da entidade. Quando por meio de sistema, o acesso somente será permitido a usuários devidamente autenticados.

6.1 De conformidade com o art. 13 e parágrafo único da Lei Complementar 130/2009, mediante assinatura de *Termo de Responsabilidade e Confidencialidade no*

Tratamento de Dados, será concedido às entidades integrantes do Sicoob, responsáveis pela gestão centralizada de processos sistêmicos em âmbito nacional ou regional, acesso, através 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.

7. A gestão de acessos tem por objetivo estabelecer critérios para acesso aos sistemas eletrônicos utilizados pelo Sicoob Confederação e pelas demais entidades do Sicoob.

8. É de responsabilidade do diretor de controle da entidade, ou de cargo equivalente quando não houver previsão estatutária, designar formalmente os responsáveis pela gestão de acesso, bem como monitorar e assegurar que as melhores práticas relativas à gestão de acessos sejam adotadas e praticadas.

9. As rotinas relacionadas à gestão de acesso aos sistemas corporativos do Sicoob deverão, de preferência, ser realizadas pelo Sicoob Confederação, adotando matriz única de acessos, ou pelas cooperativas centrais do Sicoob, observando as melhores práticas.

10. A matriz, grupos e permissões de acesso deverão respeitar a hierarquia de atividades, cargos ou funções, evitando que ocorra acessos conflitantes e cumulativos, bem como mitigar a possibilidade de eventuais riscos operacionais, financeiros e de fraudes.

11. Para acessar os aplicativos corporativos disponibilizados pelo Sicoob Confederação, 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 entidade e pessoa responsável.

12. 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 pelas entidades.

13. As revisões de acesso devem, no mínimo, ser realizadas anualmente, a fim de garantir a inativação de usuários indevidos, a revisão das permissões concedidas, a existência de perfis de acesso com privilégio maior do que o necessário para execução das atividades.

14. Nos casos em que a gestão de acesso for realizada pelo Sicoob Confederação, esta não será responsável por ações resultantes das solicitações de acessos requeridas e autorizadas pelas cooperativas.

15. É prerrogativa do Sicoob Confederação apontar os acessos conflitantes e cumulativos, que podem incorrer em riscos, e solicitar novas autorizações para concessão de acessos.

16. Cabe à entidade definir as regras para a guarda e preservação das informações conforme o nível de classificação, sendo de responsabilidade do proprietário da informação armazená-la respeitando as regras institucionalizadas para cópias de segurança (becape).

17. Todos os dados e informações das entidades, sob guarda do Sicoob Confederação e, acessados pelos serviços de tecnologia, serão armazenados conforme as regras da Confederação.

18. As informações produzidas no ambiente da entidade, por meio dos recursos próprios ou de serviço contratado, são de propriedade da entidade e somente poderão ser copiadas, divulgadas, publicadas, com autorização da área responsável pela informação.

19. Informações confidenciais não serão discutidas em locais públicos ou de circulação de pessoas não ligadas à entidade.

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

21. Todos os *softwares* utilizados pelas entidades são licenciados. Não são instalados, conectados e utilizados *softwares* não autorizados pela área responsável, independente da natureza de uso ou aplicação. As entidades e os usuários respeitam o direito à propriedade intelectual, na forma da legislação em vigor, não reproduzindo ou divulgando material sem a autorização do autor.

22. Para os contratos firmados com terceiros, as entidades incluem cláusulas de confidencialidade, de acordo de nível de serviço e em cumprimento a todas as regras definidas nesta Política e nos documentos a ela subordinados.

23. É vedada a instalação, conexão ou utilização de quaisquer dispositivos de armazenamento e conectividade (*modem* 3G, *HD* externo, *pendrive etc.*), salvo os de propriedade da entidade ou autorizados pela área responsável, em equipamentos:

    a) pertencentes ao Sicoob: em ambiente interno e externo à entidade;

    b) de terceiros que são utilizados para o trabalho no Sicoob: em ambiente interno à entidade.

24. As entidades aplicam penalidades nos casos de infrações às regras desta Política e dos documentos a ela subordinados, de acordo com o grau de impacto da infração.

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

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