SICOOB

Manual de Instruções Gerais
MIG- Classificação da Informação

Título 1 – Apresentação 3
Título 2 – Classificação da Informação 4
Capítulo 1 – Responsabilidades 4
Capítulo 2 – Diretrizes 5
Capítulo 3 – Execução 6
Capítulo 4 – Rótulos 7
Capítulo 5 – Autorizações e Restrições de Acesso 8
Capítulo 6 – Armazenamento e Descarte Seguro 9
Título 3 – Controle de Atualizações 10

Título 1 – Apresentação

1. Este Manual de Instruções Gerais (MIG) – Classificação da Informação tem por finalidade estabelecer diretrizes para classificação da informação, de forma que a informação receba um nível adequado de proteção, de acordo com sua importância.

2. Este manual aplica-se e deve ser divulgado apenas aos empregados e dirigentes das entidades que fazem parte do Sicoob, incluindo Bancoob empresas controladas e fundação patrocinada, além dos prestadores de serviços com quem o Sicoob mantém contrato e que processam ou armazenam informações do Sicoob.

3. Este manual é atualizado como proposta da estrutura centralizada de gestão da segurança cibernética.

4. No corpo deste manual, apresentamos o Conselho de Administração como órgão de administração. Caso as cooperativas centrais e singulares não disponham dessa estrutura, as funções do Conselho de Administração corresponderão, conforme o caso, à Diretoria Executiva.

5. Em caso de conflito e/ou divergências entre as disposições estabelecidas neste manual e as estabelecidas pelos órgãos reguladores, prevalecerão as últimas.

Título 2 – Classificação da Informação
Capítulo 1 – Responsabilidades

1. *Área de segurança da informação do Sicoob Confederação:*

   a) monitorar o atendimento das diretrizes fixadas neste manual.

2. *Proprietário da informação:*

   a) atribuir o nível de classificação das informações sob sua responsabilidade;

   b) delegar, caso necessário, ao custodiante da informação (usuários, grupos de trabalho ou áreas) a manutenção e guarda da informação no dia a dia;

   c) zelar para que as informações originadas em sua área passem pelo processo de avaliação e classificação;

   d) revisar/reclassificar as informações sob sua responsabilidade, no mínimo anualmente;

   e) apresentar sugestões de atualização deste manual;

   f) zelar pela qualidade dos controles de acesso adotados, voltados à proteção dos dados e das informações, inclusive na contratação de empresas prestadoras de serviço e terceiros que manuseiam dados ou informações sensíveis ou que sejam relevantes para a instituição, considerando a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

3. *Custodiante da informação:*

   a) cuidar da manutenção e guarda da informação delegada pelo proprietário da informação, conforme sua classificação.

4. *Todas as entidades do Sicoob*:

   a) observar as diretrizes fixadas neste manual e adotar os procedimentos necessários para adequado tratamento das informações.

5. *Empresas prestadoras de serviço e terceiros que manuseiam dados ou informações sensíveis do Sicoob*:

   a) observar as diretrizes fixadas neste manual e adotar os procedimentos necessários para adequado tratamento das informações;

   b) manter, enquanto o contrato estiver vigente, a segregação dos dados e dos controles de acesso para proteção das informações do Sicoob;

   c) ao final do contrato de prestação de serviço, eliminar as informações do Sicoob sob sua guarda, salvo aquelas que devem ser mantidas por exigência legal ou contratual.

Título 2 – Classificação da Informação
Capítulo 2 – Diretrizes

1. As informações de propriedade ou sob custódia do Sicoob, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de 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.

2. As informações devem ser classificadas adequadamente, a fim de evitar classificação superestimada (que pode levar à implementação de controles desnecessários, resultando em despesas adicionais) ou classificação subestimada (colocando em perigo o alcance dos objetivos do negócio).

3. Os acessos aos recursos e às informações sob responsabilidade do Sicoob são monitorados e controlados de acordo com a classificação da informação, disposta neste manual.

4. A informação deve receber tratamento adequado à sua classificação durante todo o seu ciclo de vida: criação, manutenção, armazenamento, transporte e descarte.

5. A informação deve ser classificada de modo que empregados e outros colaboradores do Sicoob sejam capazes de entendê-la e saber como lidar com as restrições de acesso e divulgação associadas.

6. A inexistência de classificação explícita não exime o proprietário da informação, o custodiante e os usuários das suas responsabilidades quanto à avaliação e tratamento conforme o nível de sensibilidade da informação.

7. Quando existirem informações classificadas de formas diferentes em um mesmo meio, adota-se a classificação mais restritiva para fins de segurança.

8. Todo programa aplicativo ou equipamento tecnológico é classificado de acordo com o nível da informação que manuseia, refletindo a classificação da informação mais sensível.

9. Sempre que forem efetuadas alterações significativas, que mudem o nível de sensibilidade ou de criticidade, conforme legislação em vigor, em um sistema informatizado, ou nas características de uma informação, a classificação deve ser revista.

10. Devem ser adotados controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis.

Título 2 – Classificação da Informação
Capítulo 3 – Execução

1. Os documentos sob responsabilidade do Sicoob recebem do proprietário da informação o nível de classificação de acordo com o conteúdo, conforme descrição a seguir:

   a) **#CONFIDENCIAL#**: Informações CONFIDENCIAIS ou de caráter sigiloso, cuja revelação não autorizada pode causar danos graves ao Sicoob (impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais) ou cuja confidencialidade é determinada por lei. É sempre restrita a um grupo específico de pessoas;

   b) **#INTERNA#**: Informações INTERNAS ou de caráter reservado cuja revelação não autorizada pode comprometer operações internas da entidade. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem ou com restrições, conforme interesse do proprietário da informação e/ou atuação/necessidade de negócio das áreas internas da entidade;

   c) **#RESTRITA#**: Informações RESTRITAS ou de caráter reservado relacionadas a assuntos de interesse exclusivo de mais de uma entidade do Sicoob, projetos ou grupos de trabalho;

   d) **#PÚBLICA#**: Informações PÚBLICAS ou de caráter informativo, comercial e/ou promocional, cuja linguagem e formato são dedicados à divulgação ao público em geral. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija sua publicidade.

2. A classificação deve ser realizada com base na avaliação individual da informação e sua importância ao negócio, além das consequências de divulgação e acessos não autorizados. Quanto mais estratégica e decisiva para a manutenção dos serviços oferecidos/prestados pelo Sicoob, maior será a importância da informação.

3. Recomenda-se que os ativos com informações possuam rótulos físicos e/ou eletrônicos de acordo com sua classificação, cabendo ao proprietário da informação providenciar tal rotulagem, conforme o capítulo 4 deste manual.

4. O proprietário da informação, ao classificá-la como confidencial, deve indicar o grupo de pessoas ou áreas com permissão para acessá-la.

Título 2 – Classificação da Informação
Capítulo 4 – Rótulos

1. A rotulação dos níveis de classificação das informações deve ser exibida de forma explícita em mensagens eletrônicas, documentos eletrônicos e físicos, bem como mídias eletrônicas e outros invólucros.

2. Informação que não esteja rotulada deve ser considerada como de classificação *Interna*.

Título 2 – Classificação da Informação
Capítulo 5 – Autorizações e Restrições de Acesso

1. O acesso às informações confidenciais e internas deve ser determinado pelo proprietário da informação, que estabelecerá as áreas ou pessoas e o nível desse acesso, conforme descrição a seguir:

   a) Somente Leitura: nível de acesso do usuário que permite somente a leitura das informações;

   b) Leitura e Alteração: nível de acesso do usuário que permite efetuar mudanças nas informações.

2. As informações públicas não estão sujeitas ao controle de acesso.

Título 2 – Classificação da Informação
Capítulo 6 – Armazenamento e Descarte Seguro

1. Informações sensíveis mantidas em documentos em papel, fitas magnéticas, gravação de voz, relatórios etc. devem ser descartadas de forma segura e protegida, por meio de incineração, trituração ou eliminação dos dados. No caso de mídia magnética, deve ser fisicamente apagada de modo que dificulte, ao máximo, a restauração de dados, antes que a mídia seja descartada ou reutilizada. Na impossibilidade de serem removidos os dados, a mídia deve ser destruída.

2. Após atendimento de prazos legais, considerando que a informação deve estar disponível para cumprimento de ordem judicial, e dos prazos definidos pelas necessidades do negócio, o descarte deve ocorrer conforme a seguir:

   a) Informações confidenciais:

   a.1) Armazenamento: acessos controlados, com concessão formal, com o envolvimento do proprietário da informação;

   a.2) Descarte: não devem ser descartadas como lixo comum. A informação deve ser destruída por completo antes do descarte, de forma que torne impossível a sua recuperação.

   b) Informações internas e restritas:

   b.1) Armazenamento: armazenadas considerando o menor investimento para manter o nível necessário de segurança;

   b.2) Descarte: convém que documentos físicos sejam fragmentados e que mídias eletrônicas sejam formatadas.

   c) Informações públicas:

   c.1) Armazenamento: armazenadas considerando o menor investimento necessário para garantir a disponibilidade necessária;

   c.2) Descarte: não requer procedimentos formais.

Título 3 – Controle de Atualizações

Data	Instrumento de comunicação