Manual de Classificação da Informação

SICOOB

Índice

Dicas de navegação:

Os ***links*** são identificados na cor turquesa ao longo do texto.
Pressione ctrl + F para pesquisar um termo específico no documento.
Clique no ícone no rodapé da página para retornar ao índice.

Caso esteja usando o Acrobat:

Pressione alt + ← para retornar à última página visitada (após utilizar um *link*).

Clique no ícone na barra direita, para navegar pelo índice.

Título 1. **Apresentação**

1 Este Manual:

a) estabelece as diretrizes para a classificação da informação, de forma que exista um nível adequado de proteção, considerando sua importância e relevância para o Sicoob, e fornece instruções para o armazenamento e o descarte (expurgo/eliminação/exclusão) da informação, com base na classificação aplicada;

b) para fins deste Manual, são *entidades do Sicoob* as cooperativas singulares, as cooperativas centrais e o Centro Cooperativo Sicoob (CCS);

c) tem como público-alvo as entidades do Sicoob;

d) regulamenta instruções e regras em conformidade com a **Política Institucional de Segurança da Informação**, e está categorizado no tema Gestão de Riscos e Controles;

e) foi elaborado e é atualizado por proposta da Superintendência de Controles, por meio da Área de Privacidade de Dados;

f) é aprovado pela Diretoria Executiva do CCS – Sicoob Confederação;

g) somente pode ser reproduzido, parcial ou totalmente, pelas entidades do Sicoob, desde que em ambiente seguro e de acesso restrito aos seus empregados e dirigentes.

Título 2. **Responsabilidades**

1 Área de Privacidade de Dados do CCS:

a) fixar as regras e instruções dispostas neste Manual, e auxiliar as entidades na resolução de dúvidas sobre o tema.

2 Proprietário da informação:

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

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

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

d) zelar pela qualidade dos controles de acesso adotados, voltados para a proteção dos dados e das informações, inclusive na contratação de empresas prestadoras de serviço e terceiros que manuseiam dados ou informações sensíveis ou relevantes para a entidade, considerando a sensibilidade dos dados e das informações a serem processadas, armazenadas e gerenciadas pelo contratado.

3 Custodiante da informação:

a) zelar pela manutenção e guarda da informação delegada pelo proprietário da informação, conforme sua classificação;

b) analisar e classificar informações que estejam sem nível de classificação atribuído;

c) reclassificar as informações que tiveram seus níveis de proteção alterados devido às mudanças no contexto.

4 Entidades do Sicoob:

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

b) orientar e conscientizar os usuários periodicamente sobre as diretrizes de classificação da informação no Sicoob.

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

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

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

c) no fim 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 3. **Regras**

1 As informações de propriedade ou sob a custódia do Sicoob, mantidas em meio eletrônico ou físico, devem ser classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, sempre que possível, 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 subestimada (colocando em perigo o alcance dos objetivos do negócio e/ou gerando aumento de riscos).

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, coleta, manutenção, armazenamento, transporte, descarte etc.

5 A informação deve ser classificada da forma em que todos os usuários do Sicoob entendam e saibam como lidar com as restrições de acesso e divulgação associadas.

6 A informação que não estiver rotulada deve ser considerada como de classificação Interna.

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

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

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

10 A classificação deve ser revista sempre que forem efetuadas alterações significativas, que mudem o nível de sensibilidade ou de criticidade, conforme a legislação em vigor, em sistemas informatizados ou processos manuais, ou nas características de uma informação.

11 Controles específicos devem ser adotados, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis.

12 As regras de classificação da informação no Sicoob, definidas neste Manual, não se confundem com a classificação de dados do Microsoft 365, embora as entidades devam empenhar os esforços necessários para que haja a maior similaridade possível entre elas.

Título 4. **Rótulos**

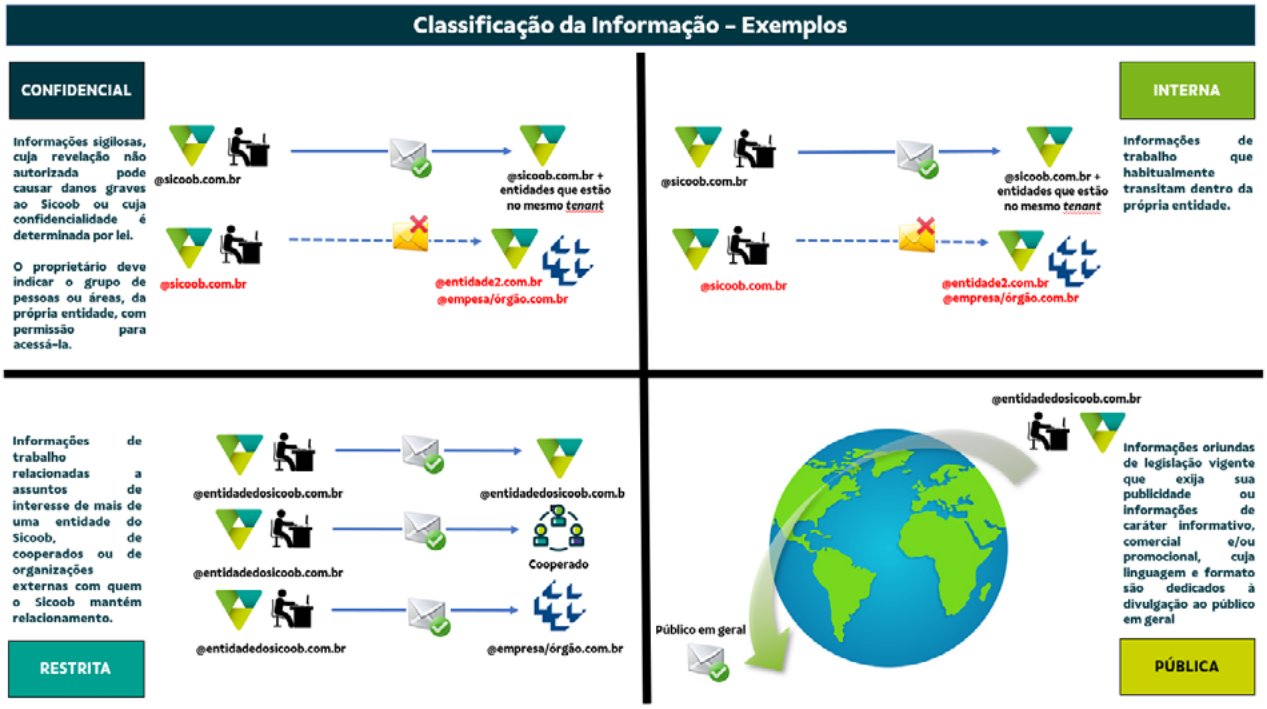
1 A classificação da informação deve ser definida com base na sua avaliação individual e na importância para o negócio, além das consequências de divulgação e acessos não autorizados. Quanto mais estratégica e decisiva para a manutenção dos serviços oferecidos e prestados pelo Sicoob for a informação,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

2 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.

3 As informações sob responsabilidade do Sicoob recebem, do proprietário da informação, nível de classificação de acordo com o conteúdo, conforme as descrições a seguir:

Informações com rótulo	Descrição
#CONFIDENCIAL#	Informações de trabalho com caráter sigiloso, cuja revelação não autorizada pode causar danos graves ao Sicoob (impactos de ordem financeira, de imagem, operacional ou sanções administrativas, civis ou criminais) ou cuja confidencialidade é determinada por lei. É sempre restrita a um grupo específico de pessoas dentro da própria entidade. O proprietário da informação, ao classificá-la com esse rótulo, deve indicar o grupo de pessoas ou áreas com permissão para acessá-la.
#INTERNA#	Informações de trabalho que habitualmente transitam dentro da própria entidade. Caso sejam acessadas indevidamente, podem causar danos à imagem, porém, não com a mesma magnitude de uma informação confidencial.
#RESTRITA#	Informações de trabalho relacionadas a assuntos de interesse de mais de uma entidade do Sicoob, de cooperados ou de organizações externas com quem o Sicoob mantém relacionamento.
#PÚBLICA#	Informações oriundas de legislação vigente que exige sua publicidade ou informações de caráter informativo, comercial e/ou promocional, com linguagem e formato dedicados à divulgação ao público em geral.

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



Título 5. **Acessos**

1 Autorizações e Restrições de Acesso.

1.1 O acesso às informações confidenciais, internas e restritas é determinado pelo proprietário da informação, que estabelece as áreas ou pessoas e o nível de acesso, conforme descrito a seguir:

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

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

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

2 Acesso de Usuários Externos.

2.1 Para ler *e-mails* e acessar arquivos com classificação *Restrita* realizada no Office365, os usuários externos devem observar os seguintes requisitos:

a) usuários do Sicoob que usam *domínios* diferentes do @sicoob.com.br devem baixar o visualizador da proteção de informações do Azure. Esse visualizador pode abrir arquivos protegidos de texto, imagens, PDF e arquivos que possuam extensão de nome.*pfile*;

b) o visualizador pode ser baixado por meio do seguinte *link*: **https://portal.azurerms.com/#/download**. Detalhes técnicos podem ser obtidos no *site* do fabricante: **https://docs.microsoft.com/pt-br/azure/information-protection/requirements**.

2.2 Usuários de domínios públicos devem seguir as recomendações dispostas no seguinte *link*: **https://support.microsoft.com/pt-br/office/como-abrir-uma-mensagem-protegida-1157a286-8ecc-4b1e-ac43-2a608fbf3098**

Título 6. Armazenamento

1 O armazenamento de informações é o processo de reter dados ou informações em meio físico ou digital.

2 É importante observar as boas práticas de armazenamento de informações para garantir a segurança e eficiência, além de proteger os ativos contra acessos não autorizados, perdas, roubos ou outros tipos de danos.

3 Armazenamento por classificação:

Informações com rótulo	Devem ser armazenadas
#CONFIDENCIAL#	Em áreas com acesso físico controlado; em locais com restrição de acesso (armários, gavetas com chaves ou salas seguras); em servidores de arquivos com controle de acesso e, se disponível, com o uso de criptografia, sempre envolvendo o proprietário da informação.
#INTERNA#	Nas entidades do Sicoob, em locais não acessíveis por pessoas externas à entidade; em servidores de arquivos, nuvem ou prestadores de serviços, desde que o contrato contenha orientações e tratamento adequados, considerando o menor investimento para manter o nível necessário de segurança.
#RESTRITA#	Pelo destinatário autorizado da informação nas entidades do Sicoob; em servidores de arquivos, nuvem ou prestadores de serviços, desde que o contrato contenha orientações e tratamento adequados, considerando o menor investimento para manter o nível necessário de segurança.
#PÚBLICA#	Sem restrição, considerando o menor investimento necessário para garantir a disponibilidade necessária.

Título 7. Descarte/Expurgo/Eliminação/Exclusão

1 O descarte, o expurgo, a eliminação, a exclusão – e os seus sinônimos – são ações que inviabilizam definitivamente o acesso às informações.

2 O descarte pode ser aplicado tanto às informações físicas, como documentos impressos ou objetos, quanto às informações digitais, como arquivos de computador ou dados armazenados em nuvem.

3 O descarte adequado e devido é importante para proteger a privacidade e a segurança das informações, bem como para cumprir as regulamentações governamentais e legais.

4 Devem ser adotadas técnicas e tecnologias apropriadas para garantir que as informações sejam destruídas de forma segura e permanente, pois o descarte inadequado pode incidir em riscos de segurança, como roubo de identidade ou violação de privacidade.

5 O processo de descarte de informações e documentos deve observar os seguintes normativos internos:

a) **Manual de Arquivamento e Guarda de documentos do Sicoob**;

b) *Tabela de Temporalidade de Dados Pessoais*, anexa ao **Manual de Privacidade e Proteção de Dados Pessoais do Sicoob**.

6 O descarte de informações e documentos deve ser realizado quando forem observados os seguintes critérios:

a) cumprimento dos prazos legais e regulatórios de retenção, conforme determinado pelo respectivo órgão regulador/fiscalizador, como o Banco Central do Brasil (BCB), a Receita Federal do Brasil (RFB), a Comissão de Valores Mobiliários (CVM), e demais autoridades competentes;

b) atendimento às necessidades operacionais de retenção documental, conforme definido pelas áreas de negócio relacionadas, incluindo exigências relacionadas à prevenção à lavagem de dinheiro, auditorias internas e externas, análises históricas e requisitos de governança corporativa;

c) ausência de impedimentos legais, regulatórios ou contratuais que exijam a preservação da informação, tais como: ordens judiciais, investigações em curso ou cláusulas contratuais.

7 Após atender os critérios supramencionados, o descarte deve ocorrer conforme a seguir:

Informações com rótulo	Como devem ser descartadas
#CONFIDENCIAL#	Não devem ser descartadas como lixo comum. A informação deve ser destruída por completo antes do descarte, de forma que a recuperação física ou lógica seja impossível. Exemplos: as 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 violação dos mecanismos que possibilitam o acesso aos 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. Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança. Na impossibilidade de remover os dados, a mídia deve ser completamente destruída.
#INTERNA#	Utilizar métodos de exclusão de dados que sobrescrevem as informações. Ferramentas de exclusão de dados são recomendadas.
#RESTRITA#	Para mídias físicas, a destruição menos rigorosa pode ser apropriada, dependendo do nível de sensibilidade.
#PÚBLICA#	De forma simples, sem o uso de recursos e procedimentos específicos para descarte.

Título 8. **Glossário**

1 Armazenamento: processo de guardar dados e informações em um meio físico ou digital, de forma que possam ser acessados e utilizados posteriormente.

2 Ativo: qualquer recurso valioso para uma organização, podendo ser tangível (como equipamentos e instalações) ou intangível (como dados, informações e propriedade intelectual).

3 Classificação da informação: atribuição de nível de sensibilidade à informação.

4 Confidencialidade, Integridade e Disponibilidade: princípios da segurança da informação:

a) confidencialidade: garantir que a informação seja acessível apenas por pessoas autorizadas;

b) integridade: assegurar que a informação não seja alterada ou destruída de maneira não autorizada;

c) disponibilidade: garantir que a informação esteja acessível e utilizável quando for necessário.

5 Criptografia: técnica de proteger informações, transformando-as em um formato ilegível para aqueles que não têm a chave de decodificação, garantindo a confidencialidade e a integridade dos dados durante a transmissão e o armazenamento.

6 Custodiante da informação: usuário que recebe a informação criada ou coletada pelo proprietário.

7 Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

8 Dado sensível: dado sobre origem racial, convicções religiosas, saúde, vida sexual etc.

9 Descarte/Expurgo/Eliminação/Exclusão: processo de remover dados ou informações de um sistema ou meio de armazenamento, garantindo que não possam ser recuperados ou reutilizados.

10 Informação: dados organizados e processados de maneira a terem significado e relevância. Pode ser textual, visual, sonora, entre outros formatos.

11 Informações sensíveis: dados que, se divulgados, acessados ou manipulados indevidamente, podem causar danos ou prejuízos a indivíduos ou organizações. Exemplos: dados pessoais, informações financeiras e segredos comerciais.

12 Invólucros: estruturas físicas ou digitais que protegem dados e dispositivos, podendo ser estojos físicos, encapsulamentos eletrônicos ou mecanismos de proteção de dados em sistemas digitais.

13 Nuvem: modelo de computação que permite o acesso remoto a recursos de armazenamento e processamento de dados por meio da internet. Provedores de serviços em nuvem oferecem infraestrutura, plataformas e *software* como serviços, escaláveis conforme a demanda.

14 Proprietário da informação: usuário responsável pela coleta ou criação da informação.

15 *Tenant* ou locatário, no contexto do Microsoft 365 e Azure: instância de serviços da Microsoft atribuída a uma organização. Ela funciona como um contêiner lógico onde a empresa gerencia usuários, configurações e recursos de TI dentro dos serviços da Microsoft.

16 Usuário externos:

a) usuários do Sicoob que usam domínios diferentes do @sicoob.com.br (usam outro *Tenant*);

b) usuários de domínios públicos: usuários que usam provadores como Gmail, Hotmail, Yahoo etc.

Título 9.

Referências normativas

Nomes	*Link* CCS	*Link* Cooperativas
Política Institucional de Segurança da Informação	ACESSE	ACESSE
Manual de Arquivamento e Guarda de documentos do Sicoob	ACESSE	ACESSE
Manual de Privacidade e Proteção de Dados Pessoais do Sicoob	ACESSE	ACESSE

Nomes	*Links* externos
Lei nº 13.709, de 14/8/2018. Lei Geral de Proteção de Dados Pessoais (LGPD)	ACESSE

Chegou por meio de um *link*?
Clique aqui para retornar à última página visitada.

Título 10. Controle de atualizações

Nomes	*Link* CCS	*Link* Cooperativas
7/10/2025 **Circular CCS 1.537**	ACESSE	ACESSE