Guia Prático:

INFORMAÇÃO CLASSIFICADA

Tratamento de Informação Classificada e Segurança Jurídica no âmbito do ICMBio

Ouvidoria ICMBio - MMA

ICMBio Instituto Chico Mendes MMA

MINISTÉRIO DO MEIO AMBIENTE E MUDANÇA DO CLIMA

Ouvidoria do Instituto Chico Mendes de Conservação da Biodiversidade - ICMBio

EQSW 103/104, COMPLEXO ADMINISTRATIVO BLOCO C, 2º andar - SETOR SUDOESTE BRASÍLIA/DF - CEP 70670-350

Presidente da República
Luiz Inácio Lula da Silva

Ministro de Estado do Meio Ambiente e Mudança do Clima – MMA
João Paulo Capobianco

Presidente do Instituto Chico Mendes de Conservação da Biodiversidade – ICMBio
Mauro Oliveira Pires

Chefe de Gabinete
Thais Ferraresi Pereira

Ouvidora
Vanessa Simas Figueiredo

Organização do Material
Freida Augusta da Costa Freitas
Vanessa Simas Figueiredo

Projeto Gráfico
Isac Luiz de Sousa Pimentel

Equipe da Ouvidoria

Alessandra Guedes
Caroline Viana
Felipe Nascimento
Freida Freitas
Isac Luiz Pimentel
Rafael Chagas
Regina Mendes

SUMÁRIO

Clique nos títulos para ir direto para a seção desejada!

SUMÁRIO

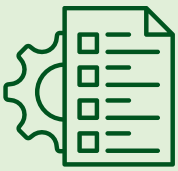
Clique nos títulos para ir direto para a seção desejada!

INTRODUÇÃO

A classificação de informações na Administração Pública Federal é um processo fundamental para equilibrar a transparência e a segurança do Estado. Este tema é regulamentado primariamente pela Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), que estabelece os procedimentos de acesso e os critérios para a restrição de informações cruciais à segurança da sociedade e do Estado. Complementarmente, o Decreto nº 7.845/2012 detalha o credenciamento de segurança e o tratamento de informações sigilosas, definindo as responsabilidades dos órgãos públicos na sua proteção e salvaguarda. Além desses, normativos como a Resolução CMRI Nº 7/2024 e a Instrução Normativa CGU nº 33/2024 fornecem diretrizes específicas para a gestão, classificação, desclassificação e proteção dessas informações.

Este Guia Prático foi desenvolvido especificamente para o ICMBio com o intuito de oferecer orientações introdutórias, claras e objetivas sobre a gestão de informações classificadas. Como material complementar para consulta e maior profundidade técnica, recomenda-se o "Guia sobre Informações Classificadas e Desclassificadas no Âmbito do Poder Executivo Federal", que atua como um recurso para a compreensão e aplicação das normas vigentes. Para detalhes adicionais e acesso ao glossário de termos, o documento completo pode ser consultado no portal oficial através do link: https://www.gov.br/acessoainformacao/pt-br/lai-para-sic/transparencia-passiva/guias-e-orientacoes/guia-inf-clalssificadas-4.pdf.

OBJETIVOS DO GUIA PRÁTICO

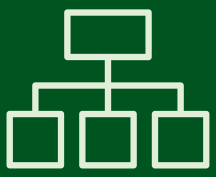


PADRONIZAÇÃO

Orientar o tratamento de informações de forma clara, detalhada e uniforme em todo o ICMBio.

SEGURANÇA JURÍDICA

Promover a conformidade com a LAI, evitando riscos administrativos e o uso indevido do sigilo.



FLUXOS E TRANSPARÊNCIA

Esclarecer competências, procedimentos de acesso e o fortalecimento da transparência pública.

A DIRETRIZ FUNDAMENTAL DA LAI

A publicidade é a regra

- Toda informação produzida nasce pública.
- Livre acesso é o padrão institucional.
- Transparência ativa e passiva.

O sigilo é a exceção

- Apenas situações excepcionais.
- Fundamento legal expresso.
- Tempo estritamente necessário.

CONCEITO JURÍDICO E LIMITES

O que é Informação Classificada?

"Informação cujo acesso público é temporariamente restringido porque sua divulgação **pode causar risco relevante à segurança da sociedade ou do Estado.**"

O Ponto Central é:

- Risco efetivo à segurança estatal.
- Dano real e demonstrável.
- Imprescindibilidade do sigilo.

O Ponto Central NÃO é:

- Desconforto institucional ou crítica pública.
- Proteção da imagem do órgão ou repercussão negativa.
- Ocultar erros administrativos ou falhas operacionais.

Lembre-se!

Toda informação classificada é sigilosa, mas nem toda informação sigilosa é classificada.

MAPA DAS CATEGORIAS DE INFORMAÇÃO

Informação Pública

DISPONÍVEL
O acesso é garantido a todos os cidadãos.

Transparência ativa e passiva

SIGILOSA
Restrição temporária ao acesso público.

LAI

Não classificada

- Informações pessoais (Art. 31)
- Casos legais específicos (Art. 22)
- Documentos preparatórios (Art. 7°, § 3°)

Foco do guia

LAI Art. 23 e 24

Classificada

- **Reservada:** Até 5 anos
- **Secreta:** Até 15 anos
- **Ultrassecreta:** Até 25 anos

DISTINÇÃO ESSENCIAL DE CONCEITOS

INFORMAÇÃO DISPONÍVEL

Regra:
Livre acesso a qualquer cidadão (LAI,art. 7º)

Exemplo ICMBio
Contratos, licitações e relatórios administrativos.

INFORMAÇÃO SIGILOSA

INFORMAÇÃO PESSOAL

Regra:
Proteção da intimidade e Privacidade (LAI, art. 31)

Exemplo ICMBio
Dados médicos de servidores, CPF e endereço residencial

INFORMAÇÃO CLASSIFICADA

Regra:
Restrição temporária por Segurança (LAI, art. 23 e 24)

Exemplo ICMBio
Planejamento sigiloso de operação contra garimpo ilegal.

DOCUMENTO PREPARATÓRIO

Regra:
Documento utilizado na elaboração de decisões administrativas, cujo acesso pode ser temporariamente restrito até a conclusão da decisão, tornando-se público posterior-mente, salvo previsão legal de sigilo (LAI, art. 7°, §3°)

Exemplo ICMBio
Minutas de notas técnicas, pareceres, relatórios preliminares, estudos internos e versões em elaboração de atos normativos ainda não publicados.

CASOS LEGAIS ESPECÍFICCOS

Regra:
Informações protegidas por legislação específica aplicável ao poder público . As disposições da lei de acesso à informação não afastam outras hipóteses legais de sigilo (LAI,art.22)

Exemplo ICMBio
Segredo de justiça, sigilo industrial e sigilo bancário

EXEMPLOS DE INFORMAÇÃO DISPONÍVEL NO ICMBIO

Informações que devem permanecer acessíveis por padrão:

- Contratos e Licitações
- Notas Técnicas e Pareceres
- Processos de Licenciamento
- Dados Orçamentários e Estatísticos
- Autos de Infração já Públicos
- Despesas, Diárias e Passagens
- Planos de Manejo Publicados
- Convênios e Acordos
- Atas de Reunião e Estudos Técnicos

Estas informações nascem públicas e o acesso só pode ser restrito em hipóteses legais específicas.

PROTEÇÃO DE INFORMAÇÃO PESSOAL


Foto: Artush

Regras de Proteção

Proteção Automática
Independe de classificação. A proteção é garantida pela Constituição, LAI e LGPD.

Privacidade e Intimidade
Dados relacionados à vida privada, à honra e à imagem das pessoas, bem como dados pessoais sensíveis protegidos pela legislação aplicável.

Atenção
Dados pessoais NÃO recebem grau de sigilo (Reservado/Secreto/ Ultrassecreto).

Exemplos no ICMBio

- Dados Bancários
- Dados Psicológicos
- Telefone Pessoal
- Exames Médicos
- CPF e RG
- Informações Familiares
- Dados Biométricos
- Endereço Residencial

A presença de dados pessoais não justifica o sigilo integral do documento. Conforme a LGPD e a LAI, basta anonimizar as informações sensíveis para garantir o acesso público ao restante do conteúdo.

CRITÉRIOS PARA CLASSIFICAÇÃO DA INFORMAÇÃO (LAI, art 23- rol taxativo)

Soberania Nacional

Pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional.

Exemplo: estratégias militares de proteção de fronteiras em terras indígenas ou unidades de conservação de fronteira, em operações integradas com Forças Armadas.

Relações Internacionais

Prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais.

Exemplo: acordos de cooperação internacional em fase de negociação; documentos trocados com organismos estrangeiros sob cláusula expressa de confidencialidade.

Vida e Saúde

Pôr em risco a vida, a segurança ou a saúde da população

Exemplo: vulnerabilidades em infraestruturas críticas de unidades de conservação; dados que possam expor comunidades em situação de conflito socioambiental a risco direto.

Risco à Ordem Econômica e Monetária

Oferecer elevado risco à estabilidade financeira, econômica ou monetária do País

Exemplo: dados estratégicos sobre recursos naturais que, se divulgados prematuramente, possam gerar impacto sistêmico em mercados de commodities ou em decisões de política ambiental de repercussão econômica nacional.

Imagem do País no exterior

Informações que possam causar dano à imagem do País no exterior.

Exemplo: dados ambientais estratégicos que, em contexto de negociação internacional, possam fragilizar a posição do Brasil em fóruns multilaterais de meio ambiente - desde que o risco seja real, concreto e demonstrável, não meramente especulativo.

Estratégias Militares

Prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas

Exemplo: informações produzidas em operações conjuntas com o Exército, Marinha ou Aeronáutica em áreas de fronteira ou de interesse militar, quando classificadas pela autoridade militar competente e custodiadas pelo ICMBio.

Projetos Estratégicos

Prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional

Exemplo: pesquisas sigilosas em parceria com órgãos de defesa nacional; dados tecnológicos sensíveis de sistemas de monitoramento ambiental de interesse estratégico.

Risco à Segurança de Autoridades e Instituições

Pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares.

Exemplo: localização temporária de autoridades sob escolta em operações de campo; informações sobre equipes de segurança em missões de risco.

Inteligência e Fiscalização

Comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações .

Exemplo: planejamento operacional de ações de combate ao garimpo ilegal, ao desmatamento ou ao tráfico de fauna - incluindo rotas, cronogramas, efetivo empregado e estratégias de abordagem - enquanto a operação não se encerrar.

EXEMPLO DE INFORMAÇÕES PASSÍVEIS DE CLASSIFICAÇÃO

Fiscalização em Curso

Planejamento operacional, rotas de deslocamento, cronograma de incursão e efetivo empregado em operações futuras.

RISCO: FRUSTRAR A OPERAÇÃO

Combate ao Garimpo Ilegal

Mapeamento de áreas sensíveis, ações integradas com forças de segurança e inteligência territorial estratégica.

RISCO: EXPOR AGENTES

Espécies Ameaçadas

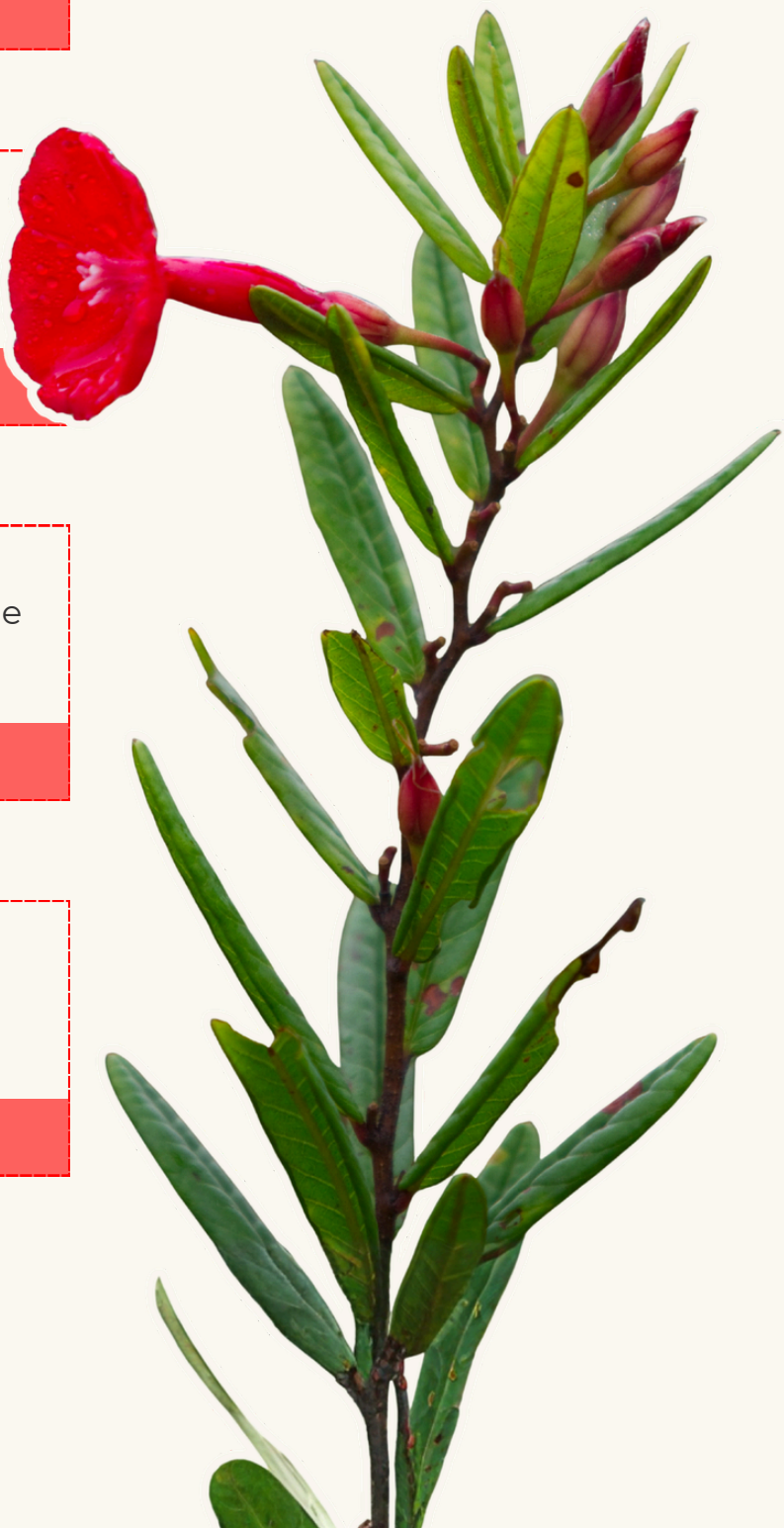
Coordenadas exatas de ninhos, áreas de reprodução e localização de espécies raras ou de alto valor comercial.

RISCO: TRÁFICO E CAÇA

Segurança Institucional

Protocolos internos de segurança, vulnerabilidades de bases e de monitoramento sensíveis.

RISCO: ATAQUES A BASES



SITUAÇÕES QUE NÃO JUSTIFICAM SIGILO

É VEDADA a classificação para:

- Ocultar erro administrativo
- Impedir crítica pública
- Dificultar fiscalização
- Restringir atuação da imprensa
- Evitar desgaste institucional
- Evitar responsabilização
- Esconder falhas operacionais
- Evitar repercussão política

EXEMPLO PRÁTICO DE VEDAÇÃO

Cenário: Um relatório interno aponta falhas graves na fiscalização de uma Unidade de Conservação.

Decisão: Este documento **NÃO pode ser classificado.** O constrangimento institucional ou a possibilidade de críticas não são hipóteses legais para o sigilo.

ANÁLISE PRÉVIA À CLASSIFICAÇÃO

A autoridade deve responder objetivamente antes de decidir classificar a informação:

1. Qual dano concreto poderá ocorrer?

Não basta alegação genérica. Deve existir um risco real, dano demonstrável e relação lógica entre divulgação e prejuízo.

2. O dano afeta a segurança do Estado?

O risco deve estar diretamente relacionado à segurança da sociedade ou do Estado, conforme requisito central da LAI.

3. Existe alternativa menos restritiva?

É possível ocultar apenas um trecho? Fornecer uma versão parcial ou realizar o tarjamento de dados sensíveis?

4. O prazo é realmente necessário?

O sigilo não pode durar indefinidamente. O prazo escolhido deve ser proporcional ao tempo em que o risco persistir.

CLASSIFICAÇÃO DA INFORMAÇÃO QUANTO AO GRAU DE SIGILO NA PRÁTICA

GRAU	PRAZO MÁXIMO	APLICAÇÃO PRÁTICA NO ICMBIO
Reservado Uso comum	Até 5 anos	**Situações sensíveis temporárias.** Exemplo: Planejamento de operação ambiental ainda em andamento ou rotas de fiscalização imediata.
Secreto Excepcional	Até 15 anos	**Risco relevante e mais robusto.** Exemplo: Informações estratégicas integradas com órgãos de inteligência e segurança nacional.
Ultrassecreto Raríssimo	Até 25 anos (prorrogável + 25)	**Hipóteses excepcionalíssimas.** Somente quando houver efetivo risco à soberania ou segurança do Estado em alto nível.

A contagem do prazo inicia na data de produção do documento, não na data de protocolo ou publicação do Termo de Classificação da Informação (TCI)

Após o término do prazo de sigilo ou o encerramento do evento que justificou a restrição de acesso, a informação classificada torna-se automaticamente pública, observadas as demais hipóteses legais de sigilo

ERROS COMUNS NA GESTÃO DO SIGILO

ESCOPO DA CLASSIFICAÇÃO

Errado
Classificar o processo inteiro sem necessidade

Certo
Restringir apenas anexos ou dados sensíveis pontuais.

MOTIVAÇÃO DO ATO

Errado
Justificativa genérica: "Documento sensível"

Certo
Explicar o risco real à operação ou aos agentes.

NATUREZA DO DADO

Errado
Confundir informação pessoal com classificada.

Certo
Tratar dados pessoais via LGPD, sem grau de sigilo.

TEMPORALIDADE

Errado
Manter sigilo indefinidamente.

Certo
Cessar o sigilo assim que o risco desaparecer.

COMPETÊNCIAS PARA CLASSIFICAÇÃO DA INFORMAÇÃO

Autoridade Classificadora

Quem pode mais, pode menos!

Reservada

- ✓ Diretores do ICMBio (autoridades equivalentes a FCE ou CCE 15 ou nível superior)
- ✓ Delegação da autoridade máxima do ICMBio

Secreta

- ✓ Presidente do ICMBio

Ultrassecreta

- ✓ Presidente e Vice Presidente da República
- ✓ Ministro do Meio Ambiente e Mudança do Clima
- ✓ Autoridades com delegação presidencial específica

Lembre-se!

A autoridade classificadora responde pessoalmente pelo ato de classificação.

PROCEDIMENTOS ESSENCIAIS: DA CLASSIFICAÇÃO AO CONTROLE

1 – Credenciamento de Segurança

O ponto de partida obrigatório

Antes de qualquer coisa, pessoas, setores, sistemas e ambientes precisam ser credenciados. Sem isso, ninguém pode produzir, acessar ou guardar informação classificada.

Responsável: GSI/PR, diretamente ou por meio de órgãos autorizados

2 – Termo de Classificação da Informação (TCI)

O documento que torna o sigilo oficial

Toda vez que uma informação for classificada, a autoridade responsável deve preencher o TCI. Nele ficam registrados: o motivo legal da classificação, o grau de sigilo (reservado, secreto ou ultrassecreto) e por quanto tempo a restrição vai durar.

Atenção: Sem o TCI preenchido e assinado, a classificação não tem validade jurídica.

Responsável: Autoridade classificadora legalmente habilitada

3 – Código de Indexação de Documento Classificado

O número que identifica e rastreia o documento

Cada documento classificado recebe um código único - o CIDIC. Esse código permite localizar, controlar e acompanhar o documento em qualquer etapa: produção, tramitação, guarda ou descarte

Responsável: Unidade produtora ou custodiante da informação

PROCEDIMENTOS ESSENCIAIS: DA CLASSIFICAÇÃO AO CONTROLE

4 – Registro no STIC

O cadastro eletrônico obrigatório

Toda informação classificada deve ser registrada no Sistema de Tratamento de Informações Classificadas (STIC), plataforma eletrônica do Governo Federal. O sistema permite acompanhar prazos de sigilo, reavaliações e desclassificações em tempo real.

Atenção: O uso do STIC é exigido para todos os órgãos do Poder Executivo Federal. Registros fora do sistema não atendem à exigência legal.

Responsável: Autoridade classificadora e unidade gestora responsável

5 – Termo de Compromisso de Manutenção de Sigilo

A assinatura antes do acesso

Qualquer pessoa que precise acessar uma informação classificada - servidor, colaborador ou terceiro - deve assinar o TCMS antes de ter acesso. No documento, a pessoa se compromete a proteger a informação e utilizá-la apenas para fins do serviço.

Responsável: Unidade custodiante, com apoio das áreas de segurança institucional e segurança da informação

6 – Posto de controle

O rastreamento de cada movimentação

O posto de controle registra tudo o que acontece com um documento classificado: quem está com ele, quando foi encaminhado, se foi reproduzido, transferido ou eliminado. Garante que nenhuma movimentação passe sem registro.

Responsável: Unidade custodiante da informação classificada

7 – Controle de credenciais e de acesso

Só acessa quem precisa e quem está autorizado

O acesso à informação classificada depende de dois critérios combinados: ter credencial de segurança válida e ter necessidade real de conhecer aquela informação para o exercício de suas funções. Ambos são indispensáveis.

Responsável: Unidade custodiante, gestores da informação e área de segurança da informação

PROCEDIMENTOS ESSENCIAIS: DA CLASSIFICAÇÃO AO CONTROLE

8 – Comissão Permanente de Avaliação

O grupo que orienta as decisões de sigilo

Cada órgão deve ter uma Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS, comissão interna que assessora as autoridades em decisões de classificar, manter o sigilo, reduzir o grau ou desclassificar documentos. É uma instância consultiva - a decisão final cabe à autoridade competente.

Responsável: Comissão instituída por ato normativo da entidade

9 – Reavaliação da classificação

O sigilo precisa ser revisto periodicamente

Informações classificadas não permanecem sigilosas automaticamente para sempre. É obrigatório reavaliar se os motivos que geraram a restrição ainda existem. A reavaliação pode resultar em três caminhos: manter o grau de sigilo, reduzir o grau ou desclassificar.

Responsável: Autoridade classificadora ou instância prevista em regulamento

10 – Recursos administrativos e supervisão

O direito de questionar a classificação

Se um servidor, cidadão ou órgão entender que uma classificação é indevida ou que o acesso foi negado sem justificativa adequada, pode apresentar recurso administrativo. As instâncias superiores revisam a decisão com base na legislação vigente.

Responsável: Autoridades recursais e instâncias de supervisão previstas na legislação

PROCEDIMENTOS ESSENCIAIS: DA CLASSIFICAÇÃO AO CONTROLE

11 – Recursos administrativos e supervisão

O direito de questionar a classificação

Se um servidor, cidadão ou órgão entender que uma classificação é indevida ou que o acesso foi negado sem justificativa adequada, pode apresentar recurso administrativo. As instâncias superiores revisam a decisão com base na legislação vigente.

Responsável: Autoridades recursais e instâncias de supervisão previstas na legislação

12 – Auditoria e fiscalização

O controle permanente de todo o ciclo

Todo o ciclo de vida das informações classificadas - da classificação à desclassificação - está sujeito a auditoria e fiscalização permanente. O objetivo é garantir que os procedimentos estejam sendo seguidos corretamente e em conformidade com a legislação.

Responsável: Auditoria interna, unidades de controle interno e órgãos de controle externo (CGU e TCU, conforme o caso)

FLUXO INSTITUCIONAL PARA CLASSIFICAÇÃO

01 - Identificação

A unidade técnica avalia a natureza da informação, o risco potencial e a hipótese legal de sigilo.

O que verificar:

A informação se enquadra em algum dos incisos do art. 23 da LAI? O risco é real e demonstrável? Existe alternativa menos restritiva, como tarjamento parcial ou fornecimento de extrato?

Atenção:

Se a informação não se enquadrar em nenhum critério legal, o processo deve ser encerrado aqui. Não há margem para interpretação extensiva — o rol do art. 23 é taxativo.

02 - Justificativa

Elaboração de explicação técnica detalhada sobre o risco identificado e o dano concreto que poderá ocorrer se a informação for divulgada.

O que a justificativa deve conter:

Descrição do risco real e demonstrável; nexo causal entre a divulgação e o dano; inciso do art. 23 da LAI aplicável; grau de sigilo proposto e prazo sugerido; análise da possibilidade de acesso parcial.

Atenção:

Justificativa genérica, como "documento sensível" ou "informação estratégica", não atende ao requisito legal. A motivação deve ser específica, objetiva e verificável.

03 - Avaliação

Manifestação formal da chefia imediata, da área jurídica e da área de gestão documental sobre a adequação técnica e legal da proposta de classificação.

Quem deve se manifestar:

Chefia da unidade proponente; assessoria jurídica ou área equivalente — para verificar o enquadramento legal; gestão documental — para verificar a compatibilidade com os procedimentos do Posto de Controle e do STIC.

Atenção:

Pareceres contrários não impedem a decisão da autoridade classificadora, mas devem ser formalmente registrados no processo. A autoridade responde pessoalmente pelo ato de classificação.

04 - Decisão Formal

Ato formal da autoridade classificadora competente, formalizado por meio do Termo de Classificação da Informação (TCI), com todos os elementos obrigatórios previstos em lei.

O que o TCI deve conter:

Fundamento legal expresso (inciso do art. 23 da LAI); grau de sigilo atribuído; prazo de restrição de acesso; motivação detalhada; identificação e assinatura da autoridade classificadora; data de produção do documento.

Atenção:

Sem TCI assinado pela autoridade competente, a classificação não tem validade jurídica. O prazo começa a ser contado a partir da data de produção do documento, não da data de assinatura do TCI.

FLUXO INSTITUCIONAL PARA CLASSIFICAÇÃO

04.1 - Atribuição do CIDIC

Etapa complementar. Imediatamente após a assinatura do TCI, o Posto de Controle atribui ao documento o Código de Indexação de Documento que contém Informação Classificada (CIDIC) — identificador único que garante a rastreabilidade do documento em todo o seu ciclo de vida.

O que o CIDIC deve registrar:

Identificador único e sequencial; grau de sigilo atribuído; data de produção — início da contagem do prazo; prazo de restrição de acesso; identificação da autoridade classificadora e da unidade custodiante.

Atenção:

O CIDIC deve ser aposto fisicamente no documento e registrado no controle do Posto. Sem ele, o documento não pode circular, ser reproduzido ou transferido com validade jurídica.

04.2 - Registro no STIC

Etapa complementar. Com o CIDIC atribuído, o responsável cadastra a informação no Sistema de Tratamento de Informações Classificadas (STIC), plataforma eletrônica de uso obrigatório no Poder Executivo Federal.

O que registrar no STIC:

CIDIC do documento; grau de sigilo e prazo; fundamento legal — inciso do art. 23 da LAI; identificação da autoridade classificadora; data de produção e data-limite do sigilo; unidade custodiante.

Atenção:

O STIC e o Posto de Controle são complementares — não se substituem. O STIC responde pelo controle sistêmico e institucional; o Posto de Controle, pela custódia física e rastreabilidade documental.

05 - Controle

Implementação dos mecanismos de rastreabilidade, restrição de acesso e controle de compartilhamento do documento classificado, sob responsabilidade do Posto de Controle.

O que deve ser controlado:

Registro de cada acesso ao documento e identificação de quem acessou; controle de cópias e reproduções, cada cópia deve ser registrada individualmente; registro de transferências entre unidades; assinatura do TCMS por todos que acessarem a informação.

Atenção:

O acesso à informação classificada exige dois requisitos simultâneos: credencial de segurança válida e necessidade funcional de conhecer. A ausência de qualquer um deles impede o acesso, independentemente do cargo.

06 - Revisão

Verificação periódica da persistência dos motivos que justificaram a classificação, podendo resultar na manutenção do sigilo, na redução do grau ou na desclassificação imediata.

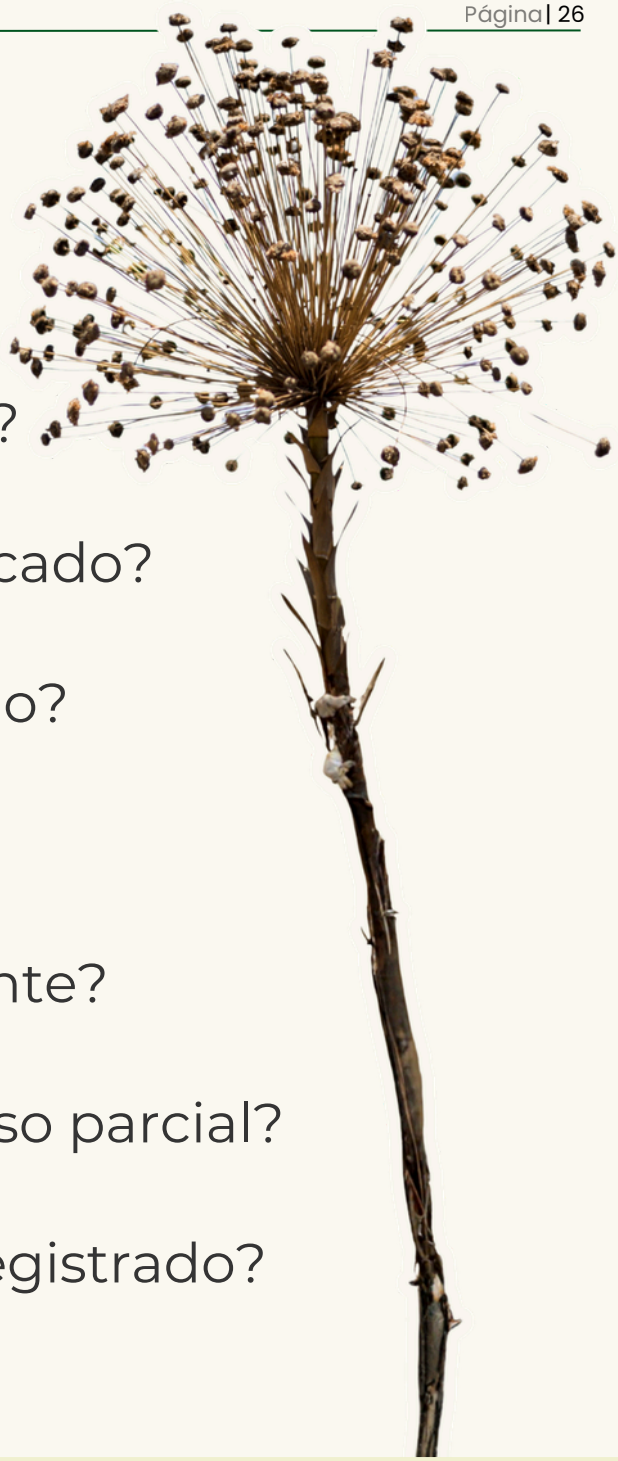
Prazos de revisão obrigatória:

Ultrassecreto e secreto: reavaliação obrigatória a cada 4 anos, enquanto durar o prazo de sigilo. Reservado: não está sujeito ao ciclo de 4 anos, mas deve ser revisto assim que o risco cessar. Qualquer cidadão pode solicitar reavaliação via SIC a qualquer tempo.

Atenção:

O sigilo não pode ser mantido por conveniência. Se o risco que o justificou deixar de existir, ainda que antes do prazo, a desclassificação é obrigatória. O término do prazo produz desclassificação automática.

CHECKLIST E DIRETRIZ FINAL



- ☑ Existe fundamento legal?
- ☑ Há risco concreto e explicado?
- ☑ O menor grau foi utilizado?
- ☑ O prazo é proporcional?
- ☑ A autoridade é competente?
- ☑ Há possibilidade de acesso parcial?
- ☑ O ato foi formalizado e registrado?

Diretriz Institucional

"No âmbito do ICMBio, a classificação deverá permanecer medida excepcional, tecnicamente motivada e vinculada à proteção da segurança da sociedade ou do Estado, vedada sua utilização como instrumento de ocultação administrativa ou restrição injustificada ao controle social."

ICMBio | Transparência Ativa

RESPONSABILIZAÇÃO

A LAI prevê sanções para as seguintes condutas:

CLASSIFICAR PARA ESCONDER IRREGULARIDADE

Atribuir grau de sigilo a uma informação com o objetivo de proteger o agente público ou seu superior, e não por razão de segurança da sociedade ou do Estado. É a forma mais grave de abuso do mecanismo e está vedada pelo art. 32, inciso V, da LAI.

DIVULGAR INFORMAÇÃO CLASSIFICADA SEM AUTORIZAÇÃO

Revelar, transmitir ou permitir acesso a documento sigiloso sem autorização prévia, seja por descuido ou de forma intencional. Enquadra-se no art. 32, inciso IV, da LAI.

NEGAR OU RETARDAR O ACESSO SEM FUNDAMENTO LEGAL

Recusar pedido de acesso sem justificativa legal, fornecer informação de forma incorreta ou incompleta, ou retardar deliberadamente a resposta.

Previsto no art. 32, inciso I, da LAI.

DESTRUIR, ALTERAR OU OCULTAR INFORMAÇÃO SOB GUARDA

Subtrair, inutilizar, desfigurar, alterar ou ocultar informação a que o agente tenha acesso em razão do cargo. Previsto no art. 32, inciso II, da LAI.

OCULTAR CLASSIFICAÇÃO DA REVISÃO DE AUTORIDADE SUPERIOR

Impedir ou dificultar que autoridade hierarquicamente superior reavalie uma classificação, beneficiando alguém ou causando prejuízo a terceiros.

Previsto no art. 32, inciso VI, da LAI.

AGIR COM DOLO OU MÁ-FÉ NA ANÁLISE DE PEDIDOS DE ACESSO

Analisar deliberadamente de forma tendenciosa os pedidos de acesso à informação, com intenção de negar acesso indevido. Previsto no art. 32, inciso III, da LAI.

RESPONSABILIZAÇÃO

Consequências

A LAI não pune apenas quem divulga indevidamente, pune igualmente quem classifica indevidamente.
O uso do sigilo como instrumento de poder ou de autoproteção é expressamente vedado.
As previsões de condutas ilícitas buscam resguardar o direito de acesso da sociedade contra possíveis arbitrariedades de agentes públicos, prevendo responsabilização em caso de práticas abusivas ou ilegais.

Atenção

Classificar mal é tão grave quanto vazar o que deveria ser sigiloso.

Penalidades

- Responsabilidade disciplinar administrativa
- Improbidade administrativa
- Responsabilidade penal

TRATAMENTO DE CÓPIAS E REPRODUÇÕES

Cada cópia de um documento classificado é tão sigilosa quanto o original. Reproduzir sem autorização e sem registro compromete a cadeia de custódia e configura conduta ilícita.

Quando a reprodução é permitida:

1. Autorização prévia

Da autoridade custodiante ou do Posto de Controle. Iniciativa própria do servidor não é suficiente, mesmo com acesso regular ao documento.

2. Necessidade funcional

A cópia deve ser necessária ao exercício de função específica. Cópias de conveniência ou para consulta pessoal não são autorizadas.

3. Credencial válida do destinatário

O destinatário deve ter credencial compatível com o grau de sigilo e necessidade de conhecer a informação.

4. TCMS assinado

O destinatário deve ter assinado o Termo de Compromisso de Manutenção de Sigilo antes de receber a cópia.

Cada cópia deve ser individualmente registrada. Cópias sem registro no Posto de Controle não têm validade jurídica e configuram falha de controle.

Quando a cópia deixar de ser necessária, ela deve ser devolvida ao Posto para descarte controlado, com registro da devolução e do método de eliminação utilizado.

TRATAMENTO DE CÓPIAS E REPRODUÇÕES

Reprodução parcial e tarjamento

Sempre que o destinatário precisar apenas de parte do documento, deve-se privilegiar a reprodução parcial com tarjamento irreversível, restringindo apenas o que precisa ser restringido.

É VEDADA:

- Reproduzir documento classificado sem autorização prévia e registro no Posto de Controle
- Enviar cópia por meios não seguros, e-mail convencional, aplicativos de mensagens, nuvem comercial ou qualquer canal sem criptografia homologada
- Deixar cópias em impressoras, scanners ou equipamentos de uso compartilhado
- Fotografar a tela ou o documento físico com dispositivo pessoal
- Manter cópia fora do ambiente seguro após o encerramento da necessidade funcional que a justificou

REVISÃO E DESCLASSIFICAÇÃO

Lembre-se!
O sigilo não pode durar indefinidamente e deve cessar assim que o risco desaparecer

Revisão de Ofício

A reavaliação periódica é dever da autoridade classificadora ou da instância por ela designada. Não depende de provocação externa. Seus prazos e procedimentos variam conforme o grau de sigilo:

- Verificação da **permanência dos motivos** que justificaram o sigilo original.
- Possibilidade de **redução de prazo ou desclassificação imediata.**
- **Ultrassecreto e Secreto** - reavaliação obrigatória a cada 4 anos;
- **Reservado** - não estão sujeitas ao ciclo obrigatório de 4 anos. A revisão de ofício é recomendada sempre que houver alteração relevante no contexto que motivou a classificação.

Desclassificação automática

- Encerrado o **prazo do sigilo**.
- Encerrado o e**vento que motivou** a restrição.
- A unidade custodiante deve **atualizar o registro no STIC** e comunicar a desclassificação ao SIC para fins de publicação no Rol anual de informações classificadas e desclassificadas.

Direito do Cidadão

- **Qualquer cidadão** pode solicitar a reavaliação da classificação via Serviço de Informação ao Cidadão - SIC.
- **Pedido deve ser fundamentado** e direcionado à autoridade classificadora.
- Autoridade classificadora, que tem **20 dias** para se manifestar, prorrogáveis por **mais 10 dias** mediante justificativa
- **Garantia de recurso em caso de indeferimento do pedido inicial.**
- Garantia de **transparência passiva e controle socia**l sobre o sigilo.

DESTINO DOS DOCUMENTOS CLASSIFICADOS

O fim do sigilo altera o regime de acesso, mas não elimina as obrigações de gestão documental. O documento passa a integrar o acervo público do órgão e deve ter seu destino formalmente definido.

Três destinos possíveis

RECOLHIMENTO AO ARQUIVO

Destino mais comum.
O documento é transferido ao arquivo do órgão e passa a integrar o acervo de livre acesso público.

GUARDA PERMANENTE

Documentos com valor histórico, científico, cultural ou probatório. Recolhidos ao Arquivo Nacional ou ao arquivo permanente do órgão. Nunca podem ser eliminados.

RESTRIÇÃO RESIDUAL

O documento contém informações protegidas por outro fundamento legal, como LGPD, segredo de justiça, sigilo bancário ou fiscal. Exige nova avaliação antes da disponibilização.

Documentos que cumpriram o prazo de guarda previsto na tabela de temporalidade e não apresentam valor permanente podem ser eliminados — mas apenas com procedimento específico.

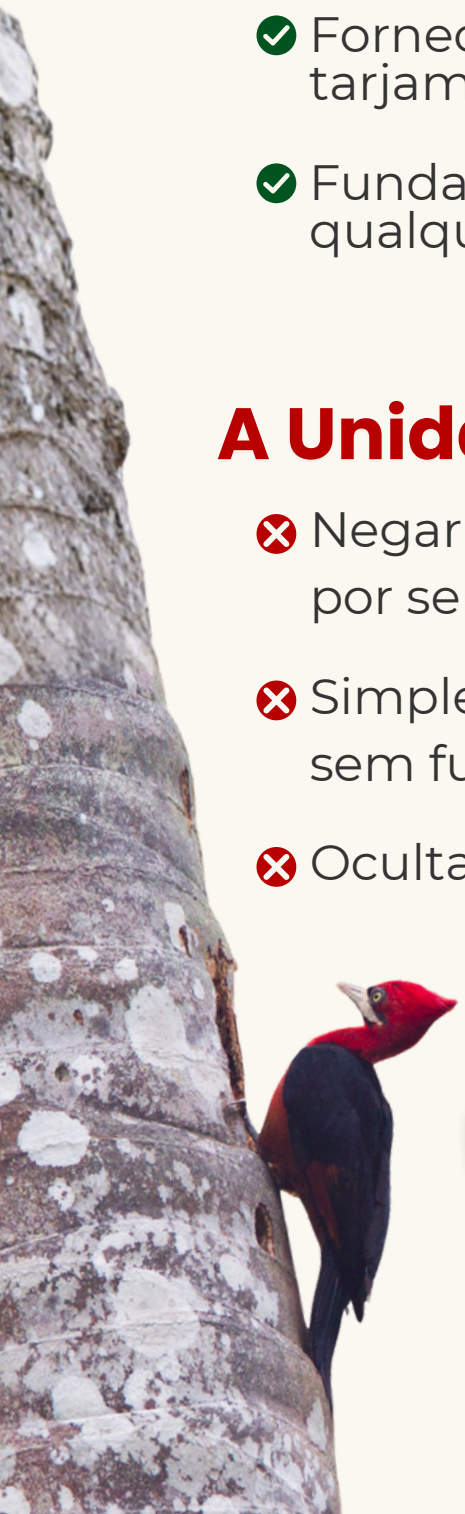
ATENDIMENTO A PEDIDOS DE ACESSO À INFORMAÇÃO(SIC)

A Unidade DEVE:

- Orientar o cidadão sbre prazos e recursos cabíveis.
- Analisar a possibilidade de acesso parcial.
- Fornecer extratos ou versões com tarjamento de dados sensíveis.
- Fundamentar detalhadamente qualquer negativa de acesso.

A Unidade NÃO deve:

- Negar o acesso automaticamente por ser "documento interno".
- Simplesmente informar "documento sigiloso" sem fundamentação.
- Ocultar a existência da informação classificada.



Lembre-se!

DIRETRIZ: Máxima publicidade possível, mínima restrição necessária.

CANAIS DE ATENDIMENTO

SIC ICMBio

Canal oficial para pedidos de desclassificação e recursos sobre sigilo.

sic@icmbio.gov.br

Competência do SIC no âmbito da Informação Sigilosa

LGPD: responsável por receber e encaminhar solicitações, dúvidas e questionamentos relacionados aos dados pessoais tratados pela instituição.

INFORMAÇÃO CLASSIFICADA: atua no recebimento e encaminhamento de solicitações, dúvidas e questionamentos relacionados às informações com restrição de acesso tratadas pela instituição

OUTROS MEIOS

ouvidoria@icmbio.gov.br

(61) 2028-9210 / (61) 2028-8918


Ouvidoria
ICMBio - MMA
ICMBio
INSTITUTO CHICO MENDES
MMA
MINISTÉRIO DO
MEIO AMBIENTE E
MUDANÇA DO CLIMA