GUIA

Classificação da Informação

MINISTÉRIO DOS
TRANSPORTES

Ministro da Infraestrutura
José Renan Vasconcelos Calheiros Filho

Secretário-Executivo
George André Palermo Santoro

Subsecretário de Planejamento, Orçamento e Administração
Manuel Augusto Alves Lima

Coordenadora - Geral de Recursos Logísticos
Rose Leuda Freitas Damasceno

Divisão de Gestão Documental
Nádia Barbosa Gonçalves

Diagramação
Elizia Hemily de Sousa Oliveira

SUMÁRIO

INTRODUÇÃO

São os instrumentos de controle social que possibilitam a fiscalização da gestão pública pelo cidadão, e dentre estes, certamente a transparência se apresenta como um dos mais frutuosos. Representa uma marca importante no processo civilizacional brasileiro, sobretudo ao potencializar as medidas que substancializam o país como uma nação mais justa e democrática.

Um dos diplomas criados para efetivar o princípio da transparência, ou ainda o direito subjetivo ao acesso à informação, previsto no inciso XXXIII do artigo 5º da Constituição Federal, trata-se da Lei de Acesso à Informação (LAI), nº 12.527, datada em 18 de novembro de 2011, visando regular as relações jurídicas que se compõe do direito à informação dos cidadãos e do dever de prestação destas por parte do Poder Público.

O SEI! desde a sua implementação tem como princípio a transparência do fluxo de informações e o trabalho colaborativo. A informatização certamente em marcha mais avançada do que o Direito consegue se propor, é aliado indispensável e indissociável da concretização do acesso à informação. Contudo, é nos limites da lei que devemos delimitar a atuação do agente público em face desse fluxo transparente e cada vez mais colaborativo em que o processo administrativo se corporifica por obra das evoluções da tecnologia.

Diante disso, o presente guia tem por escopo auxiliar autoridades, servidores e colaboradores no âmbito do Ministério dos Transportes acerca da classificação das informações com base na Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI).

Objetiva-se, também, orientar os usuários do Sistema Eletrônico de Informações SEI!/MT quanto às características e ao funcionamento dos processos com nível de acesso sigilosos.

TIPOS DE INFORMAÇÃO

O conceito do que é informação pública decorre da natureza do documento público. A Lei 8.159, de 8 de janeiro de 1991, conceitua em seu art. 7º o documento público:

> Os arquivos públicos são os conjuntos de documentos produzidos e recebidos, no exercício de suas atividades, por órgãos públicos de âmbito federal, estadual, do Distrito Federal e municipal em decorrência de suas funções administrativas, legislativas e judiciárias.
> § 1º São também públicos os conjuntos de documentos produzidos e recebidos por instituições de caráter público, por entidades privadas encarregadas da gestão de serviços públicos no exercício de suas atividades

Via de regra, documentos produzidos no contexto da instituição pública são públicos, e as informações ali registradas recebem mesmo tratamento. A restrição à informação deve ser exceção e se restringir às hipóteses legais.

Cumpre esclarecer que, quanto à acessibilidade, as informações podem ser ostensivas ou sigilosas, conforme conceitos abaixo:

a) **Informação Ostensiva:** Aquela cujo acesso pode ser franqueado a qualquer pessoa, sem restrição.
b) **Informação Sigilosa:** Aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado. O acesso deve ser restrito às pessoas que, por seu cargo ou função, tenham necessidade de tomar conhecimento do seu teor.

DAS INFORMAÇÕES PÚBLICAS

As informações públicas ou ostensivas são a regra geral e personificam o mais amplo domínio dos princípios da transparência e acesso à informação. Não caberia neste guia a descrição pormenorizado do tratamento das informações públicas, pois do ponto de vista da classificação da informação é mais pertinente tratar as exceções, e sob a perspectiva das funcionalidades do SEI depreende-se que o interlocutor já é um usuário habitual do sistema. Contudo, alguns lembretes são importantes:

- Para utilizar a pesquisa pública do SEI/MT não é necessário que o cidadão faça o cadastro como usuário externo.
- Nos processos públicos, tanto o andamento do processo, quanto os documentos assim classificados ficam ostensivamente disponíveis os usuários externos sem necessidade de liberação ou cadastro.
- Nos processos restritos, o andamento do processo e os documentos classificados como públicos ficam ostensivamente disponíveis.
- É possível conceder acesso externo aos documentos restritos e sigilosos mediante a liberação por um usuário interno.
- É possível conceder acesso externo ao processo completo ou somente a determinados documentos.
- É possível dar acesso externo a um cidadão que não tenha cadastro como usuário externo. Nesse caso, ele receberá no e-mail informado um link para download dos documentos disponibilizados. Recomenda-se, contudo, a ponderação do concedente e análise da conveniência de tal ato.
- Não é possível dar acesso externo a um processo sigiloso a usuário externo que não tenha cadastro. Para processos sigilosos o cadastro é indispensável.
- O usuário externo que peticionar no protocolo virtual terá acesso externo ao processo por ele criado e aos documentos que ele inserir. Se documentos restritos forem inseridos no MT, será necessário que um usuário interno lhe conceda outro acesso com relação a estes, mesmo o processo tendo sido criado por ele no protocolo virtual.
- Documentos protocolados por usuários externo não podem ser excluídos ou cancelados do SEI em nenhuma hipótese, mesmo com perfil de administrador.

TRATAMENTO DAS INFORMAÇÕES RESTRITAS

No SEI/MT atualmente constam as seguintes hipóteses legais de acesso restrito cadastrado:

Restrito	Apuração de Infração de Natureza Ética	Art. 13, Decreto nº 6.029/2007
Restrito	Controle Interno	Art. 26, § 3º, da Lei nº 10.180/2001
Restrito	Documento Preparatório	Art. 7º, § 3º, da Lei nº 12.527/2011
Restrito	Informação de Segurança da Aviação Civil	2.1.4, Anexo 17, Convenção de Aviação Civil Intern
Restrito	Informação Pessoal	Art. 31 da Lei nº 12.527/2011
Restrito	Investigação de Responsabilidade de Servidor	Art. 150 da Lei nº 8.112/1990
Restrito	Sigilo Contábil	Art. 1.190 da Lei nº 10.406/2002
Restrito	Sigilo Empresarial	Art. 169 da Lei nº 11.101/2005
Restrito	Sigilo Fiscal	Art. 198, caput, da Lei nº 5.172/1966
Restrito	Sigilo/Segredo de Justiça/Segredo Industrial	Art. 22, da Lei nº 12.527/2011

Se a restrição de acesso visa tutelar direitos de titularidade de usuários, da sociedade e do Estado, a restrição de acesso visa proteger interesses pessoais, de terceiros e institucionais (e não a segurança da sociedade e do Estado). Nesse caso, a sua disseminação certamente não tem a capacidade de causar dano com a mesma gradação que o vazamento de uma informação sigilosa, mas também é prejudicial e justifica a sua limitação de acesso.

Sobre os documentos restritos, cumpre destacar:

- Os processos e documentos restritos ficam legíveis somente àqueles com acesso às unidades nas quais o processo tramitar.
- Ao se incluir documento com nível de restrição de acesso em um processo, todos os documentos nele inseridos, independentemente de serem públicos ou não, assumirão o comportamento do maior nível de restrição de acesso, ou seja, o conjunto sempre assumirá as características do maior nível de restrição, mesmo que o processo seja público. É o que se denomina de "contaminação do documento restrito".
- Contudo, na pesquisa pública a "contaminação do documento restrito" não se aplica. Mesmo estando indisponíveis para os usuários internos, para os usuários externos os documentos públicos em processos com documentos restritos ficam públicos.
- Documentos restritos podem ser enviados via barramento para outros órgãos e seguem assim categorizados.
- Documentos restritos são acessíveis para usuários externos com permissão de acesso do tipo "acompanhamento integral do processo", mesmo que o documento restrito tenha sido inserido após a disponibilização.

Importante: É necessário reforçar que em um processo com nível de acesso global for inserido um documento restrito, este assume em sua completude o comportamento de restrito para o usuário interno. Contudo, para a pesquisa pública será exibido o nível de acesso global do processo e a restrição fica adstrita ao documento assim classificado. Isso quer dizer que cada documento restrito tem que ser assim classificado, a não ser que o processo esteja globalmente classificado como restrito.

Importante: Ao restringir o acesso a determinado processo ou documento, é necessário indicar a hipótese legal disponível no sistema. É salutar, outrossim, que no campo "Observações desta unidade" o usuário complemente a justificativa da restrição caso necessário.

Da proteção às informações pessoais:

Segundo o art. 5º da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), informação pessoal é aquela relacionada à pessoa natural identificada ou identificável. Um subgrupo dos dados pessoais, é o dado pessoal sensível, que recebeu atenção especial do legislador.

A LGPD elenca como dados pessoais sensíveis aqueles capazes de revelar informação sobre personalidade, relações afetivas, origem étnica ou racial, ou que se refiram às características físicas, morais ou emocionais, à vida afetiva e familiar, patrimônio, ideologia e opiniões políticas, crenças ou convicções religiosas ou filosóficas, estados de saúde físicos ou mentais, preferências sexuais ou outras análogas que afetem sua intimidade ou sua autodeterminação informativa.

A identificação de dados sensíveis depende do contexto do dado e da informação a que ele se relaciona. Contudo, pragmaticamente, podemos considerar como informações sensíveis, e passíveis de restrição de acesso, as que fazem referência a:

- dados relativos a documentos de identificação pessoal, tais como RG, CPF, título de eleitor, data de nascimento, identidade funcional, estado civil, entre outros;
- nome completo ou parcial de cônjuge ou familiares;
- informações sobre o estado de saúde do servidor ou familiares;
- informações financeiras ou patrimoniais de determinada pessoa;
- informações sobre alimentandos, dependentes ou pensões;
- endereço pessoal ou comercial de determinada pessoa;
- filiação partidária; e
- número de telefone ou endereço eletrônico pessoal.

O legislador conferiu às informações pessoais sensíveis tratamento diferenciado com o objetivo de proteger a intimidade, vida privada, honra e imagem, bem como as liberdades e garantias individuais. Independente de classificação, tais informações terão o seu acesso restrito pelo prazo máximo de 100 anos a contar da data de sua produção.

A divulgação da informação pessoal sensível pode ser autorizada ou acessada por terceiros diante de previsão legal ou consentimento expresso da pessoa a que ela se referira. A LAI e a LGPD, contudo, preveem exceções nas quais não se exigirá consentimento expresso do interessado:

- cumprimento de obrigação legal ou regulatória pelo controlador de dados;
- tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

- realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da LGPD, e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Tal proteção também não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

Importante: Deve ser redobrada a atenção com possíveis comprometimentos da segurança de informações relativas à intimidade, vida privada, honra e imagem dos interessados, e nunca hesitar em atribuir a classificação restrita para documentos que possuam tais características.

Atenção! Documentos com dados pessoais devem ter acesso restrito, o que não quer dizer que todo o processo que detém dados pessoais deve ser restrito.

Da proteção às informações a respeito de crianças e adolescentes:

Uma outra camada especial de proteção foi atribuída pela LGPD ao tratamento de dados de menores de 18 anos. Nesse caso, para tratar o dado é imprescindível obter o consentimento inequívoco de um dos pais ou responsáveis. Também é importante que o tratamento seja relativo somente ao conteúdo estritamente necessário para a atividade institucional em questão.

Todos os dados relativos a informações pessoais de crianças e adolescentes devem ser restritos.

Dos Documentos Preparatórios:

Os documentos preparatórios são aqueles que fundamentam a tomada de decisão ou o ato administrativo, de forma que o seu acesso será restrito somente

àqueles que por motivos funcionais tenham de conhecer seu conteúdo. A LAI estabelece, contudo, que após a edição do ato decisório respectivo, a causa da restrição expira e os documentos passam a ser públicos, salvo se houver outro critério de restrição associado.

São exemplos destes documentos os pareceres, notas técnicas e quaisquer documentos que subsidiem decisões, sejam elas administrativas, orçamentárias, financeiras ou consultivas.

Também recebem proteção documentos que fazem parte do processo decisório que culminarão na edição de ato normativo, bem como os artefatos que compõem o procedimento licitatório antes da publicação do edital.

Se o processo for constituído de vários atos ou decisões que podem ser consideradas etapas dotadas de certa autonomia, deve-se levar em consideração a publicização compartimentalizada dos seus respectivos documentos preparatórios caso seja oportuno.

PROCESSO SIGILOSO X INFORMAÇÃO CLASSIFICADA EM GRAU DE SIGILO

A Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI), estabeleceu rol taxativo de hipóteses nas quais a Administração pode designar o sigilo de determinada informação. Em comum, todas elas são consideradas imprescindíveis à segurança da sociedade e do Estado.

Reconhecendo a presença de uma das circunstâncias previstas na LAI, a autoridade competente, por meio de decisão administrativa, impõe o sigilo nos termos da lei. É o que se denomina classificar a informação.

Apesar da nomenclatura dar margem a outras interpretações, à luz da LAI, classificar um documento é atribuir a ele um grau de sigilo (reservado, secreto e ultrassecreto). As informações protegidas por quaisquer outros sigilos legais, informações pessoais, documentos preparatórios ou aquelas em que incidem as hipóteses dos arts. 5º e 6º do Decreto nº 7.724/2012 não são classificadas!

Sobre quaisquer outras hipóteses não previstas no art. 23 da LAI, as informações são protegidas apenas com a restrição de acesso, seja ele restrito ou sigiloso. Dessa forma, é possível exemplificar o tratamento legal à proteção da informação da seguinte forma:

Base Legal	Tratamento	Suporte
• Art. 23, Lei nº 12.527 – LAI; • Imprescindíveis à segurança da sociedade e do Estado; • Rol taxativo;	Classificação das informações em secretas, ultrassecretas e reservadas.	O SEI! não possui os requisitos de criptografia necessários para receber informações classificadas em grau de sigilo. Diante disso, tais documentos não deverão ser produzidos no SEI! ou digitalizados para inserção no sistema. Devem ser produzidos e armazenados em papel ou em outro meio adequado.
• Lei nº 12.527 – LAI (documentos preparatórios, sigilo empresarial; • Decreto nº 7.724/2012 (sigilo decorrente de risco à governança empresarial); • Lei Complementar nº 105/2001 (sigilo bancário); • Lei 9.610/98 (sigilo Decorrente de Direitos Autorais); • Código Tributário Nacional – CTN (sigilo fiscal); • Código de Processo Civil – art. 18; e Código de Processo Penal – art. 20 (segredo de justiça); • Constituição Federal, art. 5º, XXIX (sigilo industrial) e XXVII (direito autoral) • Rol não taxativo	Restrição de acesso ao documento, seja restrito ou sigiloso conforme o caso.	Podem ser produzidos, inseridos e tramitados no SEI.

Em resumo, as opções de restrito ou sigilo disponíveis no SEI! dizem respeito somente à forma como o documento será tramitado e acessado. Informações classificadas não devem estar disponíveis no SEI! e o seu rol de abrangência é restrito às hipóteses previstas na LAI.

Importante: A respeito de qualquer outro tipo de sigilo, seja ele fiscal ou segredo de justiça, a restrição de acesso desse tipo de informação sigilosa independe de classificação, pois seu sigilo tem outros fundamentos. Ou seja, a informação é sigilosa quanto à restrição de acesso, mas não é classificada.

INFORMAÇÕES CLASSIFICADAS

A LAI estabelece que as informações classificadas são aquelas cujo sigilo é imprescindível à segurança da sociedade e do Estado. Deve-se, contudo, observar o interesse público como princípio norteador e ponderar de forma restritiva qualquer tipo de limitação ao acesso. As informações que podem ser classificadas são aquelas cuja divulgação ou acesso irrestrito possam:

- pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
- 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;
- pôr em risco a vida, a segurança ou a saúde da população;
- oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
- prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
- 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;
- pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares;
- comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações; e
- colocar em risco a segurança do Presidente e Vice-Presidente da República e respectivos cônjuges e filhos(as).

Por quanto tempo as informações classificadas ficam protegidas?

O período de proteção da informação tem relação com a imprescindibilidade do sigilo à segurança da sociedade ou do Estado. Com base neste critério, poderão ser classificadas em três diferentes graus:

Reservado	5 (cinco) anos
Secreto	15 (quinze) anos
Ultrassecreto	25 (vinte e cinco) anos

Após o prazo de validade da classificação, as informações tornam-se de acesso público, contudo, tais documentos devam ser analisados de modo a proteger eventuais informações pessoais sensíveis ou cobertas por outras sigilos porventura presentes.

Importante: A classificação da informação como ultrassecreta é a única passível de prorrogação, por até igual período (25 anos, totalizando o período máximo de 50 anos). A competência para a prorrogação de uma classificação ultrassecreta por até 25 anos também é prerrogativa exclusiva da Comissão Mista de Reavaliação de Informações (CMRI).

Importante: O prazo começa a contar da data de produção do documento. Diante disso, se uma informação produzida há 10 anos for classificada como reservada na data de hoje, ela teria se tornado ostensiva há 5 anos e a classificação não teria efeito.

Quais autoridades podem classificar informações?

Como o preceito geral da Lei é que o acesso às informações públicas é a regra, classificar uma informação e limitar o seu acesso é uma decisão que exige formalidade, fundamentação e sobretudo cautela. Na ocasião, a autoridade classificadora deverá indicar o assunto sobre o qual versa a informação, o fundamento da classificação, o prazo de sigilo ou evento que definirá o seu término. Essa fundamentação tem o mesmo grau de sigilo da informação protegida.

A competência para a classificação das informações varia de acordo com o grau de proteção:

CLASSIFICAÇÃO	QUEM DECIDE
Grau ultrassecreto (25 anos)	• Presidente da República. • Vice-Presidente da República. • Ministros de Estado e autoridades com as mesmas prerrogativas. • Comandantes da Marinha, do Exército e da Aeronáutica. • Chefes de Missões Diplomáticas e Consulares permanentes no exterior.
Grau secreto (15 anos)	•Todos os autorizados para o grau ultrassecreto. • Titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista.
Grau reservado (5 anos)	•Todos os autorizados para os graus ultrassecreto e secreto. • Autoridades que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo- Direção e Assessoramento Superiores, ou de hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade.

A competência para a classificação como ultrassecreta e secreta poderá ser delegada pela autoridade responsável a agente público, inclusive em missão no exterior, vedada a subdelegação. Cumpre destacar que até a data da edição deste guia não há delegação desta competência no âmbito do MT.

Importante: A autoridade ou agente público deverá encaminhar sua decisão de classificar a informação como ultrassecreta à Comissão Mista de Reavaliação de Informações (CMRI).

COMISSÃO MISTA DE REAVALIAÇÃO DE INFORMAÇÕES (CMRI)

A Comissão Mista de Reavaliação de Informações (CMRI) prevista no art. 35 da LAI, e regulamentada pelo Decreto nº 7.724, de 16 de maio de 201, é um colegiado composto por membros de diversos órgãos do Poder Executivo federal, sob presidência da Casa Civil da Presidência da República.

A CMRI atua uniformizando o entendimento e estabelecendo orientações normativas de caráter geral a fim de suprir eventuais lacunas na aplicação da LAI. As instruções são feitas sob a forma de Súmulas ou Resoluções. Ao todo, a CMRI já emitiu 8 Súmulas e 5 Resoluções, todas disponíveis em: https://www.gov.br/acessoainformacao/pt-br/assuntos/recursos/recursos-julgados-a-cmri/sumulas-e-resolucoes .

Além disso, a CMRI recebe e decide recursos contra as decisões da CGU, sendo, portanto, a quarta e a última instância recursal prevista pela LAI. Além de decidir esses recursos, a CMRI tem outras atribuições, dentre as quais a de rever, de ofício ou mediante provocação, a classificação de informação no grau ultrassecreto ou secreto ou a prorrogação no caso do ultrassecreto.

PROCEDIMENTO PARA A CLASSIFICAÇÃO DA INFORMAÇÃO

Fluxo para criar um documento classificado

1 - Documento em suporte físico (papel) recebido externamente; projeto ou qualquer documento com informações sensíveis

2 - No SEI!, Iniciar um processo com o tipo que mais se adequado ao tema e que esteja destacado com uma tarja vermelha.

Somente processos tarjados em vermelho são passíveis de serem classificados como sigilosos. Caso não haja um tipo adequado, entrar em contato com a DIGED (diged@transportes.gov.br) e solicitar apoio.

3 - Em "Iniciar Processo" preencher os campos disponíveis e selecionar o nível de acesso "sigiloso". Em "Observações desta Unidade" preencher com o seguinte texto: Documento com informação classificada em grau de sigilo, de acordo com a Lei nº 12.527/2011.

4 – No processo sigiloso criado no SEI!, incluir o TCI, preenchendo todos os campos e deixando em branco as "Razões para a Classificação" que serão preenchidas fora do SEI!. Imprimir o TCI, pois ele acompanhará o documento principal em papel. O TCI deverá conter o CIDIC - Código de Indexação de Informação Classificada.

5 - **IMPORTANTE** – O documento principal não deve ser digitalizado e incluído no SEI!. O processo deve ser criado tão somente para gerar o NUP, e o TCI terá somente a sua parte não classificada incluída nele (mesmo tendo acesso sigiloso) para que exista algum registro que ligue o NUP ao processo sigiloso e com isso se evite reutilização indevida do NUP.

6 – Encaminhar ao chefe imediato o dossiê em papel contendo o documento principal, o despacho (assinado pelo servidor e fundamentado com as razões para a classificação em grau de sigilo) e o TCI.

7 - O chefe encaminhará o dossiê à autoridade classificadora. Se não aprovada a classificação em grau de sigilo pela autoridade competente, o despacho deverá seguir anexado ao processo e todos os documentos deverão ser inseridos no SEI! para tramitação.

Observações sobre a instrução de documentos classificados

- Cabeçalhos e rodapés devem conter o grau de sigilo do documento;
- As páginas serão numeradas;
- Expressão diagonal “Documento Controlado DC”, se o documento for assim tratado;
- O documento, bem como o Termo de Custódia ou Guarda serão registrados com protocolo e recibos específicos;
- O órgão expedidor e recebedor fará a lavratura anual de termo de inventário.
- Todo documento classificado será tratado em protocolo próprio.
- Todo documento classificado ficará acondicionado em local de acesso restrito sob guarda da DIGED-MT, conforme regramento específico.

➢ Para o envio de documentos físicos:

- Acondicionados em envelopes duplos;
- No envelope externo, sem indicação de grau de sigilo ou teor do documento;
- No envelope interno, constarão o destinatário e o grau de sigilo do documento;
- O envelope interno será expedido mediante recibo com indicação remetente, destinatário e número do documento;
- A palavra “pessoal” é posta no envelope interno se o destinatário for específico;
- No que se refere ao documento físico, a expedição, a condução e a entrega de documento físico ULTRASSECRETO será efetuada pessoalmente;
- No que se refere ao documento físico, a expedição de documento SECRETO e RESERVADO será feita pelos meios de comunicação disponíveis ou por via diplomática, sem prejuízo da entrega pessoal.

➢ Para envio de documentos digitais:

- No que se refere ao documento digital, a expedição de documento ULTRASSECRETO, SECRETO e RESERVADO será feita pelos meios de comunicação disponíveis, desde que criptografado com recurso compatível com o grau de sigilo (algoritmo de Estado);
- É PROIBIDA o tratamento da informação classificada em nuvem, mesmo o documento preparatório que fundamenta a classificação de informação em grau de sigilo.

➢ Reprodução

- A reprodução do todo ou de parte, terá o mesmo grau de sigilo do documento;
- A reprodução total ou parcial deve ter autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior;
- As cópias serão autenticadas pela autoridade classificadora;
- A operação será acompanhada por pessoal oficialmente designada.

Classificação - TCI

No âmbito do Poder Executivo federal, a classificação de realizada por meio de um ato administrativo formal denominado Termo de Classificação de Informação - TCI. Esse é um documento público, que efetivamente materializa a classificação, recaindo restrição de acesso somente a um de seus campos: o campo "razões da classificação", sob o qual incide o mesmo grau de sigilo da informação classificada.

O correto preenchimento do TCI é condição para existência e validade da decisão de classificação, razão pela qual se deve ter o máximo de cuidado no preenchimento de cada um dos seus campos.

O TCI é indexado por meio do Código de Indexação de Documento que contém Informação Classificada (CIDIC), conforme orientações existentes no Decreto nº 7.845/2012.

O Código de Indexação de Documento que contém Informação Classificada - CIDIC é composto por:

- número único de protocolo do documento ou processo (NUP);
- grau de sigilo (reservado - R, secreto - S ou ultrassecreto-U);
- categoria (01 a 17) – as categorias estão descritas no Anexo II do Decreto nº 7.845/2012. A categoria 17, por exemplo, trata de transportes e trânsito;
- data da produção da informação (DD/MM/AAAA);
- data de desclassificação da informação (data em que a informação será desclassificada - DD/MM/AAAA);
- indicação de reclassificação (sim - S ou não - N);
- data da prorrogação (DD/MM/AAAA).

CIDIC (Decreto nº 7.845/12)						
1ª Parte (NUP)	**2ª Parte**					
Art. 51	Art. 52, I Grau de sigilo	Art. 52, II Categoria	Art. 52, III Data de produção	Art. 52, IV Data de desclassificação	Art. 52, V Indicação da reclassificação	Art. 52, VI Data da prorrogação
50000...	U, S ou R	01 a 17	dd/mm/aaa	dd/mm/aaaa	S ou N	dd/mm/aaa

✓ Exemplo de processo classificado no grau RESERVADO, sem reclassificação:
50000.000001/2021-01. R.17.23/05/2021.22/05/2026.N

O Termo de Classificação da Informação – TCI é composto pelos seguintes campos:

- Código de indexação de documento;
- Grau de sigilo;
- Categoria na qual se enquadra a informação;
- Tipo de documento;
- Data da produção do documento, marco inicial de contagem do prazo de sigilo.
- Fundamentação legal que na qual se enquadra a classificação.
- Razões da classificação ou da restrição de acesso à informação, observados os critérios estabelecidos no art. 27 do Decreto nº 7.724/2012. Trata-se da motivação do ato administrativo. Relembrando que as razões da classificação têm o mesmo grau de sigilo da informação classificada.
- Indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no art. 28 do Decreto nº 7.724/2012;
- Data da classificação; e
- Identificação da autoridade que classificou a informação.

ACESSO, USO E DISSEMINAÇÃO DE INFORMAÇÕES SIGILOSAS

O acesso a informações classificadas é restrito àqueles que possuem o dever de ofício de conhecê-las, pois a limitação do seu acesso e manipulação é medida importante para a garantia do sigilo.

O conhecimento, a disseminação e a reprodução de informação sigilosa, seja ela total ou parcial, deve ser precedida de autorização expressa ou da autoridade que a classificou, ou de autoridade hierarquicamente superior com igual prerrogativa.

Importante: A reprodução terá o mesmo grau de sigilo do documento original. O responsável pela reprodução deverá ser credenciado para tanto e ter assinado o Termo de Compromisso de Manutenção de Sigilo – TCMS. Além disso, tem o dever de manter o sigilo da operação, se abstento de manter notas manuscritas ou qualquer outro recurso que dê origem a cópia não-autorizada do todo ou parte.

Responsabilização

A responsabilização do agente público no âmbito da LAI ocorre tanto nos casos em que obstruir o acesso à informação ostensiva quanto nos casos em que divulgar informação sigilosa. Esse é um dever de todos os servidores, colaboradores e autoridades do MT, independente do contexto em que tenha tido contato com a informação.

Todos devem zelar pelo controle do acesso e da divulgação de informações sigilosas e restritas produzidas ou mantidas pela sua unidade, garantindo a proteção e guarda dos documentos em condições adequadas de segurança. Contudo, também deve ser observado o dever de preservar informações obtidas de forma circunstancial, ou seja, quando não era o seu dever de ofício garantir a proteção daquela informação, mas esta chegou ao seu conhecimento por qualquer motivo. O dever de proteger a informação é de todos.

O art. 65 do Decreto nº 7.724/2012 estabelece condutas consideradas ilícitas e que podem ensejar a responsabilização do agente público, a saber:

- recusar-se a fornecer informação requerida nos termos do Decreto, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;
- utilizar indevidamente, subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda, a que tenha acesso ou sobre que tenha conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;
- agir com dolo ou má-fé na análise dos pedidos de acesso à informação;
- divulgar, permitir a divulgação, acessar ou permitir acesso indevido a informação classificada em grau de sigilo ou a informação pessoal;
- impor sigilo à informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;
- ocultar da revisão de autoridade superior competente informação classificada em grau de sigilo para beneficiar a si ou a outrem, ou em prejuízo de terceiros;
- Destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado.

DESTINAÇÃO FINAL

A avaliação e a seleção de documento com informação desclassificada devem ser feitas pela Comissão Permanente de Avaliação de Documentos de Arquivo – CPAD.

A depender da classificação, os documentos podem ficar armazenados no Arquivo Central durante o prazo de guarda, eliminados, ou recolhidos ao Arquivo Nacional. Ressalta-se, contudo, que enquanto permanecerem classificados nenhum documento com qualquer grau de sigilo será eliminado.

PROCESSOS SIGILOSOS NO SEI!

Como já explicitado, o SEI! não possui os requisitos de criptografia necessários para receber informações classificadas em grau de sigilo (Ultrassecreto, Secreto ou Reservado). Dessa forma, tais documentos não deverão ser produzidos ou digitalizados no SEI!, contudo, documentos categorizados por outras hipóteses de sigilo previstas em legislações diversas podem autuados no sistema a depender do regramento próprio.

Principais características dos processos sigilosos

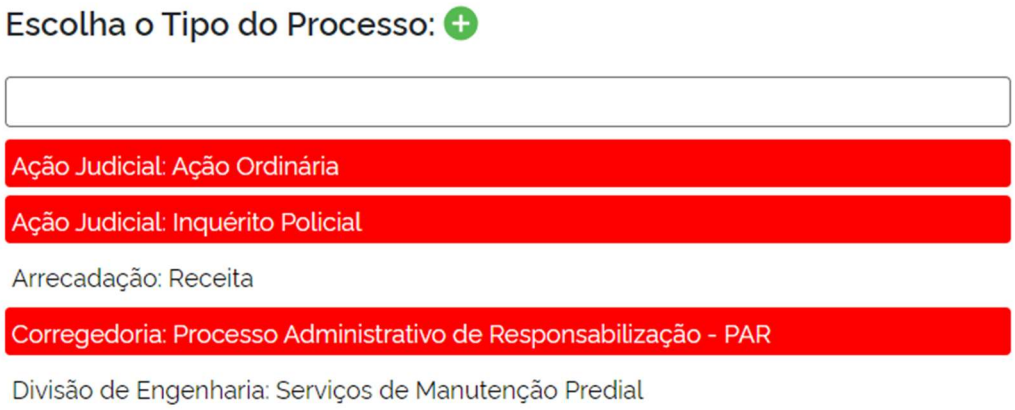
- O processo sigiloso não será visualizado por outros servidores da unidade, somente por aquele com credencial de acesso;
- A credencial de acesso é nominal, mas também é vinculada a uma unidade. O usuário não terá acesso ao processo em outras unidades diferentes da inicialmente credenciada;
- O envio dos processos sigilosos ocorre entre usuários por meio da concessão da credencial de acesso, e não pela função “enviar processos”;
- A credencial de acesso poderá ser revogada a qualquer momento por quem a concedeu, e da mesma forma o servidor credenciado poderá renunciá-la;
- Não será possível renunciar a uma credencial de acesso quando houver apenas um servidor credenciado;
- O usuário interno detentor de credencial de acesso a documento sigiloso, esteja este concluído ou em tramitação, caso tenha sua lotação ou função alterada, deve realizar a transferência de credencial nos referidos documentos ao seu sucessor ou chefe imediato;
- Caso tenha havido alteração de nível de acesso de restrito para sigiloso e existam usuários externos com permissão para visualização integral do processo, esses usuários continuarão com acesso aos autos. Caso isso não seja desejável, será necessário revogar o acesso dos usuários externos;
- No caso do usuário com a ultima credencial de acesso ser excluído do SEI!, o processo ficará disponível para o Administrador do sistema. Somente neste caso o Administrador tem acesso aos processos sigilosos sem uma credencial de acesso convencional;
- Estas funções não estão disponíveis nos processos sigilosos: anexar processos; bloco de assinatura; bloco de reunião; bloco Interno; e acompanhamento especial;
- É possível disponibilizar um processo sigiloso para usuário externo, tanto para visualização quanto para assinatura;

- Não é possível enviar um processo sigiloso pelo Tramita.BR (antigo barramento).

Trabalhando com processos sigilosos

✓ *Criando o processo*

Nem todos os processos permitem a restrição de acesso, seja na modalidade restrita ou sigilosa. Quando um processo pode ser sigiloso, ele aparece com uma tarja vermelha no momento da seleção do tipo do processo:

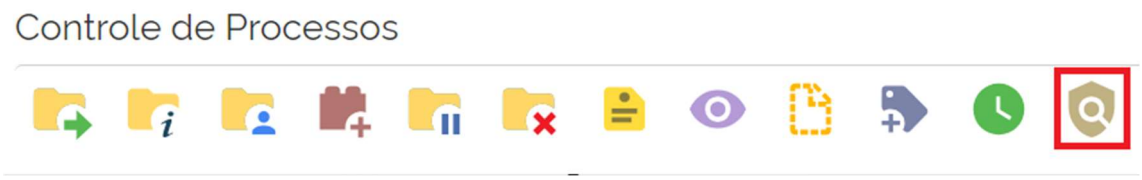


O que diferencia é a configuração do tipo do processo, e não tem nenhuma relação com o perfil do usuário. Caso seja necessário habilitar alguma opção de restrição de acesso a determinado tipo de processo, a Divisão de Gestão Documental deve ser acionada.

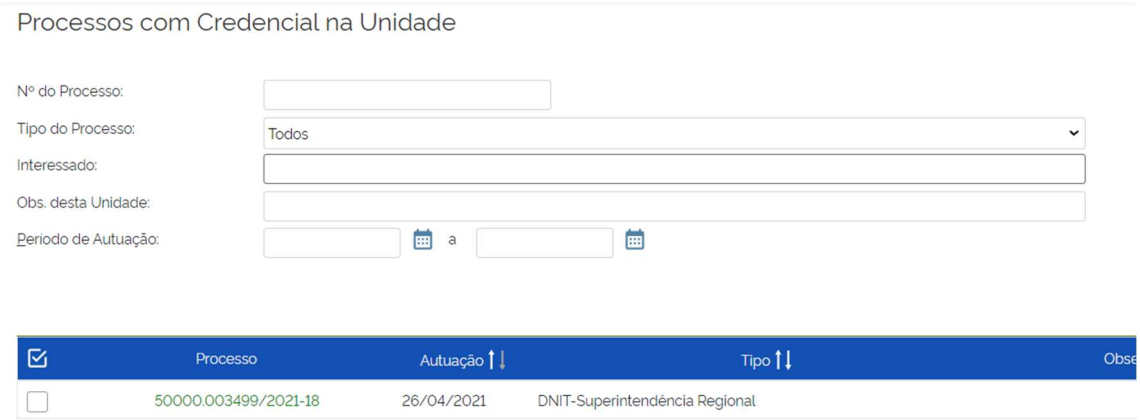
Importante: O nível de acesso pode ser atribuído ao processo ou ao documento. Ao incluir documentos no processo sigiloso, é necessária a atribuição correta do nível de acesso aos documentos, conforme o caso. Desta forma, os processos poderão conter documentos sigilosos, públicos ou restritos, conforme as informações contidas nos documentos.

A chave do processo sigiloso é na cor vermelha: 

✓ *Processos com Credencial de Acesso nesta Unidade (concluindo processos sigilosos)*



Caso o usuário possua algum processo sigiloso com credencial de acesso na unidade acessada, o ícone na figura acima será exibido. Ao clicar na funcionalidade, o sistema solicitará a senha do usuário (janela pop-up), e serão exibidos os processos que o usuário possui credencial de acesso, inclusive os processos concluídos.

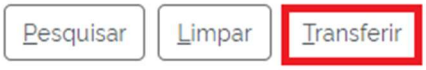


Dessa forma, depreende-se que é possível concluir um processo sigiloso e resgatá-lo, desde que não se tenha renunciado à credencial de duas formas:

1 – A busca convencional retornará o processo sigiloso desde que o usuário em questão tenha credencial;

2 – Por meio do ícone “Processos com Credencial de Acesso nesta Unidade”, conforme explicitado acima.

Importante: Na tela de “Processos com Credencial de Acesso nesta Unidade”, no canto superior direito há o ícone com a funcionalidade “Transferir”.



Apesar de estar escrito “Transferir”, não ocorre uma transferência de credencial, e sim a concessão de uma nova credencial de acesso, ou seja, o usuário que faz a ação continua tendo credencial de acesso ao processo.

✓ *Concedendo credenciais de acesso*

Acionando o ícone “gerenciando credenciais de acesso” aparecerá inicialmente o campo para selecionar o usuário a ser credenciado, e após a escolha será necessário definir a unidade de acesso e clicar em “conceder”.

O usuário credenciado receberá um e-mail automático do sistema informando do credenciamento. O processo aparecerá no “controle de processos” do usuário tarjado de vermelho caso ele não tenha acessado o processo, e azul se ele for o criador do processo ou se já tiver acessado.

Importante! Ao conceder credencial em processos sigilosos, é necessário que ambas as unidades (de quem concede credencial e de quem recebe credencial), tenham endereço de e-mail cadastrado. Caso a unidade não possua, o sistema exibirá mensagem de erro. Nessas situações, solicite que a Divisão de Gestão Documental – DIGED realize o cadastro.

✓ *Cassando / renunciando credenciais de acesso*

A cassação de credenciais é o meio capaz de cancelar o credenciamento de outro usuário. Essa funcionalidade é administrada no mesmo campo no qual são concedidas as credenciais, sendo necessário clicar no ícone no campo “ações”.

Para renunciar a uma credencial, o usuário deve clicar no ícone “renunciar credenciais de acesso” 

- ✓ *Gerenciando credenciais de assinatura*

Assinaturas em processos sigilosos também tem uma funcionalidade diferenciada em relação aos processos públicos e restritos.

No processo sigiloso, não estará disponível a funcionalidade “Bloco de Assinatura”, que permite a assinatura de membros não responsáveis pela elaboração do documento. Nesse caso, a funcionalidade correspondente chama “Gerenciar Credenciais de Assinatura”, como mostra o destaque da figura:

Ao clicar no ícone Gerenciar Credenciais de Assinatura, será exibida a tela abaixo:

Assim como na concessão de credenciais de acesso, parecerá inicialmente o campo para selecionar o usuário, e após a escolha será necessário definir a unidade de acesso e clicar em “conceder”.

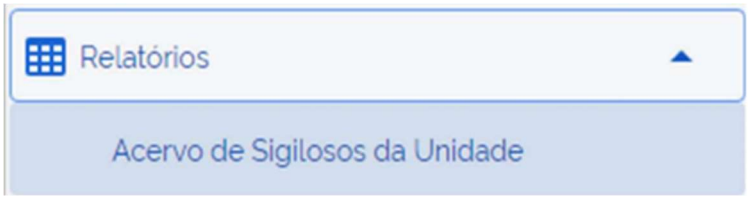
Importante: ao receber credencial de assinatura para um documento, o usuário também receberá uma credencial de acesso ao processo, ou seja, será capaz de visualizar o processo como um todo. Caso não seja desejável que ele continue com acesso ao processo, é necessário cassar tanto a credencial de assinatura quanto a de acesso.

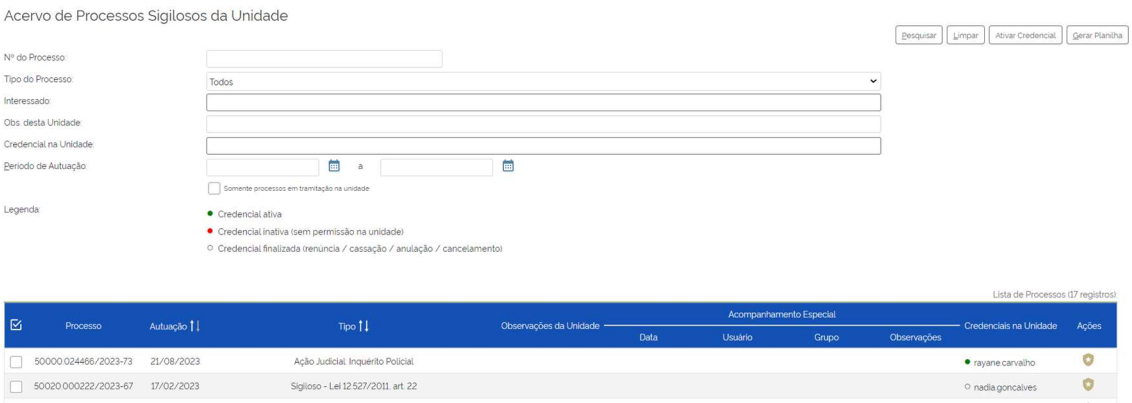
Perfil de Acervo Sigiloso na Unidade

O Perfil de Acervo de Sigilosos da Unidade deve ser solicitado pela chefia do setor, para que um usuário servidor ou com cargo comissionado possa gerenciar os processos sigilosos da unidade.

Com esse perfil, é possível visualizar a lista dos processos sigilosos que possuem ou já possuíram credencial de acesso em determinada unidade, independentemente do usuário. Importante ressaltar que se trata apenas da listagem desses processos, sem acesso ao conteúdo. É possível, contudo, ativar credencial a qualquer usuário com permissão nesta unidade, inclusive a si mesmo.

A funcionalidade fica disponível no menu “Relatórios”





A funcionalidade também oferece a possibilidade cancelar credenciais inativas na unidade. A credencial inativa é aquela em que o usuário não tem mais permissão na unidade em que recebeu credencial, portanto não consegue renunciá-la.

Há uma diferença entre o cancelamento da credencial inativa, realizado pelo perfil “Acervo de Sigilosos da Unidade”, e a cassação da credencial, que é uma ação realizada apenas por quem concedeu a credencial. Uma credencial de acesso só pode ser cassada por quem a concedeu.

REFERÊNCIAS LEGISLATIVAS

- Lei nº 12.527, de 18 de novembro de 2011, que Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991;
- Decreto nº 7.724, de 16 de maio de2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;
- Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- Lei nº 13.709, de 14 de agosto de 2016, Lei Geral de Proteção de Dados Pessoais (LGPD).

ANEXO I

MINISTÉRIO DOS TRANSPORTES	TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO – TCI Nº____/____.					
CDIC: (Código de Indexação de Documento que Contém Informação Classificada)						
PRODUTOR DA INFORMAÇÃO:						
IDENTIFICAÇÃO DO DOCUMENTO (Número Único de Protocolo – NUP, ou outra numeração que o documento tenha recebido):						
LOCALIZAÇÃO NOS AUTOS (volume e folhas):						
GRAU DE SIGILO:		Reservado		Secreto		Ultrassecreto
ASSUNTO (dados necessários para caracterização do assunto que não comprometam o sigilo):						
DESCRIÇÃO FÍSICA DO SUPORTE EM QUE A INFORMAÇÃO ESTÁ REGISTRADA (papel, cd, dvd, fita magnética, etc.):						
DATA DA CLASSIFICAÇÃO:	___/___/_____ (DD/MM/AAAA)					
DADA DA PRODUÇÃO DA INFORMAÇÃO	___/___/_____ (DD/MM/AAAA)					
PRAZO DA DURAÇÃO DO SIGILO: (seja em anos, meses ou dias, seja indicando evento que defina o seu termo)						
DATA EM QUE A INFORMAÇÃO SE TORNARÁ PÚBLICA:	___/___/_____ (DD/MM/AAAA)					
FUNDAMENTO LEGAL DA CASSIFICAÇÃO:						
RAZÕES DA CLASSIFICAÇÃO/ RECLASSIFICAÇÃO/ DESCLASSIFICAÇÃO/ REDUÇÃO DO PRAZO: (informação com mesmo grau de sigilo do documento)						
AUTORIDADE CLASSIFICADORA:	Nome:					
	Cargo:					
	Matrícula:					
DESCLASSIFICAÇÃO EM _____/_____/_____	Nome:					
	Cargo:					
	Matrícula:					
RECLASSIFICAÇÃO EM _____/_____/_____	Nome:					
	Cargo:					
	Matrícula:					
REDUÇÃO DE PRAZO EM ____/_____/_____	Nome:					
	Cargo:					
	Matrícula:					

_____
Assinatura da Autoridade Classificadora

_____
Assinatura da Autoridade Responsável pela Desclassificação

_____
Assinatura da Autoridade Responsável pela Reclassificação

_____
Assinatura da Autoridade Responsável pela Redução do Prazo

ANEXO II

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO – TCMS

[Qualificação: nome, nacionalidade, CPF, identidade (nº, data e local de expedição), filiação e endereço], perante o Ministério dos Transportes, declaro ter ciência inequívoca da legislação sobre o tratamento de informação classificada cuja divulgação possa causar risco ou dano à segurança da sociedade ou do Estado, e me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e a:

a) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo Ministério dos Transportes e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;

c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e

d) não copiar ou reproduzir, por qualquer meio ou modo: (i) informações classificadas em qualquer grau de sigilo; (ii) informações relativas aos materiais de acesso restrito do Ministério dos Transportes, salvo autorização da autoridade competente.

Declaro que [recebi] [tive acesso] ao (à) [documento ou material entregue ou exibido ao signatário], e por estar de acordo com o presente Termo, o assino na presença das testemunhas abaixo identificadas.

[Local e data]

_____

Assinatura

_____

Assinatura de testemunha identificada

_____

Assinatura de testemunha identificada

ANEXO III

<table>
<tr><td>Ministério dos Transportes</td><td colspan="6">TERMO DE AUTORIZAÇÃO
Art. 18, parágrafo único do Decreto nº 7.845/2012</td></tr>
<tr><td>CDIC: (Código de Indexação de Documento que Contém Informação Classificada)</td><td colspan="6"></td></tr>
<tr><td>IDENTIFICAÇÃO DO DOCUMENTO (Número Único de Protocolo – NUP, ou outra numeração que o documento tenha recebido):</td><td colspan="6"></td></tr>
<tr><td>GRAU DE SIGILO:</td><td></td><td>Reservado</td><td></td><td>Secreto</td><td></td><td>Ultrassecreto</td></tr>
<tr><td>MODALIDADE DE AUTORIZAÇÃO DE ACESSO: (exercício funcional, consulta, certidão, extrato ou cópia autenticada)</td><td colspan="6"></td></tr>
<tr><td colspan="7">JUSTIFICATIVA DA AUTORIZAÇÃO DE ACESSO:</td></tr>
<tr><td colspan="7">Autorizo, com fulcro no art. Art. 18, parágrafo único do Decreto nº 7.845/2012, o servidor abaixo listado
para obter acesso ao documento sigiloso aqui referenciado, condicionado à assinatura do Termo de Compromisso de Manutenção de Sigilo - TCMS.</td></tr>
<tr><td rowspan="3">IDENTIFICAÇÃO DO AUTORIZADO:</td><td colspan="2">Nome:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Cargo:</td><td colspan="3"></td></tr>
<tr><td colspan="2">Matrícula:</td><td colspan="3"></td></tr>
<tr><td colspan="7">_____
Assinatura da Autoridade Classificadora
(nome)
(cargo)
(matrícula)</td></tr>
</table>

GOVERNO FEDERAL

BRASIL

UNIÃO E RECONSTRUÇÃO