TÍTULO: **CLASSIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO DO SERPRO**

PALAVRAS – CHAVE: LAI, LGPD, informação, acesso à informação, categorização da informação, classificação da informação, tratamento, grau de sigilo, dado pessoal, dado pessoal sensível, informação pessoal, informação pessoal sensível, sigilo, privacidade e proteção de dados pessoais

ANEXO:

1 – Termo de Classificação de Informação – TCI;
2 – Formato de Apresentação do CIDIC;
3 – Termo de Compromisso de Manutenção de Sigilo – TCMS (Informações Sigilosas);
4 – Termo de Compromisso de Manutenção de Sigilo – TCMS (Informações Classificadas);
5 – Tabela de Categorização da Informação;
6 – Modelo de Matriz de Categorização da Informação;
7 – Modelo de Categorização da Informação.

PROCESSO: 12.09 – Gerenciar Segurança da Informação

1.0 FINALIDADE

Definir os procedimentos de categorização, classificação e tratamento da informação quanto ao sigilo, bem como a categorização dos dados e informações pessoais quanto à privacidade.

2.0 ÂMBITO DE APLICAÇÃO

Todos os órgãos da Empresa.

3.0 DEFINIÇÕES

Para efeito desta Norma, entende-se por:

a) ambiente restrito e controlado: espaço físico ou virtual no qual são adotadas medidas (preventivas de segurança) necessárias à limitação do acesso, bem como à efetivação desses acessos aos ativos de informação e seu respectivo controle;

b) ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso;

c) autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

d) categorização: ação coordenada corporativa de definição de categorias de sigilo ou do caráter ostensivo (incluindo a natureza do dever de transparência) das informações e dos dados – inclusive dos dados pessoais – em matrizes estabelecidas pelas Unidades Organizacionais, definindo para cada tipo de informação ou dado relevantes,

as metainformações sobre o tipo de informação, unidade organizacional, repositórios, circunstância, categorização, processo correspondente, tratamento complementar acaso existente e finalmente, tempo de retenção da informação ou do dado pessoal em questão e a forma de eliminação e/ou sanitização do ativo de informação;

e) classificação da informação: atribuição de grau de sigilo a ativos de informação nos termos da Lei nº 12.527/2011;

f) Comissão Mista de Reavaliação de Informações: comissão externa instituída nos termos do art. 46 do Decreto nº 7.724/2012, que decidirá no âmbito da administração pública federal sobre o tratamento e a classificação de informações classificadas como "ultrassecreto" e "secreto";

g) Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS: comissão interna ao SERPRO, instituída nos termos do art. 34 do Decreto nº 7.724/2012, que tem a atribuição de assessorar, opinar, propor e subsidiar a autoridade classificadora;

h) confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizada nem credenciada;

i) consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

j) controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

k) controle de acesso à informação classificada: realizado através de credencial de segurança e da demonstração da necessidade de conhecer;

l) controles de segurança: medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de hash, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros;

m) dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

n) dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

o) desclassificação: cancelamento da classificação atual de um ativo de informação pela autoridade competente ou por transcurso de prazo;

p) disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

q) documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

r) encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

s) informação: dados, processados ou não, que, contextualizados, podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

t) informação classificada em grau de sigilo: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

u) informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

v) informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo;

w) informação ostensiva: é a informação não-sigilosa relacionada com as hipóteses do dever de praticar a transparência ativa (dever de publicidade) e a transparência passiva (dever de prestar a informação solicitada);

x) integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

y) LAI: Lei de Acesso à Informação (Lei nº 12.527/2011);

z) Lei Geral de Proteção de Dados Pessoais (LGPD): Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);

aa) marcação: aposição de marca que indica o grau de sigilo da informação;

ab) necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo “necessidade de conhecer” descreve a restrição de dados que sejam considerados sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

ac) pessoa natural: é o ser humano dotado de capacidade e de titularidade de direitos e obrigações na esfera civil;

ad) RAT: registro de atividades de tratamento de dados pessoais promovido pelo Controlador, no âmbito do SERPRO, sob a orientação do Encarregado, e de acordo com a padronização por ele estabelecida, para compor ao final, o inventário de atividades de tratamento (IAT);

ae) reclassificação: alteração da classificação do ativo de informação pela autoridade classificadora;

af) recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;

ag) reservado: grau de sigilo atribuído ao ativo de informação com divulgação ou acesso restrito por 05 (cinco) anos, cujo conhecimento e manuseio por pessoas não autorizadas coloca em risco a segurança da sociedade ou do Estado;

ah) secreto: grau de sigilo atribuído ao ativo de informação com divulgação ou acesso restrito por 15 (quinze) anos, cujo conhecimento e manuseio por pessoas não autorizadas coloca em risco a segurança da sociedade ou do Estado;

ai) segredo de negócio: informação sigilosa relacionada à atividade econômica exercida pelo SERPRO cujo vazamento possa afetar o equilíbrio do negócio, seja em termos de vantagem competitiva, ou que possa de algum modo prejudicar o planejamento e a execução dos serviços, nos termos da Lei de Propriedade Industrial (Lei nº 9.297/2001, código penal, Lei nº 12.737);

aj) tarjamento: medida de proteção que possibilita a ocultação de trechos sigilosos da informação, de modo que seja assegurado ao cidadão o acesso à parte não sigilosa, conforme previsto no § 2º do art. 7 da Lei de Acesso à Informação (Lei nº 12.527/2011);

ak) tempo de retenção: tempo estabelecido para o armazenamento dos dados e informações, que devem ser eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as finalidades previstas do art. 16 da Lei 13.709/2018;

al) tratamento: toda operação realizada com dados e informações como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; e

am) ultrassecreto: grau de sigilo atribuído ao ativo de informação com divulgação ou acesso restrito por 25 (vinte e cinco) anos, cujo conhecimento e manuseio por pessoas não autorizadas coloca em risco a segurança da sociedade ou do Estado.

4.0 DETERMINAÇÕES

4.1 A informação será protegida visando a assegurar sua disponibilidade, integridade, confidencialidade e autenticidade.

4.1.1 A informação pessoal, além dos quatro aspectos gerais, será também protegida no tocante à privacidade e aos direitos fundamentais do titular.

4.1.2 O SERPRO exercerá a publicidade de seus atos como preceito geral e o sigilo como exceção, em duas modalidades diversas:

a) o sigilo das informações imprescindíveis à segurança da sociedade ou do Estado, disposto na LAI; e

b) o sigilo decorrente de legislação específica, inclusive no tocante à privacidade e proteção dos dados pessoais.

4.1.3 Para que haja clareza e para que seja eliminada qualquer ambiguidade no tocante à natureza das informações e dos dados, as unidades disponibilizarão ao CPADS suas respectivas matrizes de categorização atualizada, a partir de ação coordenada corporativa de definição das categorias de sigilo ou do caráter ostensivo (incluindo a natureza do dever de transparência) das informações e dos dados tratados – inclusive dados pessoais – em matrizes estabelecidas pelas Unidades Organizacionais.

4.1.3.1 As Unidades Organizacionais informarão, em suas respectivas matrizes, para cada tipo de informação ou de dado relevantes, as metainformações sobre "tipo de informação", "unidade organizacional", "repositórios", "circunstância", "categorização", "processo correspondente", "tratamento complementar", "tempo de retenção da informação, do dado ou dado pessoal em questão" e a "forma de eliminação e/ou sanitização do ativo de informação".

4.1.3.1.1 No caso de informação com conteúdo parcialmente sigiloso, o campo "tipo de informação" deverá ser utilizado para adição do complemento, "COM INFORMAÇÃO SIGILOSA TARJADA".

4.1.3.2 As matrizes devem ser mantidas para consulta por todos os colaboradores do SERPRO, inclusive para garantir que não haja ambiguidade ou obscuridade ou contradição no tocante à categorização de informações e de dados. E o modelo de categorização da informação adotado deve estar alinhado com as categorias da governança de dados do SERPRO, conforme modelo Anexo 7 – Modelo de Categorização da Informação.

4.1.3.3 A autoridade hierarquicamente superior ou a Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS poderão solicitar, à Unidade Organizacional competente, a reavaliação de categorização de informações ostensivas e sigilosas não classificadas.

4.2 Informação sigilosa classificada em grau de sigilo

4.2.1 As informações podem ser classificadas com grau de sigilo "ultrassecreto", "secreto" ou "reservado", em função do seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado.

4.2.1.1 A informação gerada pelo SERPRO, que não for passível de divulgação, poderá ser classificada com os seguintes graus de sigilo:

a) "secreto"; ou

b) "reservado".

4.2.2 A informação poderá ser classificada com grau de sigilo "secreto" ou "reservado" quando for considerada imprescindível à segurança da sociedade ou do Estado, e cuja divulgação e acesso irrestrito possam:

a) pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

b) prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País;

c) prejudicar ou pôr em risco informações fornecidas em caráter sigiloso por outros

Estados e organismos internacionais;

d) pôr em risco a vida, a segurança ou a saúde da população;

e) oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

f) prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;

g) 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;

h) pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou

i) comprometer as atividades de inteligência, de investigação ou de fiscalização em andamento, relacionadas com prevenção ou repressão de infrações.

4.2.3 São passíveis de classificação com grau de sigilo “secreto” e “reservado”, as informações cuja restrição, a critério da autoridade competente que as trate (conforme item 4.5.2), lhes seja conferida de modo fundado e documentado, mediante preenchimento dos documentos e observância dos requisitos adiante tratados.

4.3 Informação sigilosa protegida por legislação específica

4.3.1 As informações cujo sigilo decorre de hipóteses previstas em legislação específica, devem ser tratadas nos termos das respectivas leis.

4.3.1.1 No caso de dados e informações pessoais, o sigilo identifica-se com o dever de preservação e de proteção à privacidade e aos direitos fundamentais da Pessoa Natural e se aplica incondicionalmente no tratamento dos dados pessoais sensíveis.

4.3.1.2 As informações sigilosas estão exemplificadas no Anexo 5 – Tabela de Categorização da Informação.

4.3.2 A informação de cliente custodiada pelo SERPRO é considerada sigilosa, conforme art. 8º da Lei nº 5.615/1970, salvo se houver sido previamente classificada em grau de sigilo pelo cliente.

4.3.3 A informação que envolva potencial violação de segredo industrial, comercial ou de negócio, gerando risco ou perda efetiva de vantagem competitiva para o SERPRO, é considerada sigilosa.

4.3.4 As informações sigilosas protegidas por outras hipóteses legais de sigilo terão seu prazo de restrição de acesso de acordo com a legislação específica e, quando for o caso, observarão o tempo de retenção para sua eliminação.

4.4 Informação pessoal

4.4.1 O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e direitos individuais.

4.4.2 Às informações pessoais terão acesso restrito apenas ao titular e aos que a manipulam por necessidade de serviço, independentemente de eventual sobreposição de outras restrições, com observância do dever de privacidade da informação tratada como “dados

pessoais" e com marcação de "dados pessoais sensíveis", nos casos em que os dados pessoais sensíveis sejam de marcação obrigatória.

4.4.2.1 As informações pessoais a que se refere este item (4.4.2) são consideradas objeto de privacidade e de preservação, em termos de segurança da informação e constituem objeto de sigilo, no tocante aos "dados pessoais sensíveis" da Lei Geral de Proteção de Dados Pessoais – LGPD.

4.4.3 Ao empregado ou aos prestadores de serviço, aos estagiários, aos requisitados e aos dirigentes será facultado que solicitem o acesso às próprias informações pessoais ou funcionais.

4.4.3.1 Para o acesso às informações de terceiros deverá haver ordem judicial, previsão legal, autorização ou consentimento do titular.

4.4.4 As Unidades Organizacionais deverão definir o prazo de restrição de acesso às informações pessoais objeto de tratamento nos termos da legislação aplicável.

4.4.5 Deverão ser utilizadas, sempre que possível e necessário para a proteção dos dados pessoais não passíveis de divulgação, técnicas de tratamento adequadas e disponíveis à época, como anonimização, pseudonimização e ocultação por tarjamento.

4.4.6 As informações pessoais terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a empregados, agentes públicos legalmente autorizados e à pessoa a que elas se referirem, nos termos do art. 31 da Lei de Acesso à Informação (Lei nº 12.527/2011).

4.4.6.1 Na ausência de indicação expressa quanto ao prazo de sigilo da informação pessoal, não se pode presumir a aplicação do prazo máximo de 100 (cem) anos.

4.4.6.2 Caso não haja a indicação do prazo de restrição de acesso a informações pessoais, deve-se adotar a presunção de restrição de 15 (quinze) anos ou, quando possível, até o evento que permita determinar seu termo final. Decorrido esse prazo, o órgão responsável pela indicação da restrição, mediante requerimento, deverá realizar nova análise da situação específica da informação.

4.4.7 A negativa aos pedidos de acesso a documentos ou processos internos que contenham dados pessoais deverá ser motivadamente fundamentada, de forma específica para o caso concreto, e com a fundamentação legal respectiva, não devendo ser utilizadas fundamentações gerais e/ou abstratas para negar pedidos, sem prejuízo ao direito de solicitação de acesso à informação a qualquer tempo, nem ao exercício da autotutela administrativa.

4.4.7.1 A restrição de acesso a informações pessoais relativas à intimidade, vida privada, honra e imagem, nos termos do art. 58 do Decreto nº 7.724/2012, não poderá ser invocada quando:

a) houver o intuito de prejudicar processo de apuração de irregularidades conduzido pelo Poder Público, em que o titular das informações seja parte ou interessado;

b) as informações pessoais não classificadas estiverem contidas em conjuntos de documentos necessários à recuperação de fatos históricos de maior relevância; ou

c) for possível o tratamento e a proteção do dado por meio da ocultação, da anonimização ou da pseudonimização das informações pessoais relativas à intimidade, à vida privada, à honra e à imagem.

4.4.8 Os termos definidos para "informação pessoal", estendem-se, por força do disposto na Lei Geral de Proteção de Dados Pessoais, aos chamados dados pessoais, que se integram à categoria "dado pessoal", para todos os efeitos da Lei.

4.4.8.1 Os dados pessoais sensíveis nos termos desta norma, são categorizados como "dado pessoal sensível".

4.4.8.1.1 Em termos de sigilo e seu tratamento, o "dado pessoal sensível" equivale à informação "sigilosa".

4.5 Classificação por grau de sigilo, prazo de sigilo, reclassificação e desclassificação

4.5.1 O critério para classificação de uma informação do SERPRO nos graus de sigilo "secreto" e "reservado" deve restringir-se ao indispensável, considerando que é adotado como preceito geral a publicidade e o sigilo como exceção.

4.5.2 Terão competência para classificar, reclassificar e desclassificar as informações, no âmbito do SERPRO, por grau de sigilo:

a) "secreto": o Diretor-Presidente; e

b) "reservado": o Diretor-Presidente e os Diretores, sendo possível a delegação.

4.5.2.1 O limite de possibilidade para a delegação de que trata a alínea "b", do item 4.5.2 corresponde, nos termos da legislação, aos cargos equivalentes ao nível DAS 101.5, ou superior. É vedada a subdelegação.

4.5.2.2 É vedada a delegação da competência de classificação no grau de sigilo "secreto".

4.5.3 Os prazos máximos de classificação vigoram a partir da data de sua produção e são os seguintes, de acordo com o grau de sigilo:

a) "secreto": 15 (quinze) anos; e

b) "reservado": 5 (cinco) anos.

4.5.3.1 Transcorrido o prazo de classificação ou consumado o evento que defina o seu termo final, relativamente ao termo do prazo original, a informação será desclassificada.

4.5.3.2 A classificação das informações será reavaliada pela autoridade classificadora, por autoridade hierarquicamente superior ou por Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS, por força de ofício ou mediante solicitação, com vistas à sua reclassificação ou desclassificação.

4.5.4 Termo de Classificação da Informação – TCI

4.5.4.1 A classificação de informação nos graus de sigilo "secreto" ou "reservado" deverá ser formalizada no Termo de Classificação de Informação – TCI, conforme Anexo 1.

4.5.4.2 O Termo de Classificação de Informação – TCI, conforme Anexo 1, será mantido com o

mesmo grau de sigilo da informação classificada.

4.5.4.2.1 No caso do documento “secreto” o TCI preenchido deve ser encaminhado à Comissão Mista de Reavaliação de Informações, no prazo de 30 (trinta) dias corridos, contados a partir da data de classificação ou de sua ratificação.

4.5.4.2.2 No caso do documento “secreto” e “reservado” o TCI preenchido deve ser encaminhado à Controladoria-Geral da União, ressalvado o envio das informações das razões da classificação para última, no prazo de 30 (trinta) dias corridos, contados a partir da data de classificação ou de sua ratificação.

4.5.4.3 O Termo de Classificação de Informação – TCI, conforme Anexo 1, deverá conter o histórico dos eventos relativos à ratificação, desclassificação e reavaliação do grau de sigilo da informação.

4.5.4.4 Cada documento classificado com grau de sigilo “secreto” ou “reservado”, deverá possuir uma numeração própria, conhecida como “Código de Indexação de Documento que contém Informação Classificada (CIDIC)”, conforme Anexo 2 – Formato de Apresentação do CIDIC.

4.5.4.4.1 O código CIDIC é um código exclusivamente numérico e é gerado pela Área responsável pela gestão da publicação do rol de informações classificadas e desclassificadas e de relatórios estatísticos associados.

4.6 Proteção e controle de informações sigilosas

4.6.1 A geração, o acesso, a divulgação e o tratamento de informação sigilosa, classificada ou não, ficarão restritos às pessoas que tenham necessidade de conhecê-la por dever de ofício e que sejam devidamente autorizadas.

4.6.2 O acesso à informação sigilosa, classificada ou não, cria a obrigação para aquele que a obteve de resguardar seu sigilo.

4.6.3 A pessoa física ou entidade privada que, em razão de qualquer vínculo com o SERPRO, executar atividade de tratamento de informação sigilosa, adotará as providências necessárias para que seus empregados, contratados, prepostos ou representantes observem as condições estabelecidas entre as partes em termo de sigilo, conforme modelo do Anexo 3 – Modelo de Termo de Compromisso de Manutenção de Sigilo – TCMS (Informações Sigilosas).

4.6.3.1 No caso de informações classificadas em grau de sigilo, o TCMS deverá seguir o modelo do Anexo 4 – Modelo de Termo de Compromisso de Manutenção de Sigilo – TCMS (Informações Classificadas).

4.6.4 Nas reuniões em que serão produzidas ou manipuladas informações sigilosas, classificadas ou não, deverão ser adotados controles de segurança para acesso ao ambiente, aos documentos, às anotações, às mídias e aos demais recursos utilizados.

4.6.5 Caberá às Unidades Organizacionais adotar o adequado tratamento a ser dado às informações sigilosas, classificadas ou não, e zelar para que sejam armazenadas e arquivadas em ambiente com acesso restrito e controlado.

4.6.6 No caso dos documentos classificados com grau de sigilo, a despeito da obrigatória marcação e da obrigatória forma de tratamento, a origem do sigilo decorre da Lei e da natureza da informação e não da "marcação", em si.

4.6.7 Para os documentos contendo informação sigilosa não-classificada, o sigilo decorre de Lei, enquanto sua marcação e tratamento, no âmbito do SERPRO, são definidos pelo Titular da Unidade Organizacional, em cada caso concreto.

4.7. Marcação de ativos de informação sigilosa

4.7.1 Marcação de documentos classificados como "secreto" e "reservado"

4.7.1.1 Documentos classificados devem receber a seguinte marcação:

a) em todas as páginas do documento e nas capas, se houver, no cabeçalho e no rodapé;

b) as páginas devem ser numeradas seguidamente, devendo cada uma conter, também, a indicação do total de páginas que compõem o documento; e

c) a marcação em extratos de documentos, rascunhos, esboço e desenho sigiloso deve obedecer ao prescrito nos itens anteriores.

4.7.1.2 Os meios de armazenamento portáveis de dados (tipo pendrive, DVD e outros) devem receber a marcação obrigatória correspondente à informação ali contida em local visível e adequado, sem prejuízo dos devidos controles de acesso.

4.7.1.3 Os meios de armazenamento de informação classificada em repositório não-portável receberão a marcação obrigatória pela forma mais adequada, inclusive mediante aplicação de rótulo na interface do controle de acesso respectivo.

4.7.2 Marcação de documentos sigilosos não classificados

4.7.2.1 Os documentos que contenham informações sigilosas protegidas por legislação específica, serão tratados nos termos da Lei que rege tal hipótese de sigilo, embora possam, a critério do Titular da Unidade Organizacional, receber marcação e tratamento específicos compatíveis com a Lei de origem e com a natureza da informação protegida.

4.7.2.1.1 A marcação para os documentos de que trata o item 4.7.2.1 poderá ser feita facultativamente, a critério do Titular da Unidade Organizacional, mediante o uso da expressão "sigiloso", caso não se trate de dados pessoais, hipótese na qual se utilizará a expressão "dado pessoal sensível".

4.7.2.1.2 A marcação, caso seja determinada, deve ser feita na capa e no cabeçalho de todas as páginas do documento.

4.7.2.2 Apesar do caráter facultativo da marcação, os seguintes pontos devem ser observados:

a) adequação do caso concreto com a Lei que o fundamenta;

b) ausência de ambiguidade na marcação;

c) a prevenção de marcações paradoxais;

d) a prevenção de qualquer confusão com as marcações legais obrigatórias (informação sigilosa classificada) e com as demais marcações opcionais (informação sigilosa não classificada);

e) tratamento coerente com a hipótese de sigilo; e

f) abstenção de uso da palavra "sigiloso" para qualquer outra hipótese restritiva que não se enquadre nas hipóteses constantes do Anexo 5 – Tabela de Categorização da Informação.

4.7.2.3 A decisão discricionária sobre aplicar ou não a marcação de que trata o subitem anterior não implica dúvida sobre a natureza sigilosa do objeto de marcação, que decorre, em qualquer caso, das respectivas Leis.

4.7.2.4 O Titular da Unidade Organizacional deve zelar, para que seus colaboradores não atuem de forma contraditória com o tratamento da informação sigilosa, aplicando tratamento adequado também aos esboços, rascunhos, provas, lembretes e informações paralelas e correlatas ao objeto de sigilo.

4.7.2.5 Os meios de armazenamento portáveis de dados podem opcionalmente receber a marcação correspondente à informação ali contida em local visível e adequado, sem prejuízo dos devidos controles de acesso.

4.7.2.6 Os meios de armazenamento de informação sigilosa em repositório não-portável receberão a marcação facultativa pela forma mais adequada, inclusive mediante aplicação de rótulo na interface do controle de acesso respectivo.

4.7.2.6.1 Na hipótese de o Titular da Unidade Organizacional definir por executar marcação de dado pessoal sensível, essa marcação será feita com a terminologia "dado pessoal sensível".

4.7.2.6.2 Na hipótese de o Titular da Unidade Organizacional definir por executar marcação de dado pessoal (não-sensível), essa marcação será feita com a terminologia "dado pessoal".

4.8 Tratamento de documentos sigilosos

4.8.1 O tratamento da informação sigilosa não classificada, nela incluída a informação pessoal protegida pelas regras de privacidade e pelo sigilo de dados e informações pessoais sensíveis, deve ser objeto de cuidado e de definições, ritos e processos estabelecidos pelo Titular da Unidade Organizacional, de modo a atender à demanda da Lei específica e a não frustrar os princípios fundantes estabelecidos na Lei de Acesso à Informação e na Lei Geral de Proteção de Dados Pessoais, o que implica guarda adequada, uso de mecanismos de proteção, criptografia, quando seja o caso, adoção de ambiente restrito e controlado.

4.8.2 O Titular da Unidade Organizacional que constitua repositório inadequado à guarda segura de informação sigilosa sujeita-se à responsabilidade decorrente de sua escolha.

4.8.3 No caso específico da informação pessoal sensível (sigilo) é recomendável que o titular

da Unidade Operacional opte por determinar sua marcação nos documentos e repositórios, dadas as dimensões financeira e econômica das possíveis consequências do tratamento inadequado.

4.9 Uso e disseminação de documentos sigilosos

4.9.1 Uso e disseminação de documentos classificados

4.9.1.1 Os documentos classificados como “secreto” ou “reservado”, quando da expedição e comunicação, devem obedecer às seguintes prescrições:

a) ser acondicionados em envelopes duplos;

b) não constar qualquer indicação do grau de sigilo ou do teor do documento no envelope externo;

c) ser apostos o destinatário e a marcação “secreto” ou “reservado”, de modo a serem identificados logo que removido o envelope externo;

d) fechar, lacrar e expedir o envelope interno mediante recibo, que deve indicar, necessariamente, remetente, destinatário e número ou outro indicativo que identifique o documento; e

e) inscrever a palavra PESSOAL no envelope externo sempre que o assunto for considerado de interesse exclusivo e pessoal do destinatário.

4.9.1.2 A transmissão de documento classificado como “secreto” ou “reservado” pode ser feita por meios digitais, desde que sejam utilizados recursos de criptografia compatíveis com o grau de sigilo do documento.

4.9.1.3 É vedado o uso de recursos criptográficos não autorizados ou não homologados pelo SERPRO.

4.9.1.4 O acesso às áreas, instalações e materiais que contenham informações classificadas como “secreto” e “reservado” ou que demandem proteção deve ser regulado e tratado de forma compatível, com acesso restrito e controlado.

4.9.2 Uso e disseminação de documentos sigilosos não classificados

4.9.2.1 As informações sigilosas não classificadas podem ser acessadas pelos destinatários credenciados, de acordo com decisão do agente gerador do documento sigiloso e limitado pelos sistemas de controle de acesso, inclusive criptografia comum autorizada e homologada, quando for o caso.

4.9.2.2 Os documentos sigilosos são de circulação interna controlada no âmbito SERPRO e de acesso restrito aos que tenham necessidade de saber e atributo de acesso.

4.9.2.2.1 Em situações excepcionais, o agente gerador do documento sigiloso pode encaminhar o documento a destinatários externos ao SERPRO, com os devidos controles de entrega e manutenção de confidencialidade.

4.9.2.2.2 A informação que contenha parte do conteúdo sigiloso, e seja necessária a

divulgação, deverá ser utilizado o tarjamento como medida de proteção.

4.10 Reprodução de documentos classificados

4.10.1 A reprodução do todo ou de parte de documento “secreto” ou “reservado” deve ter o mesmo grau de sigilo do documento original.

4.10.2 O responsável pela produção ou reprodução de documento “secreto” ou “reservado” deve providenciar a eliminação de notas manuscritas, carbonos, provas ou qualquer outro recurso, que possam dar origem a cópia não-autorizada do todo ou parte.

4.10.3 Sempre que a preparação, impressão ou, se for o caso, reprodução de documento “secreto” ou “reservado” for efetuada em tipografias, impressoras, oficinas gráficas ou similares, essa operação deve ser acompanhada por agente credenciado ou que tenha assinado o TCMS, que será responsável pela garantia do sigilo durante a confecção do documento, observado o disposto no item anterior.

4.10.4 A reprodução do todo ou de parte de mídia magnética, óptica e eletrônica contendo dados classificados como “secreto” ou “reservado” deve ter o mesmo grau de sigilo do original.

4.10.5 O responsável pela reprodução deve ser agente credenciado ou que tenha assinado o TCMS, e deve manter o sigilo da operação, observado o disposto no item anterior.

4.10.6 Os arquivos temporários porventura gerados durante o processo de produção do documento devem ser eliminados ao final da operação.

4.11 Registro, tramitação e guarda de informação classificada

4.11.1 As informações classificadas com grau de sigilo “ultrassecreto”, “secreto” ou “reservado” em sistemas de informação devem:

a) ser armazenadas em equipamento, ambiente ou estrutura que ofereça grau de segurança compatível com grau de sigilo;

b) utilizar sistema de tecnologia da informação atualizado de forma a prevenir ameaças de quebra de segurança;

c) utilizar canal seguro isolado física ou logicamente, além de controle de acesso adequado se o equipamento, ambiente ou estrutura estiver conectado à Internet ou rede interna;

d) utilizar recursos criptográficos adequados ao grau de sigilo;

e) garantia de autenticidade do usuário por meio de certificado digital; e

f) manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.

4.11.2 Cabe ao responsável pelo recebimento de documento “ultrassecreto”, “secreto” ou “reservado”:

a) verificar a integridade e registrar, se for o caso, indícios de violação ou de qualquer irregularidade na correspondência recebida, dando ciência do fato ao seu superior hierárquico e ao destinatário, o qual deve informar imediatamente ao remetente;

b) proceder o registro do documento e o controle de sua tramitação, mediante cadastramento enumerado no sistema corporativo de recebimento de correspondência externa sem intromissão ou violação de seu conteúdo ou de seu sigilo classificado;

b1) o tratamento dado à correspondência classificada recebida deve garantir os mesmos requisitos de segurança prescritos na Lei e na regulamentação para tramitação segura da informação classificada em meios físicos; e

c) abster-se de abrir o envelope interno da correspondência, que deve ser aberto exclusivamente pelo destinatário, seu representante autorizado ou autoridade competente hierarquicamente superior;

c1) nos casos em que o envelope interno traga a marca "PESSOAL", representantes ou autoridades hierárquicas não estarão autorizados ao acesso; e

d) comunicar o recebimento da correspondência ao remetente no menor prazo possível;

e) manter ou guardar os documentos sob condições especiais de segurança, pela forma protetiva previamente definida para essa finalidade; e

f) transmitir a guarda ou custódia de documentos, devidamente conferidos, quando da passagem ou transferência de responsabilidade em caso de substituição dos responsáveis.

4.12 Avaliação, preservação e eliminação da informação classificada

4.12.1 A atividade de avaliação quanto à manutenção da classificação original, reclassificação ou desclassificação deve ser realizada de modo idêntico ao descrito no item 4.5.

4.12.2 As informações classificadas e seus respectivos documentos, não devem ser eliminados.

4.13 Eliminação de informação e documentos sigilosos não-classificados

4.13.1 A eliminação de informações sigilosas não-classificadas ou de seu respectivo documento, somente pode ser feita de acordo com os procedimentos e regras de preservação de documentos definidos pela área responsável pela gestão documental e arquivística.

4.13.2 A eliminação a que se refere este item envolve os procedimentos de deleção segura (para documentos em meio eletrônico) e de trituração física (para documentos em papel).

4.13.3 As informações pessoais sujeitam-se aos prazos definidos para o ciclo de vida

documental que, em qualquer hipótese, são superiores aos prazos legais de guarda.

4.14 Tempo de retenção de dados pessoais e dados pessoais sensíveis

4.14.1 O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

a) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

b) fim do período de tratamento;

c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), resguardado o interesse público; ou

d) determinação da autoridade nacional, quando houver violação ao disposto na Lei Geral de Proteção de Dados Pessoais.

4.14.2 Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei Geral de Proteção de Dados Pessoais; e

c) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que adequadamente protegidos os dados nos termos da Lei.

4.15 Do tratamento da informação ostensiva

4.15.1 Sem prejuízo do princípio da transparência, que constitui regra na Lei de Acesso à Informação, e no sentido de proteger a informação pública ostensiva com dever de transparência passiva, de acordo com a oportunidade e conveniência, deve ser considerada a descrição e controle:

a) das informações de uso interno; e

b) das informações cuja disseminação não seja conveniente ao negócio.

4.15.2 Na hipótese de haver demanda de informação do tipo tratado em 4.15.1 por via diferente do Sistema de Informação ao Cidadão – SIC do SERPRO, o empregado que receber a demanda reportar-se-á, pelo percurso hierárquico da respectiva área, ao Titular da Unidade Organizacional para que este, consultando as instâncias técnicas e hierárquicas correlatas, adote as providências necessárias ao melhor tratamento possível da demanda.

4.15.3 Se a demanda recair sobre dados pessoais ou dados pessoais sensíveis, o Titular da Unidade Organizacional deverá se reportar à pessoa do Encarregado formalmente designado para atuar como tal, nos termos da Lei.

5.0 DISPOSIÇÕES FINAIS

5.1 Qualquer empregado que venha a encontrar, extraviar ou constatar o extravio de documento ou informação sigilosa deverá comunicar imediatamente o fato à chefia imediata ou ao responsável pela custódia do documento ou da informação.

5.2 Os empregados responsáveis pela custódia de documentos, materiais, áreas e informações de natureza sigilosa estarão sujeitos às regras referentes ao sigilo profissional, em razão do ofício e às regras referentes ao Código de Ética do SERPRO.

5.3 A cessão de documentos sigilosos à Administração Pública direta e indireta deverá ser avaliada pelo Titular da Unidade Organizacional, sob orientação da Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS.

5.4 O tratamento de informações pessoais e de dados pessoais deverá estar em conformidade com a Política SERPRO de Privacidade e Proteção de Dados (PPPD) e com o Programa de Governança em Privacidade e Proteção de Dados Pessoais do SERPRO, o que conduz a titularidade e a responsabilidade de seu trato à figura do Encarregado formalmente designado para atuar como tal.

5.5 Os recursos de criptografia citados nesta Norma deverão ser homologados pela Empresa, de modo geral, e, no caso de tratamento de informações classificadas em grau de sigilo, deverá ser utilizada criptografia baseada em algoritmo de Estado para cifração e decifração das informações classificadas com grau de sigilo “secreto” e “reservado”.

5.6 Competirá às Unidades Organizacionais da Empresa definir as informações sigilosas e pessoais inerentes à área de atuação, o perfil de acesso e o tratamento associado.

5.6.1 A matriz de categorização das informações que consolida essas informações deve ser revisada anualmente e mantida atualizada pelas Unidades Organizacionais, conforme o padrão adotado no Anexo 6 – Modelo de Matriz de Categorização da Informação.

5.7 Competirá às Unidades Organizacionais da Empresa gestoras de sistemas e de ferramentas de suporte que sustentam a geração, a tramitação e a armazenagem de informação promover as adequações necessárias à adequação a esta Norma.

5.8 O responsável pela gestão e publicação do rol de informações classificadas e desclassificadas providenciará perante as áreas competentes a aquisição ou desenvolvimento da ferramenta ou solução que gerará o número CIDIC de que trata o item 4.5.4.4.1, com oficialidade e auditabilidade, para efeito de cumprimento da lei e garantia de seus controles.

5.9 É vedado o uso de informação sigilosa em trabalhos acadêmicos ou técnico-científicos paralelos ao negócio do SERPRO, ainda que de boa-fé.

5.9.1 Havendo dúvida sobre a incidência de sigilo legal, o interessado poderá obter do Titular da Unidade Organizacional competente avaliação prévia, crítica e formal sobre a incidência de sigilo.

5.9.1.1 No caso de informações pessoais, de dados pessoais ou de dados pessoais sensíveis, o Encarregado formalmente designado para o tema será o interlocutor obrigatório para o saneamento dessas dúvidas.

5.10 A informação sigilosa ou a informação classificada que tramitem em meio digital, quando disponível tecnologia corporativa para tanto, deverá ser tratada mediante

implementação, gerenciamento e manutenção de metadados que garantam o controle de acesso, tempo de retenção, segregação de papéis, dentre outros atributos, de modo a que a crítica e identificação do documento sigiloso, como tal, ocorra necessariamente antes de acessos acidentais ou equívocos, prevenindo indisponibilidades, acessos indevidos e falhas de reavaliação do sigilo.

5.11 Caberá a unidade responsável pela Gestão Documental no SERPRO orientar quanto ao Plano de Classificação e a Tabela de Temporalidade, assim como a guarda, eliminação e descarte de documentos.

5.12 Caberá a unidade responsável pela Privacidade e Proteção de Dados Pessoais orientar quanto aos aspectos relativos à categorização e ao tratamento da informação pessoal.

5.13 Os empregados que infringirem esta Norma estão sujeitos às penalidades constantes na Norma que trata do Regime Disciplinar – Apuração de Responsabilidades e Aplicação de Penalidades.

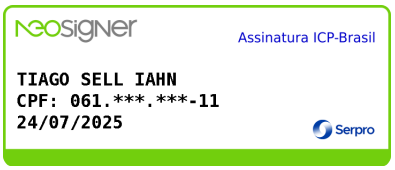
5.14 O Anexo 5 – Tabela de Categorização da Informação traz o detalhamento das categorias de informação desta Norma.

5.15 Os modelos dos anexos editáveis, mencionados nesta norma, estão disponíveis na área de Gerenciamento de Documentos/Repositório da ferramenta corporativa de Gestão Integrada de Processos – INTEGRA.

5.16 Os casos omissos serão tratados pela Superintendência da Segurança da Informação – SUPSI.

5.17 Este documento substituirá a Norma SG 005, versão 09, de 19 de setembro de 2022.

Diretor de Operações



Superintendente de Segurança da Informação

ÓRGÃO/REDATOR: DIOPE/SUPSI/SIGSC/SIRSC/rog

Serpro

ANEXO

NÚMERO	VERSÃO
1	1

TÍTULO

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO – TCI

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

Termo de Classificação de Informação – TCI

Unidade do Serpro (1)	Código de Indexação (2)	Data de Produção (3)
Grau de Sigilo (4) ☐ Secreto ☐ Reservado	Categoria (5)	
Tipo de Documento (6) ☐ Ofício ☐ Carta ☐ Memorando ☐ Relatório ☐ Outro :Especificar)		
Prazo da Restrição de Acesso (7)	Data de Classificação (8)	
Fundamento Legal para Classificação (9)		
Razões da Classificação (10)		
Assunto (11)		
Autoridade Classificadora (12) Nome: _____ Cargo: _____ Assinatura: _____		
Autoridade Ratificadora (13) Nome: _____ Cargo: _____ Assinatura: _____		
Desclassificação em (14) _____/_____/_____	Nome: _____ Cargo: _____ Assinatura: _____	
Reclassificação em (15) _____/_____/_____	Nome: _____ Cargo: _____ Assinatura: _____	
Redução de prazo em (16) _____/_____/_____	Nome: _____ Cargo: _____ Assinatura: _____	
Prorrogação do prazo em (17) _____/_____/_____	Nome: _____ Cargo: _____ Assinatura: _____	

TÍTULO

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO – TCI

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

(Instrução de Preenchimento)

(1) Unidade do SERPRO: nome da unidade/área de emissão, ou responsável pela desclassificação, reclassificação, redução do prazo ou CPADS.

(2) Código de Indexação: conforme Anexo 2.

(3) Data de Produção: DD/MM/AAAA (data de criação do documento).

(4) Grau de Sigilo: secreto ou reservado.

(5) Categoria: categoria na qual se enquadra a informação de acordo com o VCGE – Vocabulário Controlado de Governo Eletrônico, conforme Anexo 2 – Formato de apresentação do CI-DIC.

(6) Tipo de Documento: ofício, carta, memorando, relatório ou outro documento que deve ser especificado.

(7) Prazo da Restrição de Acesso: DD/MM/AAAA

(8) Data de Classificação: DD/MM/AAAA, data em que a autoridade competente classificou a informação.

(9) Fundamento Legal para Classificação: indicar o inciso do Art. 23 da Lei No. 12.527/2011 (item 4.2.2.1 da Norma).

(10) Razões da Classificação: justificativa da classificação, desclassificação, reclassificação, ou redução do prazo.

(11) Assunto: assunto a que se refere a informação, com a descrição de elementos mínimos que permitam a identificação do tema de que trata a classificação.

(12) Autoridade Classificadora, contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato.

(13) Autoridade Ratificadora (quando aplicável), contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato.

(14) Desclassificação em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável desclassificou a informação, contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato;
- Assinatura: assinatura da autoridade responsável pelo ato.

(15) Reclassificação em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável reclassificou a informação, contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato;

- Assinatura: assinatura da autoridade responsável pelo ato.

(16) Redução do prazo em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável reduziu o prazo da classificação da informação, contemplando:

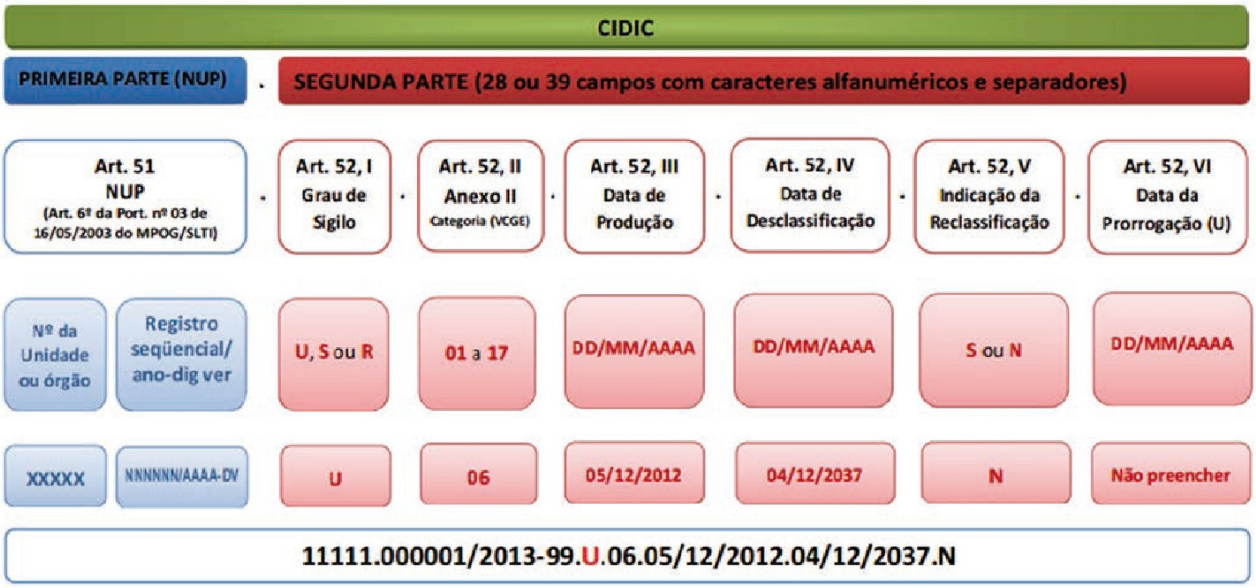
- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato;
- Assinatura: assinatura da autoridade responsável pelo ato.

(17) Prorrogação do prazo em (quando aplicável): DD/MM/AAAA, data em que a autoridade responsável prorrogou o prazo da classificação da informação, contemplando:

- Nome: nome completo da autoridade responsável pelo ato;
- Cargo: cargo da autoridade responsável pelo ato;
- Assinatura: assinatura da autoridade responsável pelo ato.

Formato de Apresentação do Código de Indexação de Documento que Contém Informação Classificada (CIDIC)

1. O formato de apresentação do Código de Indexação de Documento que contém Informação Classificada (CIDIC) obedece às regras constantes neste Anexo, de acordo com os artigos 50 a 54 do Decreto nº 7.845/2012, cujo modelo é exemplificado é mostrado a seguir:



2. A 1ª parte do CIDIC corresponde ao Número Único de Protocolo – NUP do documento que contém a informação.

3. A 2ª parte do CIDIC é separada da 1ª parte por um "." e contém o seguinte formato:

a) Grau de sigilo: um caractere alfabético ("U", "S" ou "R"), de acordo com o grau de sigilo ultrassecreto (U), secreto (S) ou reservado (R), com as iniciais na cor vermelha, quando possível.

b) Categoria: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme tabela a seguir.

CATEGORIAS	CÓDIGO NUMÉRICO
Agricultura, extrativismo e pesca	1
Ciência, informação e Comunicação	2
Comércio, Serviços e Turismo	3
Cultura, Lazer e Esporte	4
Defesa e Segurança	5

Economia e Finanças	6
Educação	7
Governo e Política	8
Habitação, Saneamento e Urbanismo	9
Indústria	10
Justiça e Legislação	11
Meio ambiente	12
Pessoa, família e sociedade	13
Relações internacionais	14
Saúde	15
Trabalho	16
Transporte e trânsito	17

c) Data de produção da informação classificada: registro da data de produção da informação classificada, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);

d) Data de desclassificação da informação classificada em qualquer grau de sigilo: registro da potencial data de desclassificação da informação classificada, efetuado no ato da classificação, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos).

e) Indicação de reclassificação: indicação de ocorrência ou não, S (sim) ou N (não), de reclassificação da informação classificada, respectivamente, conforme as seguintes situações:

e1) Reclassificação da informação: resultante de reavaliação ou primeiro registro da classificação; e

e2) Indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ultrassecreto, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível.

4. Os separadores utilizados serão: "." e "/" (este último, para as datas).

5. Para as informações classificadas no grau reservado e secreto, a 2ª parte do CIDIC terá sempre 28 (vinte e oito) posições com caracteres alfanuméricos e separadores.

6. Para as informações classificadas no grau ultrassecreto, a 2ª parte do CIDIC terá 28(vinte e oito) posições com caracteres alfanuméricos e separadores, enquanto não ocorrer prorrogação do prazo do sigilo.

7. Quando ocorrer a prorrogação do prazo de sigilo da informação classificada no grau ultrassecreto, a nova data deverá constar no final da 2ª parte do CIDIC, totalizando 39 (trinta e nove) posições com caracteres alfanuméricos e separadores.

Termo de Compromisso de Manutenção de Sigilo – TCMS

Eu, [nome completo da pessoa], [nacionalidade], CPF nº [número do CPF], documento de identificação nº [número do documento de identificação], emitido pelo [nome do Órgão Expedidor] na data [DD/MM/AAAA], domiciliado em [endereço], declaro perante o Serviço Federal de Processamento de Dados – SERPRO, ter ciência da legislação sobre o tratamento de informação sigilosa (Lei n° 12.527/2011, Decreto nº 7.724/2012 e Decreto nº 7.845/2012), assim entendida aquela informação cuja divulgação ou acesso indevido possam causar risco ou dano à segurança das informações da Empresa e de seus clientes, comprometendo-me a:

a) tratar as informações sigilosas ou os materiais de acesso restrito que me forem fornecidos pelo SERPRO e garantir o tratamento adequado, em conformidade, com as restrições e cuidados impostos pelas ferramentas corporativas;

b) preservar o conteúdo das informações sigilosas 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 sigilosas, ou dos materiais de acesso restrito;

d) não copiar ou reproduzir, por qualquer meio ou modo: (i) informações sigilosas; (ii) informações relativas a materiais de acesso restrito do SERPRO, e (iii) dados pessoais de qualquer natureza, salvo com autorização formal da autoridade competente; e

e) praticar as condutas de conformidade acima descritas em qualquer acesso lógico ou físico que lhe seja garantido por meio de credenciamento aos ambientes do SERPRO.

Declaro estar ciente de que o presente compromisso é firmado a partir deste momento e que o dever de sigilo não depende de qualquer manifestação formal a cada acesso ou compartilhamento que ocorra, subscrevo-o, para todos os fins de direito.

[Local] – [UF], [dia] de [mês] de [ano].

_____

[NOME COMPLETO DA PESSOA]

Termo de Compromisso de Manutenção de Sigilo – TCMS

Eu, [nome completo da pessoa], [nacionalidade], CPF nº [número do CPF], documento de identificação nº [número do documento de identificação], emitido pelo [nome do Órgão Expedidor] na data [DD/MM/AAAA], situado em [endereço], perante o Serviço Federal de Processamento de Dados – SERPRO, declaro ter ciência da legislação sobre o tratamento de informação classificada (Lei n° 12.527/2011, Decreto nº 7.724/2012 e Decreto nº 7.845/2012) cuja divulgação ou acesso indevido pode causar risco ou dano à segurança das informações da Empresa e de seus clientes, comprometendo-me a guardar o sigilo e a:

a) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo SERPRO 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 SERPRO, salvo autorização da autoridade competente.

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

[Local] – [UF], [dia] de [mês] de [ano].

_____

[NOME COMPLETO DA PESSOA/ASSINATURA]

_____

[NOME COMPLETO DA TESTEMUNHA 1]

_____

[NOME COMPLETO DA TESTEMUNHA 2]

Serpro

ANEXO

NÚMERO	VERSÃO
5	1

TÍTULO

TABELA DE CATEGORIZAÇÃO DA INFORMAÇÃO

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

INFORMAÇÃO OSTENSIVA

TIPO DE INFORMAÇÃO	CARACTERÍSTICA	CATEGORIZAÇÃO DA INFORMAÇÃO	DETALHAMENTO	FUNDAMENTO LEGAL	TRATAMENTO
Informação cujo sigilo não é protegido por lei:				LAI Art. 6º., I e II	
OSTENSIVA	INFORMAÇÃO SEM AMPARO LEGAL DE SIGILO	OSTENSIVA (ATIVA)	Publicação obrigatória ou discricionária.	LAI, Art. 2º., parágrafo único	PUBLICAR AS INFORMAÇÕES DE ACORDO COM A LAI OU A CRITÉRIO DO SERPRO
		OSTENSIVA (PASSIVA)	Solicitação de informação via SIC (Sistema de Informação ao Cidadão). Sem prejuízo do princípio da transparência, que constitui regra na Lei de Acesso à Informação, deve ser considerada a descrição e controle das informações de uso interno e das informações cuja disseminação não seja conveniente ao negócio.	LAI, Art. 3o., parágrafo único, Art. 6o., I LAI, Art. 6o. II Tratamento de contenção e preservação, sem violação ao princípio da transparência.	RESPONDER DEMANDA DO SIC AO RECEBER DEMANDA FORA DO SIC INFORMAR AO TITULAR DA UNIDADE, PARA QUE ESTE ADOTE AS PROVIDÊNCIAS CABÍVEIS. (4.15) SE FOR DEMANDA DE DADOS PESSOAIS (SENSÍVEIS OU NÃO) O TITULAR DA UNIDADE DEVERÁ SE REPORTAR AO ENCARREGADO, FORMALMENTE DESIGNADO. (4.15)

Serpro

ANEXO

NÚMERO	VERSÃO
5	1

TÍTULO

TABELA DE CATEGORIZAÇÃO DA INFORMAÇÃO

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

INFORMAÇÃO SIGILOSA

TIPO DE INFORMAÇÃO	CARACTERÍSTICA	CATEGORIZAÇÃO DA INFORMAÇÃO	DETALHAMENTO	FUNDAMENTO LEGAL	TRATAMENTO
Informação cujo sigilo é protegido por legislação especifica:				LAI Art. 6o., III, LAI Art. 22	
SIGILOSA	INFORMAÇÃO NÃO CLASSIFICADA EM GRAU DE SIGILO NA LAI	SIGILOSA	SIGILO FISCAL	Lei No. 5.172, Art. 198. LAI, Art. 22	MARCAÇÃO: FACULTATIVA. SE FOR MARCAR USAR "SIGILOSO" NO CABEÇALHO EM TODAS AS PÁGINAS. (4.7.2) MANIPULAÇÃO: ACESSO RESTRITO APENAS AOS CREDENCIADOS QUE POSSUEM NECESSIDADE DE SERVIÇO OU DEVER DE OFÍCIO. (4.6) GUARDA: INFORMAÇÃO SIGILOSA DEVE TER ACESSO CONTROLADO (FÍSICO E/OU LÓGICO). (4.8 e 4.9.2) ELIMINAÇÃO: DELEÇÃO SEGURA OU TRITURAÇÃO FÍSICA APÓS AUTORIZAÇÃO DO TITULAR DA UO, CONSIDERANDO OS PROCEDIMENTOS DE GESTÃO DOCUMENTAL DEFINIDOS (4.13)
			SIGILO BANCÁRIO	Lei 105/01, Art. 1o. LAI, Art. 22	
			SIGILO INVESTIGATÓRIO	Lei 9.784, Art. 2º e 46. LAI, Art. 22	
			SIGILO COMERCIAL	Lei 6.404, Art. 155. LAI, Art. 22	
			SEGREDO DE JUSTIÇA	CPC Lei 5.869 + CPP DL 3.689, Art. 201. LAI Art. 22	
			SEGREDO PROFISSIONAL	CPP DL 3.689, Art. 20	
			SIGILO INQUÉRITO E SEGREDO DE JUSTIÇA	Arts. 5º. LX	
			SIGILO CONTÁBIL	L.10.406, CC Art. 1.190 e 1.191	
			SIGILO EMPRESARIAL (NA RECUPERAÇÃO)	L.11.101, Recup. Art.169	
			SIGILO ADVOGADO – CLIENTE	L. 8.906 34, VII e 7º., II, XIX	
			SIGILO JORNALISTA	CF, sigilo da fonte, Art. 5º., XIV	
			SIGILO ASSISTENTE SOCIAL	Lei 8.662 + Estatuto, Art. 2º., d + Cap. 5º.	
			SIGILO POSTAL	LEI Nº 6.538, de 22 de junho de 1978.	
			SIGILO MÉDICO	RES. CFM No. 999/80 Art. 102 e segs.	

INFORMAÇÃO SIGILOSA

TIPO DE INFORMAÇÃO	CARACTERÍSTICA	CATEGORIZAÇÃO DA INFORMAÇÃO	DETALHAMENTO	FUNDAMENTO LEGAL	TRATAMENTO
Informação cujo sigilo é protegido por legislação específica:				LAI Art. 6o., III, LAI Art. 22	
SIGILOSA	INFORMAÇÃO NÃO CLASSIFICADA EM GRAU DE SIGILO NA LAI	SIGILOSA	SIGILO SEGREDO DE NEGÓCIO	LAI – Lei 12.527, Art. 22. LPI – L. 9.279/96 Art. 195, XI, XII, XIV. Art. 206. Código Penal, Art. 154, 154-A, § 3o. Art. 325 (funcional). CLT, Art. 482, CLT, Art. 482, g	MARCAÇÃO: FACULTATIVA. SE FOR MARCAR USAR "SIGILOSO" NO CABEÇALHO EM TODAS AS PÁGINAS. (4.7.2) MANIPULAÇÃO: ACESSO RESTRITO APENAS AOS CREDENCIADOS QUE POSSUEM NECESSIDADE DE SERVIÇO OU DEVER DE OFÍCIO. (4.6) GUARDA: INFORMAÇÃO SIGILOSA DEVE TER ACESSO CONTROLADO (FÍSICO E/OU LÓGICO). (4.8 e 4.9.2) ELIMINAÇÃO: DELEÇÃO SEGURA OU TRITURAÇÃO FÍSICA APÓS AUTORIZAÇÃO DO TITULAR DA UO, CONSIDERANDO OS PROCEDIMENTOS DE GESTÃO DOCUMENTAL DEFINIDOS (4.13)
			SIGILO CLIENTE DO SERPRO	Lei do SERPRO, Art. 8°.	
			DIREITO AUTORAL	Lei 9.610/1998	
			PROPRIEDADE INTELECTUAL – SOFTWARE	Lei 9.609/1998	
			SIGILO DO PROCESSO ADMINISTRATIVO DISCIPLINAR (EM CURSO)	Art. 2, V, e 46 da Lei 9.784/1999	
			SIGILO DE INQUÉRITO POLICIAL	Art. 20 da Lei 3.689/1941	
			SEGREDO DE JUSTIÇA NO PROCESSO CIVIL	Art. 155 da Lei 5.869/1973	
			SEGREDO DE JUSTIÇA NO PROCESSO PENAL	§ 6º do art. 201 da Lei 3.689/1941	
			RESTRIÇÃO DISCRICIONÁRIA DE ACESSO A DOCUMENTO PREPARATÓRIO	§ 3º do art. 7 da Lei 12.527/2011	
			SIGILO DADOS PESSOAIS SENSÍVEIS	Lei 13.709/2018	

Serpro

ANEXO

NÚMERO 5 **VERSÃO** 1

TÍTULO

TABELA DE CATEGORIZAÇÃO DA INFORMAÇÃO

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

INFORMAÇÃO SIGILOSA (CLASSIFICADA)

TIPO DE INFORMAÇÃO	CARACTERÍSTICA	CATEGORIZAÇÃO DA INFORMAÇÃO	DETALHAMENTO	FUNDAMENTO LEGAL	TRATAMENTO
Informação sigilosa que é classificada em grau de sigilo, nos termos da LAI:				LAI, Art. 23.	
SIGILOSA	INFORMAÇÃO CLASSIFICADA EM GRAU DE SIGILO NA LAI	SECRETA	Informação imprescindível à segurança da sociedade ou do Estado	LAI, Art. 24, II.	MARCAÇÃO: OBRIGATÓRIA. MARCAR "SECRETO" OU "RESERVADO" NO CABEÇALHO E RODAPÉ EM TODAS AS PÁGINAS. (4.7.1) MANIPULAÇÃO: ACESSO RESTRITO APENAS AOS CREDENCIADOS QUE POSSUEM NECESSIDADE DE SERVIÇO OU DEVER DE OFÍCIO. (4.6, 4.10 e 4.11) GUARDA: INFORMAÇÃO SIGILOSA DEVE TER ACESSO CONTROLADO (FÍSICO E/OU LÓGICO). (4.8, 4.9.1, 4.11) ELIMINAÇÃO: NÃO É PERMITIDA A ELIMINAÇÃO DE INFORMAÇÃO CLASSIFICADA (4.12)
		RESERVADA	Informação imprescindível à segurança da sociedade ou do Estado	LAI, Art. 24, III.	

Serpro

ANEXO

NÚMERO 5 **VERSÃO** 1

TÍTULO

TABELA DE CATEGORIZAÇÃO DA INFORMAÇÃO

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

INFORMAÇÃO PESSOAL

TIPO DE INFORMAÇÃO	CARACTERÍSTICA	CATEGORIZAÇÃO DA INFORMAÇÃO	DETALHAMENTO	FUNDAMENTO LEGAL	TRATAMENTO
Dado pessoal, nos termos da LGPD:				LGPD Art. 5º e 14º	
PESSOAL	INFORMAÇÃO RELACIONADA A PESSOA NATURAL IDENTIFICADA OU IDENTIFICÁVEL	DADO PESSOAL	Dado pessoal: informação relacionada à pessoa natural identificada ou identificável; Tratamento administrativo com garantia de privacidade; Necessita de privacidade, de proteção e controles, mas não necessariamente de sigilo	LGPD Art. 5º e 14º	MARCAÇÃO: RECOMENDADA. MARCAÇÃO "DADO PESSOAL" NO CABEÇALHO EM TODAS AS PÁGINAS. (4.7.2) MANIPULAÇÃO: ACESSO RESTRITO APENAS AOS CREDENCIADOS QUE POSSUEM NECESSIDADE DE SERVIÇO OU DEVER DE OFÍCIO. PODERÃO TER SUA DIVULGAÇÃO OU ACESSO POR TERCEIROS AUTORIZADOS POR PREVISÃO LEGAL OU CONSENTIMENTO EXPRESSO DA PESSOA A QUE SE REFERIREM. TRATAMENTO E A PROTEÇÃO DO DADO POR MEIO DA OCULTAÇÃO, DA ANONIMIZAÇÃO OU DA PSEUDONIMIZAÇÃO DAS INFORMAÇÕES PESSOAIS RELATIVAS À INTIMIDADE, À VIDA PRIVADA, À HONRA E À IMAGEM. (4.4) GUARDA: DADOS PESSOAIS DEVEM TER ACESSO CONTROLADO (FÍSICO E/OU LÓGICO). (4.8, 4.9.2) TEMPO DE RETENÇÃO: PERÍODO DE TEMPO ESTABELECIDO NA MATRIZ DE CATEGORIZAÇÃO (ANEXO 6) E NO RAT (REGISTRO DE ATIVIDADE DE TRATAMENTO) QUANDO HOUVER TRATAMENTO DE DADOS PESSOAIS ELIMINAÇÃO: DELEÇÃO SEGURA OU TRITURAÇÃO FÍSICA APÓS AUTORIZAÇÃO DO TITULAR DA UO, CONSIDERANDO OS PROCEDIMENTOS DE GESTÃO DOCUMENTAL DEFINIDOS (4.13)
Dado pessoal Sensível, nos termos da LGPD:				LGPD Art. 5º e 14º	
PESSOAL SENSÍVEL	INFORMAÇÃO SENSÍVEL RELACIONADA A PESSOA NATURAL IDENTIFICADA OU IDENTIFICÁVEL	DADO PESSOAL SENSÍVEL (SIGILOSA)	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; Necessita de privacidade, de proteção e controles, como também, de sigilo.	LGPD Art. 5º e 14º LAI, Art. 31º	MARCAÇÃO: RECOMENDADA. MARCAÇÃO "DADO PESSOAL SENSÍVEL" NO CABEÇALHO EM TODAS AS PÁGINAS. (4.7.2) MANIPULAÇÃO: ACESSO RESTRITO APENAS AOS CREDENCIADOS QUE POSSUEM NECESSIDADE DE SERVIÇO OU DEVER DE OFÍCIO. PODERÃO TER SUA DIVULGAÇÃO OU ACESSO POR TERCEIROS AUTORIZADOS POR PREVISÃO LEGAL OU CONSENTIMENTO EXPRESSO DA PESSOA A QUE SE REFERIREM. TRATAMENTO E A PROTEÇÃO DO DADO POR MEIO DA OCULTAÇÃO, DA ANONIMIZAÇÃO OU DA PSEUDONIMIZAÇÃO DAS INFORMAÇÕES PESSOAIS RELATIVAS À INTIMIDADE, À VIDA PRIVADA, À HONRA E À IMAGEM. (4.4) GUARDA:DADOS PESSOAIS DEVE TER ACESSO CONTROLADO (FÍSICO E/OU LÓGICO). (4.8, 4.9.2) TEMPO DE RETENÇÃO: PERÍODO DE TEMPO ESTABELECIDO NA MATRIZ DE CATEGORIZAÇÃO (ANEXO 6) E NO RAT (REGISTRO DE ATIVIDADE DE TRATAMENTO) QUANDO HOUVER TRATAMENTO DE DADOS PESSOAIS ELIMINAÇÃO: DELEÇÃO SEGURA OU TRITURAÇÃO FÍSICA APÓS AUTORIZAÇÃO DO TITULAR DA UO, CONSIDERANDO OS PROCEDIMENTOS DE GESTÃO DOCUMENTAL DEFINIDOS (4.13)

Serpro

ANEXO

NÚMERO	VERSÃO
6	1

TÍTULO

MODELO DE MATRIZ DE CATEGORIZAÇÃO DA INFORMAÇÃO

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

MATRIZ DE CATEGORIZAÇÃO DA INFORMAÇÃO						Período de Revisão		Data da Categorização	
Tipo de Informação	UO	Característica	Categorização da Informação	Detalhamento	Fundamento Legal	TRATAMENTO		Processo	Repositório
						Marcação			
						Manipulação			
						Credenciado			
						Guarda			
						Eliminação			
						Tempo			
						Circunstância			

O modelo de Matriz de Categorização da Informação deverá ser utilizado como padrão para criar ou atualizar matrizes existentes.

O *template* está disponibilizado no repositório de documentos da ferramenta corporativa de Gestão Integrada de Processos.

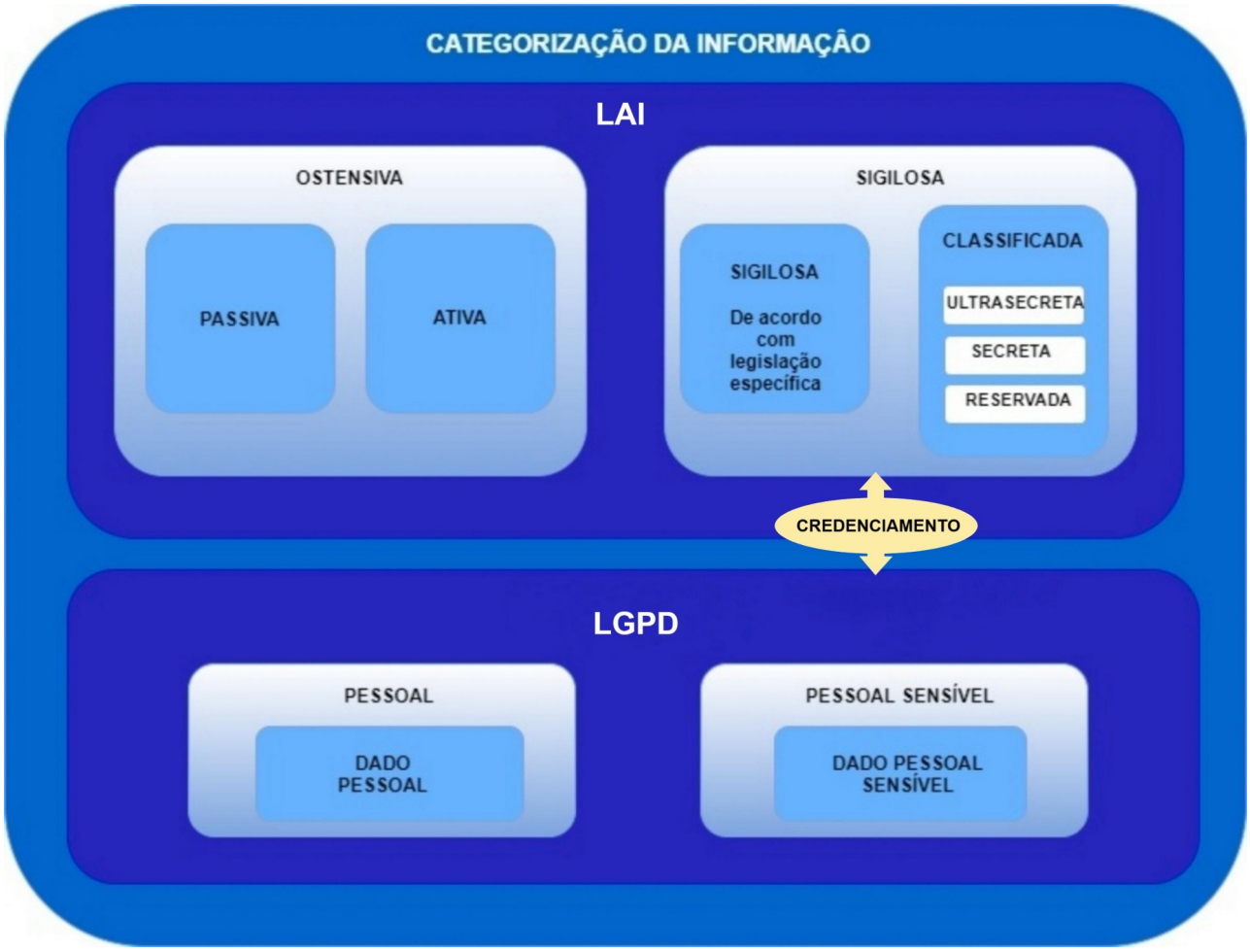
Serpro

ANEXO

NÚMERO 7 **VERSÃO** 1

TÍTULO

MODELO DE CATEGORIZAÇÃO DA INFORMAÇÃO

CÓDIGO DE CLASSIFICAÇÃO ARQUIVÍSTICA: 010.01 **CLASSIFICAÇÃO DA INFORMAÇÃO:** Ostensivo

1.0 Modelo de Categorização da Informação