

Assunto:
Manual de Classificação da Informação no âmbito do Sistema Cofen/Conselhos Regionais de Enfermagem.

Aprovação:

Vigência:

**MANUAL DE
CLASSIFICAÇÃO DA
INFORMAÇÃO
– MAN 108**

Controladoria-Geral

Gestão 2021-2023

Créditos

Conselho Federal de Enfermagem (Cofen)
Assessoria de Planejamento e Gestão (ASPLAN)
Centro de Documentação e Memória (CDM)

Conselheiros Efetivos

Presidente: Betânia Maria Pereira dos Santos – Coren-PB nº42.725
Vice-Presidente: Antônio Marcos Freire Gomes – Coren-PA nº 56.302
Primeira-Secretária: Sílvia Maria Neri Piedade – Coren-RO nº 92.597
Segundo-Secretário: Osvaldo Albuquerque Sousa Filho – Coren-CE nº 56.145
Primeiro-Tesoureiro: Gilney Guerra de Medeiros – Coren-DF nº 143.136
Segundo-Tesoureiro: Wilton José Patrício – Coren-ES nº 68.864
Helga Regina Bresciani – Coren-SC nº 29.525
Daniel Menezes de Souza – Coren-RS nº 105.771
Vancelau Jackson da Conceição Pantoja – Coren-AP nº 75.956

Conselheiros Suplentes

Claudio Luiz da Silveira – Coren-SP nº 25.368-IR
Dannyelly Dayane Alves da Silva – Coren-AL nº 271.580
Emília Maria Rodrigues Miranda Damasceno Reis – Coren-TO nº 122.726
Josias Neves Ribeiro – Coren-RR nº 142.834
Ivone Amazonas Marques Abolnik – Coren-AM nº 82.356
Leocarlos Cartaxo Moreira – Coren-MT nº 12.054-IR
Lisandra Caixeta de Aquino – Coren-MG nº 118.636
Marcio Raleigue Abreu Lima Verde – Coren-AC nº 85.068
Tatiana Maria Melo Guimarães – Coren-PI nº 110.720

Equipe Técnica

Marcelo Felipe Moreira Persegona.
Denise Araújo do Prado Pinto.
João Marcos Vasconcelos de Assis.

Versionamento

Versão	Data	Detalhamento da versão	Preparado por	Aprovado por
1.0	22/09/2021	Preparação inicial do documento.	João Marcos Vasconcelos de Assis	Não se aplica.
1.0	01/03/2023	Revisão do documento.	Marcelo Felipe Moreira Persegona	Não se aplica.
1.0	04/04/2023	Matéria remetida ao Conselheiro Federal Dr. Daniel Menezes de Souza para análise e emissão de parecer antes de levar ao conhecimento do Plenário.	191ª Reunião Ordinária de Diretoria	Não se aplica.
1.0	05/04/2023	Revisão do documento.	Denise Araújo do Prado Pinto	Não se aplica.
1.0	01/06/2023	Atualização do documento com as observações do CDM.	Marcelo Felipe Moreira Persegona	Não se aplica.
1.0	16/06/2023	Revisão do documento.	Conselheiro Federal Dr. Daniel Menezes de Souza	Não se aplica.
1.0	24/11/2023	<p>Atualização do documento com as observações do Conselheiro Federal Dr. Daniel Menezes de Souza, inclusão das Resoluções Cofen, no título 5 deste manual:</p> <ul style="list-style-type: none"> • Resolução Cofen nº 507/2016 – Institui e implementa o Código de Ética dos Empregados Públicos do Sistema Cofen/Conselhos Regionais de Enfermagem. • Resolução Cofen nº 645/2020 - Aprova o Código de Processo Administrativo Disciplinar do Sistema Cofen/Conselhos Regionais de Enfermagem, e dá outras providências. • Resolução Cofen nº 706/2022 - Aprova o Código de Processo Ético do Sistema Cofen/Conselhos Regionais de Enfermagem. <p>Inclusão da Corregedoria-Geral no capítulo que trata das competências das unidades funcionais, no título 4 deste manual.</p> <p>Itens 7.1 - 7.1.2 - 7.4.1 - 7.11,1: substituição do termo “empregado(s) público(s)” pelo termo “agentes públicos”.</p>	Conselheiro Federal Dr. Daniel Menezes de Souza	559ª Reunião Ordinária de Plenário, de 24/11/2023.

Sumário

1. FINALIDADE	4
2. ÁREA RESPONSÁVEIS	4
3. CONCEITUAÇÃO	4
4. ABREVIATURAS	7
5. LEGISLAÇÕES E DOCUMENTOS DE REFERÊNCIA	7
6. COMPETÊNCIAS	8
7. PROCEDIMENTOS	12
8. DISPOSIÇÕES GERAIS	24
9. FORMULÁRIOS	24
9.1. Anexo 1 - Termo de Classificação de Informação (TCI)	24
9.2. Anexo 2 - Termo de Credenciamento para Acesso à Informação Sigilosa (TCAIS)	26
9.3. Anexo 3 - Termo de Compromisso de Manutenção de Sigilo (TCMS).....	27
9.4. Anexo 4 - Lista de informações desclassificadas	28
9.5. Anexo 5 - Lista de informações classificadas.....	28
10. APÊNDICES	28

1. FINALIDADE

- 1.1. Estabelecer critérios para a identificação e classificação da informação no âmbito do Sistema Cofen/Conselhos Regionais de Enfermagem.

2. ÁREA RESPONSÁVEIS

- 2.1. Área Gestora – Centro de Documentação e Memória do Cofen.
- 2.2. Área Corresponsável – Unidades funcionais do Cofen.

3. CONCEITUAÇÃO

3.1. ÁREA GESTORA

Área responsável pela elaboração, atualização e gestão do manual.

3.2. ÁREA CORRESPONSÁVEL

Área que compartilha a responsabilidade sobre o manual, levando em conta que seu teor interfere, substancialmente, nos procedimentos de sua área de competência.

3.3. AUTORIDADE CLASSIFICADORA

É aquela que tem competência para classificar os documentos nos graus de sigilo reservado, secreto e ultrassecreto.

3.4. AUTORIZADO

Pessoa a qual foi concedido o acesso à informação sigilosos.

3.5. CIFRAÇÃO

Ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem clara por outros ininteligíveis por pessoas não autorizadas a conhecê-la.

3.6. COMPARTIMENTAÇÃO

Tem o propósito de permitir acesso somente às pessoas que tenham a necessidade de conhecer o conteúdo de uma informação.

3.7. COMPROMETIMENTO

Perda de segurança resultante do acesso não autorizado.

3.8. CONTRATO SIGILOSO

Ajuste, convênio ou termo de cooperação cujo objeto ou execução implique tratamento de informação classificada.

3.9. CREDENCIAL DE SEGURANÇA

Certificado que autoriza pessoa para o tratamento de informação classificada.

3.10. CREDENCIAMENTO DE SEGURANÇA

Processo utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada.

3.11. DADO

Conjunto de símbolos que, ao se atribuir significado, gera informação.

3.12. DADO ANONIMIZADO

É o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo.

3.13. DECIFRAÇÃO

Ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.

3.14. DISPONIBILIDADE

É a qualidade da informação conhecida, podendo ser acessada e utilizada por pessoas, equipamentos ou sistemas autorizados quando solicitado.

3.15. DOCUMENTO

É a informação registrada, independente da forma ou do suporte, produzida ou recebida no decorrer das atividades de uma instituição ou pessoa, dotada de organicidade, que possui elementos constituídos suficientes para servir de prova dessas atividades (CONARQ, 2005).

3.16. FORMATO

É a configuração física ou digital do documento gerado. É o suporte, o meio onde a informação foi registrada, considerando sua natureza e função.

3.17. GESTOR DE SEGURANÇA E CREDENCIAMENTO

Responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle.

3.18. GESTORES DA INFORMAÇÃO

Empregados(as) públicos(as) do Sistema Cofen/Conselhos Regionais de Enfermagem e funcionários de empresas prestadoras de serviços, que no exercício de suas competências vinculadas ao Cofen ou Coren, produzem, recebem, guardam, ou gerenciam informações de propriedade de pessoa natural ou jurídica.

3.19. INFORMAÇÃO PÚBLICA

Toda informação que seja de domínio público, ou seja, informações veiculadas continuamente nas mídias, nas obras de domínio público e em especial as informações constantes nos órgãos públicos. Por consequência, são públicos os bancos de dados e os documentos que dão suporte a essas informações.

3.20. INFORMAÇÃO PESSOAL

É aquela cuja associação é feita à pessoa natural identificada ou identificável.

3.21. INFORMAÇÃO SIGILOSA

É a informação restrita de maneira provisória ao público, visando a segurança da sociedade e do Estado.

3.22. INTEGRIDADE

É a qualidade da informação não alterada, preservando sua transitividade entre origem, tramitação e destino.

3.23. MARCAÇÃO

Aposição de marca que indica o grau de sigilo da informação classificada.

3.24. MEDIDAS DE SEGURANÇA

Medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo.

3.25. METADADO

Dados referentes a outros dados, os quais são dados estruturados e codificados que descrevem e permitem encontrar, gerenciar, compreender ou preservar outros dados ao longo do tempo

3.26. POSTO DE CONTROLE

Unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo.

3.27. PSEUDONIMIZAÇÃO

É a técnica de tratar dados pessoais de uma forma em que os dados somente possam ser atribuídos a um titular de dados mediante a utilização de informações adicionais, não disponíveis a todos, desde que essas informações sejam mantidas em ambiente separado, controlado e seguro.

3.28. QUEBRA DE SEGURANÇA

Ação ou omissão que implica comprometimento ou risco de comprometimento de informação classificada em qualquer grau de sigilo.

3.29. SOLICITANTE

É a pessoa que requer acesso à informação.

3.30. TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI)

É o formulário estruturado para formalização da decisão de classificação da informação.

3.31. TRANSPARÊNCIA ATIVA

É ação das instituições públicas de disponibilizar as informações de forma diligente, de modo a possibilitar que o cidadão tenha acesso rápido e fácil ao dado sem necessitar encaminhar solicitação de informação.

3.32. TRANSPARÊNCIA PASSIVA

É a disponibilização de informações após a sua solicitação pelos cidadãos.

3.33. TRATAMENTO DA INFORMAÇÃO

Conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.

4. ABREVIATURAS

- 4.1. Art - Artigo.
- 4.2. CIDIC - Código de Indexação de Documento que contém Informação Classificada.
- 4.3. Cofen - Conselho Federal de Enfermagem.
- 4.4. Coren - Conselho Regional de Enfermagem.
- 4.5. CPF - Cadastro de Pessoa Física.
- 4.6. e-SIC - Sistema Eletrônico do Serviço de Informação ao Cidadão.
- 4.7. LAI - Lei de Acesso à Informação.
- 4.8. LGPD - Lei Geral de Proteção de Dados Pessoais.
- 4.9. MAN - Manual.
- 4.10. SEI - Sistema Eletrônico de Informações.
- 4.11. SIC - Serviço de Informação ao Cidadão.
- 4.12. TCAIS - Termo de Credenciamento para Acesso à Informação Sigilosa.
- 4.13. TCI - Termo de Classificação de Informação.
- 4.14. TCMS - Termo de Compromisso de Manutenção de Sigilo.
- 4.15. TI - Tecnologia da Informação.

5. LEGISLAÇÕES E DOCUMENTOS DE REFERÊNCIA

- 5.1. Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir 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.
- 5.2. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo no âmbito do Poder Executivo federal, e dispõe sobre o Núcleo de Segurança e Credenciamento, conforme o disposto nos arts. 25, 27, 29, 35, § 5º, e 37 da Lei nº 12.527, de 18 de novembro de 2011.
- 5.3. Anexo I – Manual de Transparência e Classificação de Informações do Senado Federal.

- 5.4. Guia de Publicação de Lista de Informações Classificadas e Desclassificadas e de Relatórios Estatísticos sobre a Lei de Acesso à Informação - 5ª Versão.
- 5.5. Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD) - Guia de Boas Práticas para Implementação na Administração Pública Federal. Versão 2.0. Gov.br. Agosto/2020.
- 5.6. Resolução Cofen nº 576/2018 - MAN 501 – Estabelece responsabilidades, premissas e orientações para a o acesso à informação e a aplicação da Lei nº 12.527, de 18 de novembro de 2011, no âmbito dos Conselhos Federal e Regionais de Enfermagem.
- 5.7. Resolução Cofen nº 507/2016 – Institui e implementa o Código de Ética dos Empregados Públicos do Sistema Cofen/Conselhos Regionais de Enfermagem.
- 5.8. Resolução Cofen nº 645/2020 - Aprova o Código de Processo Administrativo Disciplinar do Sistema Cofen/Conselhos Regionais de Enfermagem, e dá outras providências.
- 5.9. Resolução Cofen nº 706/2022 - Aprova o Código de Processo Ético do Sistema Cofen/Conselhos Regionais de Enfermagem.

6. COMPETÊNCIAS

6.1. Compete das unidades funcionais do Cofen e dos Conselhos Regionais de Enfermagem:

- I. Assegurar o cumprimento das normas relativas às informações classificadas/desclassificadas em qualquer grau de sigilo, de forma eficiente e adequada aos objetivos da legislação federal reguladora e deste manual.
- II. Garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.
- III. Classificar as informações sob sua jurisdição até o grau de sigilo “RESERVADO”.
- IV. Fiscalizar o cumprimento das normas e tratamento de informação classificada, no âmbito de suas competências.
- V. Orientar e recomendar ao Plenário, à Presidência e às demais unidades funcionais do Cofen/Conselhos Regionais de Enfermagem as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto na legislação federal reguladora e neste manual quanto a classificação/desclassificação da informação constantes da:
 - a) lista de informações a serem classificadas em cada grau de sigilo;
 - b) lista das informações classificadas/desclassificadas dos graus de sigilo pelo menos nos últimos 12 (doze) meses, acompanhadas da data, do grau de sigilo correspondente, dos fundamentos da classificação/desclassificação e da autoridade responsável pela classificação.

6.2. Compete à Ouvidoria-Geral:

- I. Ser responsável pelo Serviço de Informação ao Cidadão (SIC) no âmbito do Cofen.
- II. Atender e orientar o público quanto ao acesso as informações.
- III. Informar aos cidadãos sobre a tramitação de documentos.
- IV. Receber e dar andamento a requerimentos de acesso a informações.
- V. Manter e gerenciar o Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC) para requerimento e acesso à informação, observando e fazendo cumprir todos os dispositivos, prazos legais e normas conexas.
- VI. Providenciar a publicação, no Portal da Transparência do Cofen, de relatório estatístico anual contendo a quantidade de pedidos de informações recebidos, atendidos e indeferidos, bem como informações genéricas sobre os solicitantes.
- VII. Garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.
- VIII. Fiscalizar o cumprimento das normas e tratamento de informação classificada, no âmbito de suas competências.
- IX. Classificar as informações recebidas nos graus de sigilo correspondentes no Sistema Eletrônico do Serviço de Informação ao Cidadão (e-SIC), até o grau de sigilo “RESERVADO”.

6.3. Compete ao Departamento de Tecnologia da Informação e Comunicação:

- I. Fornecer soluções de TI e de infraestrutura tecnológica para o cumprimento deste manual e o aprimoramento do Portal Cofen como instrumento de promoção da transparência e de acesso à informação.
- II. Garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.
- III. Fiscalizar o cumprimento das normas e tratamento de informação classificada, no âmbito de suas competências.
- IV. Garantir o acesso às informações classificadas nos graus de sigilo atribuído a cada empregado(a) público(a) no âmbito dos Conselhos Federal e Regionais de Enfermagem, respeitando a compartimentação e o grau de acesso à informação.
- V. No tratamento da informação classificada deverão ser utilizados sistemas de informação e canais de comunicação seguros que atendam aos padrões mínimos de qualidade e segurança definidos pelo Poder Executivo Federal.
 - a) A transmissão de informação classificada em qualquer grau de sigilo por meio de sistemas de informação deverá ser realizada, no âmbito da rede corporativa, por meio de canal seguro, como forma de mitigar o risco de quebra de segurança.

- b) A autenticidade da identidade eletrônica do usuário da rede deverá ser garantida pelo uso de login e senha pessoal ou pelo uso de certificado digital.
 - c) Os sistemas de informação deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos graus de sigilo.
 - d) Os sistemas de informação deverão 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.
- VI. Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam física ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.
- VII. A cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado.
- VIII. Os procedimentos de tratamento de informação classificada em qualquer grau de sigilo aplicam-se aos recursos criptográficos, atendidas as seguintes exigências:
- a) realização de vistorias periódicas, com a finalidade de assegurar a execução das operações criptográficas;
 - b) manutenção de inventários completos e atualizados do material de criptografia existente;
 - c) designação de sistemas criptográficos adequados a cada destinatário;
 - d) comunicação, ao superior hierárquico ou à autoridade competente, de anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de informações criptografadas; e
 - e) identificação de indícios de violação, de interceptação ou de irregularidades na transmissão ou recebimento de informações criptografadas.

6.4. Compete à Corregedoria-Geral:

- I. Orientar e recomendar ao Plenário, à Presidência e às demais unidades funcionais do Cofen as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto na legislação federal reguladora e neste manual quanto a classificação/desclassificação de Sindicâncias e Processos Disciplinares:
 - a) a lista das informações classificadas/desclassificadas nos graus de sigilo nos últimos 12 (doze) meses, acompanhadas da data, do grau de sigilo correspondente, dos fundamentos da classificação/desclassificação e da autoridade responsável pela classificação/desclassificação; e

- b) monitorar a aplicação do disposto na legislação federal reguladora da classificação das informações e neste manual e apresentando relatórios anuais sobre o seu cumprimento no que se refere aos processos de sua área de competência.
- II. Garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.
- III. Fiscalizar o cumprimento das normas e tratamento de informação classificada, no âmbito de suas competências.
- IV. Classificar as informações sob sua jurisdição até o grau de sigilo “RESERVADO”.

6.5. Compete ao Setor de Processos Éticos:

- I. Orientar e recomendar ao Plenário, à Presidência e às demais unidades funcionais do Cofen as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto na legislação federal reguladora e neste manual quanto a classificação/desclassificação dos Processos Éticos:
 - a) a lista das informações classificadas/desclassificadas nos graus de sigilo nos últimos 12 (doze) meses, acompanhadas da data, do grau de sigilo correspondente, dos fundamentos da classificação/desclassificação e da autoridade responsável pela classificação/desclassificação; e
 - b) monitorar a aplicação do disposto na legislação federal reguladora da classificação das informações e neste manual e apresentando relatórios anuais sobre o seu cumprimento no que se refere aos Processos Éticos.
- II. Garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.
- III. Fiscalizar o cumprimento das normas e tratamento de informação classificada, no âmbito de suas competências.
- IV. Classificar as informações sob sua jurisdição até o grau de sigilo “RESERVADO”.

6.6. Compete ao Escritório de Proteção de Dados:

- I. Disponibilizar o Termo de Classificação de Informação (TCI) às demais unidades funcionais do Cofen.
- II. Garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.
- III. Fiscalizar o cumprimento das normas e tratamento de informação classificada, no âmbito de suas competências.
- IV. Classificar as informações até o grau de sigilo “RESERVADO”.
- VI. Orientar e recomendar ao Plenário, à Presidência e às demais unidades funcionais do Cofen as medidas indispensáveis à implementação e ao

aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto na legislação federal reguladora e neste manual quanto a classificação/desclassificação da informação constantes da:

- a) lista de informações a serem classificadas em cada grau de sigilo;
- b) lista das informações classificadas/desclassificadas dos graus de sigilo pelo menos nos últimos 12 (doze) meses, acompanhadas da data, do grau de sigilo correspondente, dos fundamentos da classificação/desclassificação e da autoridade responsável pela classificação.

6.7. Compete aos Conselhos Regionais de Enfermagem:

- I. Disponibilizar o Termo de Classificação de Informação (TCI) às demais unidades funcionais do Coren.
- II. Garantir a segurança da informação classificada em qualquer grau de sigilo sob sua responsabilidade.
- III. Fiscalizar o cumprimento das normas e tratamento de informação classificada, no âmbito de suas competências.
- IV. Classificar as informações sob sua jurisdição até o grau de sigilo “RESERVADO”.
- V. Orientar e recomendar ao Plenário, à Presidência e às demais unidades funcionais do Coren as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto na legislação federal reguladora e neste manual quanto a classificação/desclassificação da informação citada no rol:
 - a) da lista de informações a serem classificadas em cada grau de sigilo;
 - b) da lista das informações classificadas/desclassificadas dos graus de sigilo pelo menos nos últimos 12 (doze) meses, acompanhadas da data, do grau de sigilo correspondente, dos fundamentos da classificação/desclassificação e da autoridade responsável pela classificação.

7. PROCEDIMENTOS

7.1. Os(as) Conselheiros(as) Federais, Conselheiros(as) Regionais e agentes públicos do Sistema Cofen/Conselhos Regionais de Enfermagem devem adotar os procedimentos indicados no Manual da Classificação de Informações na produção, recebimento, classificação, acesso, gestão e arquivamento dos documentos e informações do Sistema Cofen/Conselhos Regionais de Enfermagem.

7.1.1. Diante da importância do tema tratado na Lei de Acesso à Informação para a transparência e a consolidação do Estado Democrático de Direito, foi publicado no Conselho Federal de Enfermagem, em 08 de junho de 2018, a Resolução Cofen nº 576/2018, que estabelece responsabilidades, premissas e orientações

para a o acesso à informação e a aplicação da Lei nº 12.527, de 18 de novembro de 2011, no âmbito dos Sistema Cofen/Conselhos Regionais de Enfermagem.

- 7.1.2. Em complemento à edição do MAN 501 – Acesso à Informação, elaborou-se o presente manual com vistas a auxiliar Conselheiros(as) Federais, Conselheiros(as) Regionais e agentes públicos do Sistema Cofen/Conselhos Regionais de Enfermagem a identificar os tipos de informações públicas, a conhecer possíveis classificações, a apresentar procedimentos quanto à gestão de informações classificadas, propiciando desta forma um instrumento para facilitar as atividades que de acesso, com observância de eventuais restrições previstas no corpo normativo vigente.
- 7.1.3. Esclarecemos que no Sistema Cofen/Conselhos Regionais de Enfermagem as informações geradas em processos iniciados em sistemas eletrônicos de gerenciamento de informações ou criadas em meio físico, podem receber a classificação de grau “RESTRITO OU SIGILOSO” e as demais classificações, “SECRETO” e “ULTRASSECRETO”, não se aplicam.

7.2. IDENTIFICAÇÃO DA INFORMAÇÃO

7.2.1. As informações tratadas no âmbito do sistema Cofen/Conselhos Federais de Enfermagem podem se categorizadas em:

- I. pública ou ostensiva;
- II. restrita; e
- III. sigilosa.

7.2.2. INFORMAÇÃO “PUBLICA” ou “OSTENSIVA”

7.2.2.1. A informação “PUBLICA” ou “OSTENSIVA” é aquela cujo acesso pode ser franqueado a qualquer pessoa, sem nenhum tipo de restrição.

7.2.3. INFORMAÇÃO RESTRITA

7.2.3.1. Nesta categoria de informação, o Sistema Cofen/Conselhos Regionais de Enfermagem classifica a informação ou o documento como “RESTRITO” aos assuntos que não devam ser do conhecimento do público em geral devendo ser acessados apenas pelos diretamente interessados e por agentes públicos das unidades administrativas nas quais são tramitados.

7.2.4. INFORMAÇÃO SIGILOSA

7.2.4.1. Nesta categoria de informação, o Sistema Cofen/Conselhos Regionais de Enfermagem possui apenas o grau de classificação “SIGILOSO”, o qual é atribuído a todos os assuntos que não devam ser do conhecimento do público em geral e de agentes públicos não autorizados. Exige rigorosas medidas de segurança, e seu teor deve ser acessado, exclusivamente, por agentes públicos credenciados e diretamente ligados à sua análise. Tais como os que:

- I. Expõem informações pessoais ou sensíveis, conteúdo de investigação ou decisão interna *corporis*, relativa a **processos éticos**, processos administrativos disciplinares, processos de sindicância ou o conteúdo de votos não ostensivos por imposição constitucional ou legal.

7.2.4.2. Para que uma informação seja considerada sigilosa ela deve se enquadrar em uma das hipóteses de sigilo previstas na Constituição Federal.

7.2.5. INFORMAÇÃO PESSOAL

7.2.5.1. A informação pessoal é aquela relacionada à pessoa natural identificada ou identificável. São consideradas informações pessoais as relativas à intimidade, à vida privada, à honra e à imagem, dentre outras:

- I. Nomes de cônjuge, ou companheiro, e parentes até o 4º grau, endereço de residência e número de telefone, número de CPF e de documentos de identidade, exceto quando constarem de documentos comprobatórios de despesas indenizáveis pelo Sistema Cofen/Conselhos Regionais de Enfermagem.
- II. Número identificador de contrato firmado pelo Presidente do Conselho com companhia telefônica e de outros contratos de telecomunicações passíveis de reembolso de despesas pelo Sistema Cofen/Conselhos Regionais de Enfermagem.
- III. Prontuários, laudos, exames, perícias, relatórios médicos.
- IV. No caso de reembolso de despesas médico-hospitalares: qualquer elemento identificador do prestador de serviço ou a identificação ou descrição do procedimento realizado.
- V. Discriminação de quaisquer descontos facultativos, ou decorrentes de ação judicial, incidentes sobre remuneração, proventos, subsídios, gratificações e vantagens.

7.2.5.2. A Lei de Acesso à Informação determina que as informações pessoais relativas à intimidade, à vida privada, à honra e à imagem devem ter seu acesso restrito aos agentes públicos legalmente autorizados no exercício de suas funções e à pessoa a que elas se refiram, independentemente de classificação de sigilo, e pelo prazo máximo de 100 (cem) anos, a contar da sua data de produção. Porém, diante de previsão legal ou mediante consentimento expresso da pessoa a que elas se refiram, essas informações podem ser divulgadas ou pode ser concedido acesso a terceiros.

7.3. CLASSIFICAÇÃO DE INFORMAÇÕES

7.3.1. Classificar um documento é atribuir a ele um grau de acesso que pode ser PÚBLICO, RESTRITO, RESERVADO, SIGILOSOS, SECRETO e ULTRASSECRETO.

7.3.2. A classificação e a desclassificação dos documentos relacionadas a níveis de acesso é uma ação muito importante na transparência das informações, pois, garante a todos os cidadãos a proteção de seus direitos básicos de acesso à

informação ao mesmo tempo que restringe, dentro dos parâmetros da lei, o conhecimento dos dados pessoais e dados sensíveis presentes nos documentos e processos por pessoas não autorizadas.

7.3.3. O Sistema Eletrônico de Informações (SEI) possibilita a classificação de documentos em 3 (três) níveis de acesso: PÚBLICO, RESTRITO e SIGILOSO.

7.3.4. Qualquer usuário do SEI pode atribuir o grau de acesso RESTRITO a processos no SEI e a documentos gerados em sua unidade, desde que indique a hipótese legal que justifica essa ação.

7.3.5. Apenas administradores do Sistema SEI, atendendo a pedido de autoridades competentes, podem atribuir o grau de acesso “SIGILOSO” a processos e documentos no SEI, sempre indicando a hipótese legal.

7.3.6. A permissão dada ao usuário solicitante para classificação de processos e documentos no SEI, em nível de acesso “SIGILOSO”, é dada a cada ocorrência e retirado imediatamente após concluída a ação.

7.3.7. CASOS QUE UMA INFORMAÇÃO É SIGILOSA

7.3.7.1. Segundo o art. 23 da Lei de Acesso à Informação, as informações passíveis de classificação são aquelas que podem:

- I. Pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional.
- II. 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.
- III. Pôr em risco a vida, a segurança ou a saúde da população.
- IV. Oferecer elevado risco à estabilidade financeira, econômica ou monetária do país.
- V. Prejudicar ou causar risco a planos ou operações estratégicas das Forças Armadas.
- VI. 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.
- VII. Por em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares.
- VIII. Comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento relacionadas com a prevenção ou repressão de infrações.

7.3.7.2. Quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

7.3.7.3. Documentos e informações sobre condutas que impliquem a violação de direitos humanos praticada por ou a mando de agentes públicos não podem ser objeto de restrição de acesso.

7.3.7.4. A Lei de Acesso à Informação no seu art. 22 prevê tipos de informações que podem ser classificadas como sigilosas, mas em categoria própria, estão o sigilo bancário (Lei Complementar nº 105/2001), o sigilo fiscal (Lei nº 5172/66) e as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica (pelo estado ou por entes que tenham vínculo com o poder público).

7.4. AUTORIDADES CLASSIFICADORAS

7.4.1. A atribuição de grau de sigilo “RESTRITO OU SIGILOSO” dos documentos produzidos ou sob a guarda do Sistema Cofen/Conselhos Regionais de Enfermagem será declarado pelas seguintes autoridades: Conselheiros Federais e Regionais, Chefe de Gabinete, Assessores, Chefes de Departamento, Divisão, Setor e agentes públicos indicados por esses.

7.4.2. Os documentos físicos que contêm informações pessoais; resultantes de tratados, acordos ou atos internacionais; segredo de justiça; sigilo telefônico; ou qualquer outra hipótese legal de restrição de acesso, devem receber marcação, bem como ter sua tramitação protegida. Nesses casos, a marcação da restrição pode ser realizada por qualquer empregado(a) público(a).

7.5. GESTÃO DA INFORMAÇÃO CLASSIFICADA

7.5.1. Na produção do documento com informação classificada, independente do meio e formato deve-se:

- I. Juntar ou criar documento no SEI pelo setor responsável pelo seu recebimento.
- II. Preencher os metadados relativos aos dados do documento de forma a não comprometer o sigilo da informação.
- III. Realizar a classificação do documento e preencher o “TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI)”, ver anexo 1, que receberá a mesma classificação do documento.

7.6. RECEBIMENTO DE DOCUMENTO COM INFORMAÇÃO CLASSIFICADA

7.6.1. No recebimento do documento com informação classificada ou que precise ser classificada, independente do meio e formato, deve-se:

- I. Registrar documento no SEI pelo setor responsável.
- II. Verificar a integridade do meio de recebimento e registrar indícios de violação ou de irregularidade, comunicando ao destinatário, que informará imediatamente ao remetente.
- III. Informar ao remetente o recebimento da informação, no prazo mais curto possível.

IV. Manter os documentos recebidos de acordo o grau de sigilo conferido pela instituição de origem.

7.6.2. Nos casos em que a instituição de origem não tiver classificado um documento que deveria ser classificado ou quando a classificação estiver incorreta, o documento deverá ser encaminhado à autoridade competente do Conselho Federal ou Regional, com a recomendação de classificação devidamente justificada. A autoridade deverá consultar o órgão de origem do documento e classificar ou reclassificar o documento.

7.7. FORMALIZAÇÃO DA CLASSIFICAÇÃO

7.7.1. Ao identificar um documento que possua informações que exija a classificação do nível de acesso, o(a) empregado(a) público(a) deve encaminhar o documento à autoridade competente com um despacho, devidamente justificado, recomendando uma classificação para que a autoridade analise a pertinência de classificar o documento utilizando o “TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI)”, ver anexo 1.

7.7.2. A autoridade, por sua vez, deve:

- I. Analisar o conteúdo do documento e, se constatar que a divulgação deste pode comprometer a segurança da sociedade ou do Estado, deve definir o nível de acesso ou o grau de restrição adequado, visando manter a informação restrita durante o tempo estritamente necessário para minimizar os riscos que sua divulgação possa acarretar à segurança da sociedade ou do Estado.
- II. Preencher o “TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI)”, ver anexo 1, que terá a mesma classificação do nível de acesso e da restrição do documento classificado.
- III. Introduzir uma marcação do grau de restrição, por meio de carimbo ou outro meio equivalente¹, nos cabeçalhos e rodapés das páginas que contiverem informação classificada, e nas capas do documento, de modo a não prejudicar a compreensão da informação.
- IV. Numerar as páginas seguidamente, devendo cada uma conter indicação do total de páginas que compõem o documento.
- V. Inserir a marcação “PESSOAL”, se o documento classificado em algum grau de restrição também possuir informações pessoais relativas à intimidade, vida privada, honra e imagem de pessoa física.

7.7.3. Na hipótese de o documento classificado integrar processo ostensivo, este deverá ser tramitado como anexo em envelope lacrado, observando os procedimentos para documentos sigilosos.

¹ No caso de mapas, fotocartas, fotografias, quaisquer outros tipos de imagens e meios eletrônicos de armazenamento, a marcação do grau de sigilo também deverá ser feita utilizando carimbo ou outro meio equivalente, sempre que possível; nos casos em que a aposição de rótulo for inviável, podem ser usadas outras formas de identificar a classificação, desde que os controles existentes sejam suficientes para proteger a informação de forma compatível com a classificação.

7.7.4. Na hipótese de documento que contenha informações classificadas em diferentes graus de restrição, deve ser atribuído ao documento tratamento do grau mais elevado, ficando assegurado o acesso às partes ostensivas por meio de certidão, extrato ou cópia, com ocultação das partes não permitidas.

7.8. EXPEDIÇÃO E TRAMITAÇÃO DE INFORMAÇÃO CLASSIFICADA

7.8.1. A expedição, a condução e a entrega de documento com informação classificada deverão ser efetuadas pessoalmente, por empregado(a) público(a) autorizado(a), ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia compatíveis com o grau de classificação da informação, vedada sua postagem. Na impossibilidade de uso de sistema seguro, os documentos digitais poderão ser enviados em mídias.

7.8.2. Na expedição e na tramitação de documentos físicos ou em mídia deverão ser realizados os seguintes procedimentos:

- I. Acondicionar o documento ou mídia em dois envelopes.
- II. Registrar no envelope externo apenas o destinatário e o remetente.
- III. Registrar no envelope interno o destinatário e o grau de sigilo do documento, de modo a serem identificados logo que removido o envelope externo. O envelope interno somente poderá ser aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior.
- IV. Fechar, lacrar e expedir os envelopes de forma que a tramitação do documento seja controlada de acordo com as regras de protocolo.
- V. Inserir a palavra “PESSOAL” no envelope que contiver documento de interesse exclusivo do destinatário, e somente ele, seu representante legal ou mandatário, com poderes específicos, poderá abri-lo.

7.9. ARMAZENAMENTO DA INFORMAÇÃO CLASSIFICADA

7.9.1. A informação classificada deverá obrigatoriamente ser mantida e arquivada em ambiente ou estrutura que ofereça proteção compatível com o grau de restrição, de forma a prevenir ameaças de quebra de segurança, de acordo com Política de Segurança de Informação vigente no Cofen/Coren.

7.10. PRESERVAÇÃO E GUARDA DE INFORMAÇÃO CLASSIFICADA

7.10.1. Após o cumprimento do seu trâmite, todo documento classificado com grau de restrição deve ser encaminhado para arquivamento no Setor de Arquivo-Geral, e preservados de acordo com os prazos da Tabela de Temporalidade de Documentos, não podendo ser desfigurado ou destruído até o cumprimento dos respectivos prazos de guarda, sob pena de responsabilidade na forma da lei.

7.11. CONTROLE DE ACESSO DE INFORMAÇÃO CLASSIFICADA

7.11.1. Todos os agentes públicos e autoridades do Sistema Cofen/Conselhos Regionais de Enfermagem devem zelar pelo controle do acesso e da divulgação de informações sigilosas ou restritas produzidas ou mantidas pelo seu Conselho, garantindo a sua proteção por meio da guarda dos documentos em condições especiais de segurança.

7.12. CREDENCIAMENTO PARA ACESSO À INFORMAÇÃO RESTRITA OU SIGILOSA

7.12.1. Caso seja identificada a necessidade de um(a) empregado(a) público(a) acessar processo ou documento restrito ou sigiloso que contenha informação pessoal, a autoridade competente ou o titular de unidade administrativa ou o diretamente interessado, deverá expressamente comprovar motivação válida e prevista em lei, para obter a devida autorização ou credencial de acesso.

7.12.2. O credenciamento confere ao credenciado, autorização para acessar um determinado processo ou documento e deve ser feito mediante preenchimento de “TERMO DE CREDENCIAMENTO PARA ACESSO À INFORMAÇÃO SIGILOSA (TCAIS)”, ver anexo 2, que deve ser assinado pela pessoa que credencia e pelo credenciado. Esse Termo deve identificar o processo ou documento para o qual o empregado(a) público(a) está sendo credenciado a acessar, com justificativa prevista em lei.

7.12.3. O credenciado também deverá assinar o “TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (TCMS)”, ver anexo 3.

7.13. SISTEMAS DE INFORMAÇÃO QUE CONTENHAM INFORMAÇÕES CLASSIFICADAS

7.13.1. No tratamento da informação classificada em qualquer grau de restrição deverão ser utilizados sistemas de informação e canais de comunicação seguros, no âmbito da rede corporativa, que atendam aos padrões mínimos de qualidade e segurança definidos pelo Cofen, como forma de mitigar o risco de quebra de segurança.

7.14. REPRODUÇÃO DE DOCUMENTO COM INFORMAÇÃO CLASSIFICADA

7.14.1. A reprodução total ou parcial de documentos com informação classificada condiciona-se à autorização expressa da autoridade classificadora competente ou autoridade competente hierarquicamente superior com igual prerrogativa para dispor sobre o assunto. As cópias serão autenticadas pela autoridade e estarão sujeitas ao mesmo grau de sigilo ou restrição do documento original.

7.15. ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

7.15.1. Segundo a LGPD, **dado anonimizado** é o dado que, considerados os meios técnicos razoáveis no momento do tratamento, perde a possibilidade de associação, direta ou indireta, a um indivíduo. A não identificação da relação entre

o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta. A partir do momento em que o dado é considerado anonimizado, e não permite mais qualquer identificação do seu titular, esse dado sai do escopo da legislação, por não mais se tratar de um dado pessoal, conforme previsto no art. 12 da LGPD.

7.15.2. É importante ressaltar que, ainda que o dado seja considerado anonimizado pelo controlador, uma vez observada a possibilidade de reversão do processo que obteve a anonimização, permitindo a reidentificação do titular de dados, não se está diante de um dado verdadeiramente anonimizado, mas de um dado potencialmente pseudonimizado.

7.15.3. Exemplos de anonimização:

7.15.3.1. Excluir ou não coletar o nome completo da pessoa ou qualquer outro dado que permita a identificação, tais como CPF, número de identidade, número de passaporte, número de Coren, parentesco, endereço, número de celular ou telefone e outros.

7.15.4. **Pseudonimização** é a técnica de tratar dados pessoais de uma forma em que os dados somente possam ser atribuídos a um titular de dados mediante a utilização de informações adicionais, não disponíveis a todos, desde que essas informações sejam mantidas em ambiente separado, controlado e seguro. A título ilustrativo, criptografia é um método de pseudonimização, quando os dados somente podem ser atribuídos a um titular mediante o conhecimento da chave criptográfica. Sem conhecer a chave, os dados são ininteligíveis.

7.15.5. De acordo com a legislação em vigor, esses processos devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis, na ocasião do tratamento dos dados.

7.15.6. A seguir, algumas recomendações para subsidiar a escolha da técnica a ser utilizada (anonimização e pseudonimização):

- I. Elencar os principais processos de trabalho que realizam tratamento de dados pessoais para a realização de estudos, especialmente em órgão de pesquisa, conforme art. 7º, IV da LGPD.
- II. Identificar os dados pessoais a que se referem os processos de trabalho listados, que não podem ter os titulares relacionados.
- III. Analisar o ciclo de vida de tratamento do dado a fim de mitigar riscos de violação de dados que não são mais de uso corrente. E, ainda, propor arquivamento ou eliminação dos dados, visto que a gestão de dados desnecessários no ambiente de produção causa aumento não apenas do quantitativo de dados a serem geridos, como também a manutenção do custo operacional relacionado a este processo (em atividades como armazenamento e gestão da segurança).
- IV. Avaliar o risco de identificação do titular dos dados listados. Deve-se levar em consideração que, quanto maior o uso de tecnologias de análise de dados, quanto maior o volume de dados processados e quanto mais significativos forem estes dados, maior será o risco de violação.

- V. Quando houver a obrigatoriedade de proteção de dados pessoais, sem a necessidade de guarda dos dados que associam estes aos titulares, pode-se optar pelo processo de anonimização, sem prejuízo de atividades do órgão ou entidade. Caso contrário, pode-se optar pela técnica de pseudonimização.
- VI. Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo cumprimento das atividades.
- VII. Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.
- VIII. Promover a conscientização contínua acerca da importância da proteção de dados no órgão ou entidade.

7.15.7. Cabe destacar que a pseudonimização, como técnica utilizada para proteção de dados pessoais, pode ser utilizada, por exemplo, para preservação da identidade do denunciante, conforme previsto no §4º do art. 6º do Decreto nº 10.153/2019.

Art. 6º O denunciante terá seus elementos de identificação preservados desde o recebimento da denúncia, nos termos do disposto no § 7º do art. 10 da Lei nº 13.460, de 2017.

§ 4º A unidade de ouvidoria responsável pelo tratamento da denúncia providenciará a sua pseudonimização para o posterior envio aos órgãos de apuração competentes, observado o disposto no § 2º.

7.15.8. A pseudonimização também pode ser utilizada para proteger a identidade do usuário de serviço público ou autor de manifestação conforme previsão do art. 24 do Decreto nº 9.492/2018.

Art. 24. As unidades que compõem o Sistema de Ouvidoria do Poder Executivo federal assegurarão a proteção da identidade e dos elementos que permitam a identificação do usuário de serviços públicos ou do autor da manifestação, nos termos do disposto no art. 31 da Lei nº 12.527, de 18 de novembro de 2011.

7.15.9. Exemplos de pseudonimização:

7.15.9.1. Utilizar as iniciais do nome completo da pessoa: MFMP.

7.15.9.2. Ocultação de alguns números do CPF da pessoa: xxx.852.xxx-xx.

7.15.9.3. Utilizar criptografia.

7.16. DIVULGAÇÃO DE INFORMAÇÃO CLASSIFICADA

7.16.1. Atendendo às determinações da Lei de Acesso à Informação (LAI), a Ouvidoria-Geral do Cofen publicará mensalmente relatório estatístico contendo a quantidade de pedidos de informação recebidos, atendidos e indeferidos, bem como informações genéricas sobre os solicitantes.

7.16.2. Por sua vez, o Setor de Processos Éticos publicará anualmente, ou quando ocorre alguma alteração, extrato com a lista de Processos Éticos classificados/desclassificados, acompanhadas da data, do grau de sigilo e dos fundamentos da classificação.

7.16.3. No contexto da implementação da Lei de Acesso à Informação sobre a publicação dos itens estabelecidos pelo art. 45 do Decreto nº 7.724/2012, transcrito a seguir:

Art. 45: A autoridade máxima de cada órgão ou entidade **publicará anualmente, até o dia 1º de junho, em sítio na Internet:**

I - rol das informações desclassificadas nos últimos doze meses;

II - rol das informações classificadas em cada grau de sigilo, que deverá conter:

- a) código de indexação de documento;
- b) categoria na qual se enquadra a informação;
- c) indicação de dispositivo legal que fundamenta a classificação; e
- d) data da produção, data da classificação e prazo da classificação;

III - relatório estatístico com a quantidade de pedidos de acesso à informação recebidos, atendidos e indeferidos; e

IV - informações estatísticas agregadas dos requerentes.

7.16.4. Orientações sobre o conteúdo do item de navegação “Informações Classificadas”.

- I. Texto de apresentação: deverá trazer um texto explicativo sobre o seu objetivo de atender aos incisos I e II, do art. 45, do Decreto nº 7724/2012.
- II. Apresentação das listas de informações classificadas e desclassificadas: deverá conter duas áreas específicas para a apresentação das listagens requeridas, com as seguintes nomenclaturas:
 - Lista de informações classificadas (atualizado em DD/MM/AAAA).
 - Lista de informações desclassificadas nos últimos 12 meses (atualizado em DD/MM/AAAA).

7.16.4.1. Conteúdo da área “Lista de informações desclassificadas”: Essa área deverá conter a lista dos documentos desclassificados nos últimos doze meses, conforme determina a Lei de Acesso à Informação. Recomenda-se, ainda, que se mantenha publicada a relação de informações desclassificadas em períodos anteriores, ver anexo 4 “LISTA DE INFORMAÇÕES DESCLASSIFICADAS”.

7.16.4.2. Sugere-se que a lista apresente, no mínimo, as seguintes informações acerca de cada documento desclassificado:

- I. Número Único de Protocolo (NUP).
- II. Grau do sigilo ao qual o documento ficou submetido.
- III. Data da produção.
- IV. Data da desclassificação.
- V. Tema ou assunto da informação.

7.16.5. Orienta-se que divulgue o tema e o assunto dos de que se trata a informação desclassificada com o intuito de aumentar a transparência em relação ao conteúdo dos documentos desclassificados. O objetivo é facilitar a identificação de documentos de interesses por parte da sociedade e jornalistas. O órgão ou

entidade pode, ainda, divulgar a razão para classificação contida no “Termo de Classificação da Informação” e o dispositivo legal que embasou a classificação.

7.16.6. A lista de informações classificadas deverá relacionar, obrigatoriamente, todas as informações com classificação formalizada por “Termo de Classificação da Informação” por parte do órgão ou entidade, como prevê o art. 28 da Lei nº 12.527/2011 e o art. 31 do Decreto nº 7.724/2012. Ou seja, qualquer informação com classificação válida existente no órgão/entidade deverá ser listada nesse rol.

7.16.6.1. O conteúdo dessa área deverá apresentar as seguintes informações:

- I. Código de Indexação de Documento que contém Informação Classificada (CIDIC).
- II. Categoria na qual se enquadra a informação.
- III. Indicação do dispositivo legal que fundamenta a classificação.
- IV. Data da produção da informação.
- V. Data da classificação.
- VI. Prazo da classificação.

7.16.6.2. Somente devem ser incluídas na “Lista de informações classificadas” as informações classificadas nos termos do §1º do art. 24 da Lei nº 12.527/2011, ou seja, como reservadas. Por isso, informações cujo sigilo seja devido a outras legislações (como fiscal e tributária), documentos preparatórios e informações pessoais não estão sujeitos aos termos de divulgação apresentados neste manual, ver anexo 5 “LISTA DE INFORMAÇÕES CLASSIFICADAS”.

7.17. FORMATO PARA PUBLICAÇÃO DAS LISTAGENS

7.17.1. A disponibilização das listagens deve observar o disposto no art. 8º, parágrafo 3, inciso II, da Lei de Acesso à Informação, ou seja, as informações devem ser publicadas em formatos “abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações”.

7.17.2. O formato (como, por exemplo: pdf, html, csv, ods etc.) a ser utilizado pode ser definido pelo próprio órgão ou entidade, considerando as normas e procedimentos internos de segurança da informação.

7.18. DESCLASSIFICAÇÃO, RECLASSIFICAÇÃO OU ALTERAÇÃO DOS PRAZOS DE SIGILO

7.18.1. A desclassificação, a reclassificação ou a alteração (redução ou prorrogação) do prazo de sigilo, deverá ser avaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício. Nesta avaliação deverão ser examinadas a permanência dos motivos do sigilo e a possibilidade de danos decorrentes do acesso ou da divulgação da informação.

8. DISPOSIÇÕES GERAIS

8.1. Tendo em vista que o acesso é a regra e o sigilo a exceção, os gestores da informação e as autoridades do Sistema Cofen/Conselhos Regionais de Enfermagem devem sempre privilegiar o acesso aos documentos e às informações.

8.2. Apenas em casos previstos na Constituição ou em normas infraconstitucionais é que será necessário classificar uma informação ou documento.

8.3. Nesses casos a autoridade classificadora deverá classificar a informação ou documento no grau menos restritivo possível, isto, de acordo com o risco que a divulgação da informação pode trazer para segurança da sociedade ou do Estado.

9. FORMULÁRIOS

9.1. Anexo 1 - Termo de Classificação de Informação (TCI)

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO (TCI)	
Unidade funcional:	
Código de indexação:	
Categoria de sigilo:	
Tipo de documento:	
Data de produção:	
Fundamento legal para classificação:	
Razões para a classificação: (idêntico ao grau de sigilo do documento)	
Prazo da restrição de acesso:	
Data de classificação:	
Autoridade Classificadora	Nome:
	Cargo:
Autoridade Ratificadora (quando aplicável)	Nome:
	Cargo:

Desclassificação em ____/____/____ (quando aplicável)	Nome:
	Cargo:
Reclassificação em ____/____/____ (quando aplicável)	Nome:
	Cargo:
Redução de prazo em ____/____/____ (quando aplicável)	Nome:
	Cargo:
Prorrogação de prazo em ____/____/____ (quando aplicável)	Nome:
	Cargo:

Assinatura da autoridade classificadora

Assinatura da autoridade ratificadora
(quando aplicável)

Assinatura da autoridade responsável por desclassificação
(quando aplicável)

Assinatura da autoridade responsável por reclassificação
(quando aplicável)

Assinatura da autoridade responsável por redução de prazo
(quando aplicável)

Assinatura da autoridade responsável por prorrogação de prazo
(quando aplicável)

9.2. Anexo 2 - Termo de Credenciamento para Acesso à Informação Sigilosa (TCAIS)

TERMO DE CREDENCIAMENTO PARA ACESSO À INFORMAÇÃO SIGILOSA (TCAIS)	
Categoria (sigiloso e pessoal):	
Grau de sigilo:	
Documento classificado:	
Modalidade de autorização de acesso: (exercício funcional, consulta, certidão, extrato ou cópia autenticada)	
Justificativa da autorização de acesso:	
Identificação da pessoa interessada	Nome:
	Cargo:
	Matrícula:
<p>Credenciado para acesso à informação sigilosa constante no documento identificado no presente termo, 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:</p> <p>a) tratar as informações pessoais ou classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo Sistema Cofen/Conselhos Regionais de Enfermagem e preservar o seu sigilo, de acordo com a legislação vigente;</p> <p>b) preservar o conteúdo das informações pessoais ou classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-lo a terceiros;</p> <p>c) não praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações pessoais ou classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito; e</p> <p>d) não copiar ou reproduzir, por qualquer meio ou modo:</p> <p> i. informações pessoais ou classificadas em qualquer grau de sigilo;</p> <p> ii. informações relativas aos materiais de acesso restrito do Sistema Cofen/Conselhos Regionais de Enfermagem, salvo autorização da autoridade competente.</p>	
Identificação do credenciado	Nome:
	Cargo:
	Matrícula:
Local e data:	

9.3. Anexo 3 - Termo de Compromisso de Manutenção de Sigilo (TCMS)

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (TCMS)

[Qualificação: nome, nacionalidade, CPF, identidade (número, data e local de expedição), filiação e endereço], perante o(a) [órgão ou entidade], 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 de informações pessoais, 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 pessoais ou classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo Sistema Cofen/Conselhos Regionais de Enfermagem e preservar o seu sigilo, de acordo com a legislação vigente;
- b) preservar o conteúdo das informações pessoais ou 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 pessoais ou 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 pessoais ou classificadas em qualquer grau de sigilo; e
 - ii. informações relativas aos materiais de acesso restrito do Sistema Cofen/Conselhos Regionais de Enfermagem, salvo autorização da autoridade competente.

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

[Brasília-DF, data e assinatura]

[Duas testemunhas identificadas]

9.4. Anexo 4 - Lista de informações desclassificadas

Conselho Federal de Enfermagem (Cofen)**Ano: XXXX****LISTA DE INFORMAÇÕES DESCLASSIFICADAS**

NUP	Data de Produção	Data de desclassificação	Grau de sigilo anterior	Fundamentação da desclassificação	Razões da classificação	Assunto do documento

9.5. Anexo 5 - Lista de informações classificadas

Conselho Federal de Enfermagem (Cofen)**Ano: XXXX****LISTA DE INFORMAÇÕES CLASSIFICADAS**

NUP	Data de Produção	Data de classificação	Grau de sigilo anterior	Fundamentação da desclassificação	Prazo de restrição de acesso	Fundamentação legal

10. APÊNDICES

Não há.