POLÍTICA DE CLASSIFICAÇÃO DE INFORMAÇÃO, SIGILO E TEMPORALIDADE DA EBSERH

EBSERH
HOSPITAIS UNIVERSITÁRIOS FEDERAIS

2021

Identificação geral

CNPJ	15.126.437/0001-43
Administração Central	Brasília-DF
Tipo de estatal	Empresa Pública
Acionista controlador	União
Tipo societário	Sociedade por Cotas de Responsabilidade Limitada – Empr Pública
Tipo de capital	Fechado
Abrangência de atuação	Nacional
Setores de atuação	Educação e Saúde
Presidente	**Oswaldo de Jesus Ferreira** Telefone: (61) 3255-8921 E-mail: oswaldo.ferreira@ebserh.gov.br
Auditor Interno	**Adriano Augusto de Souza** Telefone: (61) 3255-8970 E-mail: souza.adriano@ebserh.gov.br
Auditores independentes atuais da Empresa	Audilink & Cia. Auditores
Membros da Diretoria Executiva subscritores da Política de Proteção de Dados Pessoais da Ebserh	**Oswaldo de Jesus Ferreira** Cargo: Presidente CPF: ***.430.***-** **Eduardo Chaves Vieira** Cargo: Vice-Presidente CPF: ***.431.***-** **Giuseppe Cesare Gatto** Cargo: Diretor de Ensino, Pesquisa e Atenção à Saúde CPF: ***.214.***-** **Simone Henriqueta Cossetin Scholze** Cargo: Diretora de Tecnologia da Informação CPF: ***.824.***-** **Iara Ferreira Pinheiro** Cargo: Diretora de Orçamento e Finanças CPF: ***.894.***-** **Erlon Cesar Dengo** Cargo: Diretor de Administração e Infraestrutura CPF: ***.884.***-** **Rodrigo Augusto Barbosa** Cargo: Diretor de Gestão de Pessoas CPF: ***.368.***-**
Aprovação	129ª reunião do Conselho de Administração em 16/12/2021
Versão	1.0

POLÍTICA DE CLASSIFICAÇÃO DE INFORMAÇÃO, SIGILO E TEMPORALIDADE

Dispõe sobre a Política de Classificação de Informação, Sigilo e Temporalidade e documentos em grau de sigilo, a Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) e dá outras providências.

CAPÍTULO I
DO OBJETIVO E ESCOPO DA APLICAÇÃO

Art. 1º O objetivo da Política de Classificação de Informação, Sigilo e Temporalidade é estabelecer diretrizes para o acesso à informação, para a classificação das informações institucionais e definir o grau de sigilo e temporalidade dessas no âmbito da EBSERH, para fins do disposto na Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação e na Lei nº 13.709, de 14 e agosto de 2018 - Lei Geral de Proteção de Dados Pessoais.

§ 1º A publicidade desta Política é ostensiva e pública.

§ 2º Complementarmente, esta política visa a:

I – orientar a administração a responder pedidos de informação do cidadão;

II – preservar o sigilo das informações classificadas;

III – estabelecer procedimentos para a desclassificação; e

IV – estabelecer critérios para definir a temporalidade das informações, dos documentos e dos processos no âmbito da Rede.

Art. 2º A Política de Classificação de Informação, Sigilo e Temporalidade abrange todas as informações, os documentos e os processos desta Estatal, incluídos os do Sistema Eletrônico de Informações – SEI e aplica-se a todas as unidades e aos colaboradores que integrem a Rede EBSERH – Administração Central, e aos Hospitais Universitários Federais filiados.

Art. 3º No âmbito da Rede EBSERH, a publicidade deve ser preceito geral e o sigilo, a exceção.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 4º Para fins desta Política, as seguintes definições são consideradas:

I - dado pessoal - informação relacionada a pessoa natural identificada ou identificável;

II - 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;

III - grau de sigilo - nível de classificação de informações, processos e documentos;

IV - informação classificada - informação contida em documentos e processos, definida em grau de sigilo e nível de acesso estabelecido por lei e que pode ser somente parte ou constituir integralmente um documento ou processo, que será classificado por integração;

V – informação pública - aquela de livre divulgação e acesso pelos cidadãos, disponibilizada por meio da transparência ativa ou passiva;

VI – informação restrita - protegida por legislação específica, cujo acesso será restrito a determinadas pessoas e não necessitam receber o tratamento dado às informações classificadas em grau de sigilo;

VII - informação sigilosa - aquela classificada temporariamente como ultrassecreta, secreta ou reservada, em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, nos termos estabelecidos pela Lei nº 12.527, de 2011;

VIII - Lista de Intenção de Classificação de Informações (LICI) - lista de informações para as quais se pretende estabelecer classificação e que, após aprovada pela autoridade classificadora, comporá o rol anual de informações classificadas da Rede EBSERH;

IX - nível de acesso - grau de permissão para o conhecimento da informação ou do documento classificado;

X - nível de acesso SEI! - nível de classificação de informações, documentos e processos que permite a visualização do conteúdo no SEI!, por usuários credenciados, de maneira individual ou coletiva, podendo ser público, restrito e sigiloso;

XI - prazo de guarda - tempo necessário para que os conjuntos documentais atendam às necessidades da administração que os produziu e cumpram as finalidades para as quais foram criados, devendo ser definido, preferencialmente, em anos. Constitui-se de fase corrente e fase intermediária;

XII - Sistema Eletrônico de Informação (SEI!) – ferramenta de gestão eletrônica de informações, documentos e processos;

XIII - transparência ativa - princípio que exige de órgãos e entidades públicas a divulgação de informações de interesse coletivo e geral, independentemente de serem solicitadas;

XIV - transparência passiva - permissão de acesso à informação a partir de solicitações específicas, por meio de procedimentos e prazos previstos na Lei de Acesso à Informação (LAI) e em sua regulamentação; e

XV- tratamento da informação classificada - conjunto de ações referentes à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, ao transporte, à transmissão, à distribuição, ao arquivamento, ao armazenamento, à eliminação, à avaliação, à destinação ou ao controle de informação classificada em qualquer grau de sigilo.

CAPÍTULO III
DO ACESSO À INFORMAÇÃO PÚBLICA

Art. 5º Toda informação pública está sujeita à publicidade.

Parágrafo único. O requerimento de acesso à informação e a obtenção de resposta da Rede EBSERH são direitos do cidadão.

Art. 6º O acesso à informação visa a aumentar a eficiência da Empresa, prevenir a corrupção, elevar a participação social e fortalecer a gestão pública.

Art. 7º A informação produzida, guardada, organizada e gerenciada pela Rede EBSERH é pública e o acesso a ela deve ser restringido nos casos específicos previstos em lei.

Art. 8º Entende-se por informação pública aquela que não se enquadra em hipóteses de sigilo ou restrição e que:

I - seja produzida ou acumulada por órgãos e entidades públicas;

II - seja produzida ou mantida por pessoa física ou jurídica decorrente de um vínculo com órgãos e entidades públicas;

III - disponha sobre atividades de órgãos e entidades, inclusive a relativa à sua política, organização e serviços;

IV - seja pertinente ao patrimônio público, utilização de recursos públicos, licitação e contratos; e

V - disponha sobre políticas públicas, inspeções, auditorias, prestações e tomadas de contas.

Parágrafo único. A Ouvidora-Geral é o canal de acesso da informação pelo cidadão.

Art. 9º Para garantir a efetividade do acesso à informação pública, deve ser observado um conjunto de padrões estabelecidos com base nos melhores critérios e nas práticas internacionais, destacando-se os seguintes princípios:

I - limitação da classificação de sigilo;

II - facilitação ao acesso à informação;

III - gratuidade da informação;

IV - extensão do direito a qualquer interessado;

V - identificação razoável do demandante; e

VI - prescindibilidade de justificativa para pedido de acesso.

Art. 10. Podem ser obtidas sem consulta prévia sobre classificação de sigilo:

I - orientações sobre os procedimentos para obter o acesso e sobre o local onde a informação poderá ser obtida;

II - informação ou documentos ostensivos, produzidos ou acumulados por suas unidades, recolhidos, ou não, a arquivos públicos; e

III - informação produzida ou mantida por pessoa física ou entidade privada decorrente de vínculo com seus órgãos ou entidades, mesmo que esse vínculo já tenha terminado, respeitando-se a privacidade dos dados pessoais.

§ 1º Prontuários médicos e dados pessoais devem ser considerados restritos, exceto se houver consentimento expresso do paciente, do titular de dados ou determinação judicial.

§ 2º Informações eletrônicas ou físicas classificadas como restritas ou sigilosas, conforme a classificação do art. 29, poderão ser reveladas com a seleção da informação a ser encaminhada, tarjando-se ou utilizando-se de outro meio para preservar o trecho classificado, segundo o gestor da área demandada e ouvida a CPADS.

Art. 11. Não são considerados pedidos de informação:

I - desabafos, reclamações, elogios ou solicitações de providência, que devem ser formalizados à Ouvidoria;

II - consultas sobre a aplicação de legislação;

III - denúncias sobre a aplicação da LAI no âmbito do Poder Executivo Federal, que devem ser registradas no portal da Controladoria-Geral da União; e

IV - quaisquer outros assuntos não contemplados nesta Política, que devem ser encaminhados à Ouvidoria local, nos HUFs, ou à Ouvidoria-Geral, na Administração Central da EBSERH.

Art. 12. Não serão atendidos pedidos de acesso à informação genéricos, desproporcionais ou desarrazoados.

CAPÍTULO IV
DA RESTRIÇÃO DE ACESSO ÀS INFORMAÇÕES

Art. 13. As restrições de acesso à informação são instituídas para garantir que as informações excepcionalmente restritas sejam acessíveis apenas às instâncias legalmente competentes para acessá-las, conforme o disposto na legislação específica.

Art. 14. As informações pessoais não são públicas e têm seu acesso restrito, independentemente de classificação de sigilo, pelo prazo máximo de 100 (cem) anos, a contar da sua data de produção, ou seja, não necessitam receber o tratamento dado às informações classificadas em grau de sigilo, mas, sim, conforme o que regra a Lei Geral de Proteção de Dados Pessoais (LGPD).

§1º A divulgação das informações pessoais deve ser feita de forma transparente, respeitando-se a intimidade, a vida privada, a honra e a imagem, bem como as liberdades e as garantias individuais.

§2º Somente terão acesso à informação pessoal os agentes públicos autorizados e as pessoas a quem a informação se referir.

§3º Havendo previsão legal ou consentimento expresso da pessoa a quem a informação faz referência, terceiros poderão ter acesso a tais informações.

Art. 15. Serão classificadas no nível de acesso restrito, sem prejuízo das demais proteções previstas em lei específica, as informações que comprometam as atividades de investigação ou fiscalização em andamento, relacionadas à prevenção ou repressão de infrações.

Art. 16. Informações classificadas no SEI! deverão atender às legislações específicas listadas pelo sistema para estabelecimento da restrição ou do sigilo e não devem ser classificadas em nenhum dos graus de sigilo previstos no art. 29.

Ar. 17. Os processos correcionais deverão receber a classificação no SEI! como sigiloso.

Parágrafo único. Os documentos integrantes dos processos correcionais deverão receber, preferencialmente, a classificação SEI! como “restrito”, podendo receber a classificação SEI! como público, este a critério do colaborador e em observância ao disposto na LAI e na LGPD.

Art. 18. As informações classificadas protegidas por legislação específica deverão ser documentadas em cada unidade por elas responsáveis e compor seu processo de trabalho.

CAPÍTULO V
CLASSIFICAÇÃO DAS INFORMAÇÕES SIGILOSAS E TEMPORALIDADE

Seção I
Das Disposições Gerais

Art. 19. A informação produzida em documentos oficiais somente pode ser classificada como sigilosa nas hipóteses previstas no art. 23 da Lei de Acesso à Informação, tais como quando for considerada imprescindível à segurança da sociedade, à vida, à segurança ou à saúde da população ou do Estado, à soberania nacional, à integridade do território nacional e ao risco às relações internacionais.

Parágrafo único. As informações e os documentos que não versem sobre os assuntos de que trata o **caput** podem receber a restrição ou o sigilo estabelecidos em legislações específicas.

Art. 20. A informação pode ser classificada como sigilosa somente em parte do documento, de modo que ao interessado será assegurado o acesso à parte não sigilosa, com ocultação da parte sob sigilo com tarjas ou outra forma de preservar a informação classificada.

Art. 21. Para a classificação da informação em determinado grau de restrição ou sigilo, deve-se observar o interesse público da informação utilizar o critério menos restritivo possível e considerar a imprescindibilidade prevista no art. 18.

Art. 22. Verificada a necessidade de classificação da informação e identificada a respectiva justificativa legal, a autoridade competente deve formalizar a decisão no Termo de Classificação de Informação (TCI), conforme modelo disposto no Anexo I.

§1º O TCI é o formulário onde se registra, dentre outros dados, o grau de sigilo, a categoria na qual se enquadra a informação, o tipo de documento, as razões da classificação, o prazo de sigilo ou o evento que definirá o seu término, o fundamento da classificação e a identificação da autoridade classificadora.

§2º Após preenchido e assinado, o TCI deve seguir anexo à informação classificada.

§3º O TCI deve ser formalizado para documentos classificados antes e durante a produção dos efeitos da LAI, respeitadas as atuais regras de prazos de restrição e de autoridade competente, inclusive para efeito de desclassificação, reclassificação ou reavaliação.

§4º O conteúdo do TCI é informação pública e tem acesso ostensivo, com exceção do campo razões para a classificação, que terá o mesmo grau de sigilo da informação classificada e deverá ser ocultado para fins de acesso ao Termo.

Art. 23. O rol de informações classificadas no âmbito da Administração Central e em cada Hospital Universitário Federal filiado deve relacionar todas as informações com classificação em grau de sigilo, ou seja, as formalizadas por TCI e deve conter:

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; e

VI - prazo da classificação.

Parágrafo único. Somente devem ser incluídas nesse rol as informações classificadas como reservadas, secretas ou ultrassecretas.

Art. 24. Na hipótese de documento ou processo que contenha informações classificadas em diferentes graus de sigilo, deve ser atribuído o grau de sigilo mais elevado, assegurado o acesso às partes não classificadas ou desclassificadas por meio de certidão, extrato ou cópia.

Art. 25. Quando o colaborador julgar necessário tramitar informação classificada fora do SEI!, deverá iniciar um processo sigiloso e incluir um despacho público:

I - o interessado;

II - a data;

III - o assunto genérico;

IV - que a informação é classificada;

V - a legislação específica; e

VI - se possível:

a) o artigo desta Política;

b) o grau de sigilo;

c) o prazo de guarda;

d) a destinação final do documento; e

e) que tramitará fisicamente fora do SEI!.

Parágrafo único. Se parte de um processo eletrônico com informação classificada tiver que tramitar fora do SEI!, o procedimento do parágrafo anterior será aplicado no referido processo.

Art. 26. Subsídios para o tratamento de informação classificada, na Administração Central da EBSERH, que tenham origem nos Hospitais Universitários filiados, serão providos pelas Superintendências destes.

Art. 27. O nível de acesso a determinado grau de sigilo é equivalente ao da competência da autoridade classificadora conforme o art. 31.

§1º O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS), constante do Anexo III, documento pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

§2º Todos os colaboradores da Rede EBSERH, sejam celetistas, de regime jurídico único, precarizados ou terceirizados, devem ser signatários do TCMS.

Art. 28. Para fins de temporalidade, fica estabelecido o previsto na tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal, do Código de Classificação e Tabela de Temporalidade e Destinação de Documentos Relativos às Atividades-meio do Poder Executivo Federal, do Conselho Nacional de Arquivos - CONARQ.

§ 1º A EBSERH estabelecerá o seu próprio Código de Classificação e Tabela de Temporalidade e Destinação de Documentos Relativos às Atividades-fim, com atenção aos códigos do Ministério da Educação e do Ministério da Saúde.

§ 2º A atualização dos prazos de guarda deverá seguir o que for estabelecido pelo CONARQ.

Seção II
Dos Graus e Prazos de Sigilo

Art. 29. Os graus de sigilo são classificados conforme o risco decorrente de sua exposição e podem ser de três níveis:

I - ultrassecreto - com prazo de restrição de até 25 (vinte e cinco) anos, prorrogável uma única vez;

II - secreto - com prazo de restrição de até 15 (quinze) anos, não prorrogável; e

III – reservado - com prazo de restrição de até 05 (cinco) anos, não prorrogável.

Parágrafo único. Documentos reservados, secretos e ultrassecretos não devem tramitar no SEI! e devem ser removidos e destruídos, caso não seja possível sua guarda segura.

Art. 30. A classificação em grau de sigilo deve ser realizada quando a informação for gerada ou, posteriormente, quando necessária.

§ 1º O documento pode ser considerado como classificável quando de um pedido de informação nele contido, no todo ou em parte.

§ 2º As informações cujo sigilo se deva a outras legislações, documentos preparatórios e informações pessoais não devem ser classificadas nos graus referidos no art. 29.

Seção III
Da Competência

Art. 31. A decisão quanto à classificação do sigilo das informações é de competência:

I - no grau ultrassecreto - do Presidente da República, do Vice-Presidente da República e do Ministro de Estado;

II - no grau secreto - das autoridades previstas no inciso I e do Presidente da EBSERH; e

III - no grau reservado - das autoridades previstas nos incisos I e II, dos Diretores, do Chefe de Gabinete da Presidência da EBSERH e dos Superintendentes dos Hospitais Universitários Federais da Rede EBSERH.

§ 1º A área técnica que produziu a informação possui competência inicial para indicar o seu grau de sigilo, assim como a temporalidade, desde que com observância às legislações específicas.

§ 2º Os Superintendentes dos Hospitais Universitários Federais filiados podem delegar a competência para classificação no grau reservado aos Gerentes, sendo vedada a subdelegação.

§ 3º É vedada a delegação de competência de classificação nos graus de sigilo ultrassecreto ou secreto.

§ 4º Caso o documento seja entendido como ultrassecreto, o TCI deve ser encaminhado ao Ministro da Educação para conhecimento e providências cabíveis.

§ 5º Quando o documento for classificado como secreto, o Presidente da EBSERH deverá encaminhar, por intermédio da Secretaria-Geral, cópia do TCI à Comissão Mista de Reavaliação de Informações (CMRI) (art. 35, §1º da LAI), no prazo de 30 (trinta) dias corridos.

§ 6º Caso o Presidente da EBSERH, os Diretores, a Chefia de Gabinete da Presidência da EBSERH e os Superintendentes dos Hospitais Universitários Federais da Rede EBSERH entendam que o documento tenha classificação superior à que está no âmbito das respectivas competências, deverá manter o sigilo da informação, reclassificar, encaminhar à autoridade superior para conhecimento e adotar as demais providências cabíveis, a exemplo da destruição, guarda segura ou imposição de sigilo no SEI!.

§ 7º Se a autoridade de nível superior entender que um subordinado seu deva tomar conhecimento de documento que só a si lhe cabe, deverá providenciar a elaboração de TCMS sigilo específico para aquela informação ou aquele documento.

Seção IV
Da Reavaliação e Desclassificação

Art. 32. A desclassificação, a reclassificação e as alterações do prazo de sigilo são resultantes da reavaliação da informação classificada.

Art. 33. A classificação da informação deve ser reavaliada pelo colaborador que a classificou ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, de acordo com a legislação aplicável.

Art. 34. A classificação da informação deve ser reavaliada pelo colaborador que a classificou ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, para desclassificação ou redução do prazo de sigilo, em conformidade com a legislação aplicável.

§ 1º Para o cumprimento do disposto no **caput** deverá ser observado:

I - o prazo máximo de restrição de acesso à informação;

II - a permanência das razões da classificação;

III - a possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação; e

IV - a peculiaridade das informações produzidas no exterior por autoridades ou agentes públicos.

§ 2º A revisão pelos órgãos classificadores das informações classificadas no grau ultrassecreto ou secreto deve ser feita, no máximo, a cada 2(dois) anos, conforme dispõe o art. 39 da Lei 12.527, de 2011, a fim de subsidiar a CMRI.

§ 3º O prazo para revisão de ofício das informações classificadas no grau ultrassecreto ou secreto pela CMRI é de 04 (quatro) anos.

Art. 35. A decisão de desclassificação, reclassificação ou alteração de prazo de sigilo deve ser formalizada em TCI, conforme o CIDIC – Categorias, constante do Anexo II.

§ 1º Para cada alteração na classificação da informação, deve-se abrir um novo TCI, com o respectivo código de indexação de documento.

§ 2º A motivação do referido ato deve ser realizada complementando-se o TCI, no campo razões para classificação e um novo Termo deve ser anexado à informação classificada, junto ao TCI anterior, a fim de manter o histórico da classificação.

Art. 36. A reclassificação da informação pode ser feita por autoridade competente para a classificação no novo grau de sigilo, observado o prazo máximo de restrição de acesso desse novo grau de classificação.

Art. 37. O novo prazo de restrição manterá a data da produção da informação e, verificada a necessidade de reclassificá-la em grau secreto, alterar-se-á o prazo de restrição da informação, contado a partir da data de sua produção, a qual não muda.

Art. 38. Após a reavaliação, verificado que não existem as razões da classificação, a informação deve ser desclassificada.

Art. 39. O rol das informações desclassificadas deve apresentar, no mínimo, as seguintes informações:

I - Número Único de Protocolo (NUP) ou outro identificador que o substitua;

II - grau de sigilo ao qual o documento ou o processo ficou submetido; e

III - breve resumo do documento desclassificado.

§ 1º A informação classificada em qualquer grau de sigilo ou o documento que a contenha, quando de sua desclassificação, manterá apenas o Número Único de Protocolo (NUP) ou outro identificador que o substitua, utilizado para controle dos documentos, avulsos ou processos, produzidos ou recebidos pela EBSERH.

§2º Na hipótese de prorrogação do prazo, a competência é exclusiva CMRI, que pode fazê-la por uma única vez, por período determinado e somente quanto à informação classificada no grau ultrassecreto.

Seção V
Das Comissões Permanentes de Avaliação de Documentos Sigilosos (CPADS)

Art. 40. Todas as Unidades integrantes da Rede EBSERH deverão compor uma CPADS para orientar e realizar o processo de análise, avaliação e seleção dos documentos produzidos e acumulados no seu âmbito de atuação, garantindo a sua destinação final, nos termos da legislação vigente e das normas do Sistema de Gestão de Documentos de Arquivo, do Arquivo Nacional.

Art. 41. A constituição das CPADS deverá atender ao descrito no art. 11 do Decreto 10.148, de 2 de dezembro de 2019.

Art. 42. A CPADS assessorará as autoridades mencionadas nos incisos II e III do **caput** do art. 29 quanto à classificação, à desclassificação, à reclassificação ou à reavaliação da informação classificada em qualquer grau de sigilo, sem prejuízo das demais atribuições que lhe competem.

Art. 43. A CPADS, por delegação do Presidente, deverá manter atualizada a Lista de Intenção de Classificação de Informações (LICI), no sítio eletrônico da Empresa, a partir dos TCI informados em cada Hospital Universitário Federal filiado, após a apreciação e determinação do Presidente da EBSERH.

Parágrafo único. O Hospital Universitário Federal filiado deverá propor a atualização das informações classificadas e desclassificadas ao Presidente, até 30 dias antes da publicação prevista no **caput**.

Art. 44. À CPADS caberá a recepção dos TCIs e composição da LICI para encaminhamento e apreciação de justificativa de classificação pela autoridade classificadora.

CAPÍTULO VII
DISPOSIÇÕES FINAIS

Art. 45. A área gestora desta Política é a Secretaria-Geral da Presidência da EBSERH, que contará, para fins consultivos e executivos, com a CPADS da Administração Central.

Art. 46. A Secretaria-Geral deve divulgar anualmente, até o dia 1º de junho, o rol das informações classificadas e desclassificadas em cada grau de sigilo em seu portal oficial na internet que deverá conter:

I - código de indexação de documento;

II - categoria na qual se enquadra a informação;

III - indicação de dispositivo legal que fundamenta a classificação;

IV - data da produção; e

V - data e prazo da classificação.

Art. 47. Em relação ao tratamento da informação em ambiente de computação em nuvem, a Rede EBSERH, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as seguintes diretrizes:

I - informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II - informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e

III - poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a) a informação com restrição de acesso prevista em legislação específica;

b) o material de acesso restrito regulado pelo próprio órgão ou pela entidade;

c) a informação pessoal relativa à intimidade, vida privada, honra e imagem; e

d) o documento preparatório não previsto no inciso II do **caput**.

Art. 48. A introdução de novas tecnologias, particularmente as relacionadas aos programas de tecnologia da informação, pode refletir sobre esta Política, a qual deverá ser revisada a cada 2 (dois) anos ou, eventualmente, a cada novo produto agregado para os fins a que se destina.

Art. 49. São consideradas condutas ilícitas:

I – acesso a informações pessoais sem permissão e uso inadequado destas;

II – recusa de fornecimento de informações requeridas nos termos da lei;

III – destruição ou alteração de documentos sem fundamento legal; e

IV – imposição de sigilo a documento para obtenção de proveito pessoal.

Parágrafo único. Deverá haver a responsabilização administrativa, cível e penal do responsável pelo cometimento de ato ilícito acima listado, podendo caracterizar, também, improbidade administrativa

Art. 50. Os casos omissos ou não previstos nesta Política devem ser direcionados à CPADS para análise e encaminhamentos pertinentes.

Art. 51. Esta Política entra em vigor na data de sua publicação.

ANEXO I

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO

ÓRGÃO/ENTIDADE:

CÓDIGO DE INDEXAÇÃO:

GRAU DE SIGILO:

CATEGORIA:

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 e Cargo)

DESCLASSIFICAÇÃO em ___/___/_____ (quando aplicável) (Nome e Cargo)

RECLASSIFICAÇÃO em ___/___/_____ (quando aplicável) (Nome e Cargo)

REDUÇÃO DE PRAZO em ___/___/_____ (quando aplicável) (Nome e Cargo)

PRORROGAÇÃO DE PRAZO em ___/___/_____ (quando aplicável) (Nome e Cargo)

Assinatura da AUTORIDADE CLASSIFICADORA _____

Assinatura da Autoridade Classificadora responsável por DESCLASSIFICAÇÃO (quando aplicável) _____

Assinatura da Autoridade Classificadora responsável por RECLASSIFICAÇÃO (quando aplicável) _____

Assinatura da Autoridade Classificadora responsável por REDUÇÃO DE PRAZO (quando aplicável) _____

Assinatura da Autoridade Classificadora responsável por PRORROGAÇÃO DE PRAZO (quando aplicável) _____

Obs.:

1. O TCI deve ser realizado de forma legível e correta.

2. As informações devem ser claras, objetivas e sucintas, para o TCI permanecer com, no máximo, duas páginas (frente e verso).

3. O classificador deve preencher o formulário conforme se segue:

a. cabeçalho: identificar o órgão/unidade e seu respectivo endereço, telefone e e-mail para contato;

b. órgão/entidade: identificar o órgão/unidade classificador;

c. código de indexação: informar o CDIC;

d. grau de sigilo: indicar o grau de classificação de sigilo da informação – reservado, secreto, ultrassecreto, sigiloso (SEI!) e restrito (SEI!). Após selecionado, no formulário eletrônico, o grau de sigilo será exibido no canto superior direito do TCI;

e. categoria: identificar o código numérico da categoria na qual se enquadra a informação que está sendo classificada;

f. tipo de documento: descrever o documento, identificando-o;

g. data de produção: identificar a data em que o documento/processo foi produzido;

h. fundamento legal para classificação: identificar o dispositivo legal que fundamenta a classificação, dentre os estabelecidos nas alíneas abaixo:

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

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

3) prejudicar ou pôr em risco informações fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

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

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

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

7) 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, observado o disposto no inciso II do **caput** do art. 6º;

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

9) comprometer atividades de inteligência, de investigação ou de fiscalização em andamento, relacionadas com prevenção ou repressão de infrações;

i. razões para classificação - demonstrar como a informação se enquadra à hipótese legal, observados os critérios abaixo:

1) a gravidade do risco ou dano à segurança da sociedade e do Estado; e

2) o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final;

j. quando houver decisão de desclassificação, reclassificação ou alteração do prazo de sigilo, o campo razões para qualificação, deverá ser complementado com a motivação da respectiva decisão em novo TCI;

k. prazo da restrição de acesso: indicar o prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu término;

l. data de classificação: identificar a data em que o documento/processo foi classificado com grau de sigilo;

m. autoridade classificadora: identificar (nome e cargo) a autoridade competente para classificar, de acordo com o grau de sigilo;

n. autoridade ratificadora (quando aplicável): identificar (nome e cargo) o Ministro de Estado, no prazo de 30 dias a partir da classificação. É necessária somente quando se tratar de informação classificada no grau ultrassecreto;

o. desclassificação em (quando aplicável): informar a data, bem como nome e cargo da autoridade competente, mediante decisão de desclassificação da informação;

p. reclassificação em (quando aplicável): informar a data, bem como nome e cargo da autoridade competente, mediante decisão de reclassificação da informação;

q. redução de prazo em (quando aplicável): informar a data, bem como nome e cargo da autoridade competente, mediante decisão de redução de prazo de classificação da informação; e

r. prorrogação de prazo em (quando aplicável): informar a data, bem como nome e cargo da autoridade competente, mediante decisão de prorrogação de prazo de classificação da informação. Somente informações classificadas em grau de sigilo ultrassecreto podem ter seus prazos prorrogados.

ANEXO II

CÓDIGO DE INDEXAÇÃO DE DOCUMENTO QUE CONTÉM

INFORMAÇÃO CLASSIFICADA – CATEGORIAS

Nr	Categoria	Código Numérico
1		
2		
3		
4		
5		
6		

Observações quanto à composição da CIDIC:

1. a primeira parte do CIDIC será composta pelo NUP, originalmente cadastrado conforme normativa de gestão documental;

2. a informação classificada ou o documento que a contenha, quando de sua desclassificação, manterá apenas o NUP;

3. não serão usadas tabelas de classificação de assunto ou de natureza do documento, em razão de exigência de restrição temporária de acesso à informação classificada, sob pena de pôr em risco sua proteção e confidencialidade;

4. a segunda parte do CIDIC será composta dos seguintes elementos:

a. grau de sigilo: indicação do grau de sigilo, ultrassecreto (U), secreto (S), reservado (R), Sigiloso (SEI!) ou Restrito (SEI!) com as iniciais na cor vermelha, quando possível;

b. categorias: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE) (https://www.gov.br/governodigital/pt-br/governanca-de-dados/vcge_2_1_0.pdf);

c. data de produção da informação classificada, conforme a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos);

d. data de desclassificação da informação classificada em qualquer grau de sigilo, 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:

1) reclassificação da informação resultante de reavaliação; e

2) primeiro registro da classificação; e

f. indicação da data de prorrogação da manutenção da classificação, com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível.

ANEXO III

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

[Qualificação: nome, nacionalidade, CPF, identidade (nº, 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 me comprometo a guardar o sigilo necessário, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e a:

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

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

[**Local, data e assinatura**]

[**Duas testemunhas identificadas**]