



UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA

Comitê de Governança Digital

NORMA COMPLEMENTAR Nº 1/2021

Estabelece as normas de classificação da informação em ambientes de Computação em Nuvem no âmbito da UFRA.

O **Comitê de Governança Digital (CGD-UFRA)** da Universidade Federal Rural da Amazônia – UFRA, no uso de suas atribuições regimentais e considerando a necessidade de se salvaguardar dados, informações e serviços sob sua responsabilidade e, ainda, considerando:

- A Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- O Decreto nº 7.724, de 16 de maio de 2012;
- A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais);
- A Norma Complementar 14/IN01/DSIC/SCS/GSIPR, de 14 de março de 2018;
- A Resolução nº 55 CONSAD, de 04 de julho de 2014, que aprova as diretrizes da Política de Segurança da Informação e Comunicações (PoSIC) no âmbito da UFRA; e
- A Portaria GSI/PR nº 93, de 26 de setembro de 2019 (Glossário de Segurança da Informação).

RESOLVE estabelecer diretrizes e normas para a classificação das informações a serem utilizadas em ambientes de Computação em Nuvem, no âmbito da UFRA, nos seguintes termos:

- Art. 1º. Para os efeitos desta Norma, e em consonância com a legislação vigente, e tendo por fonte o Glossário de Segurança da Informação do GSI/PR, conceitua-se como:
- I. informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
 - II. documento - unidade de registro de informações, qualquer que seja o suporte ou formato;
 - III. informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
 - IV. informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;
 - V. tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
 - VI. disponibilidade - qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
 - VII. integridade - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

- VIII. confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;
- IX. autenticidade - propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade, devidamente autorizado ou credenciado para tal;
- X. documento preparatório - documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas.
- XI. computação em nuvem - modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços.
- XII. APF - Administração Pública Federal.
- XIII. DICA - Abreviação para os princípios Disponibilidade, Integridade, Confidencialidade e Autenticidade.
- Art. 2º. A classificação das informações produzidas pela UFRA observa a publicidade como preceito geral, sendo a eventual atribuição de sigilo uma exceção.
- Art. 3º. Compete aos dirigentes das Unidades Administrativas, Acadêmicas e demais órgãos da UFRA a classificação prévia de todas as informações que serão produzidas, enviadas, tratadas, compartilhadas e/ou armazenadas nos ambientes de Computação em Nuvem, assegurados os direitos e garantias fundamentais no tratamento das informações pessoais e normativas internas e externas vigentes.
- Art. 4º. As informações produzidas pela UFRA e que sejam passíveis de utilização em ambiente em nuvem classificam-se nos graus de confidencialidade público, reservado, secreto, pessoal e sigiloso.
- §1º. Classifica-se como **pública** a informação cujo acesso pode ser franqueado a qualquer pessoa.
- §2º. Classifica-se como **reservada** ou **secreta** a informação imprescindível à segurança da sociedade ou do Estado, nos termos do art. 6º desta Norma.
- §3º. Classifica-se como **pessoal** a informação que diz respeito à intimidade, à vida privada, à honra e à imagem da pessoa, bem como às liberdades e garantias individuais.
- §4º. Classifica-se como **sigilosa** a informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo.
- §5º. A descrição detalhada dos níveis de classificação, conforme previstos na Norma Complementar 14/IN01/DSIC/SCS/GSIPR, pode ser encontrada no Anexo I desta Norma.
- Art. 5º. Para a classificação da informação em grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível, considerados:
- I. a gravidade do risco ou dano à segurança da sociedade e do Estado; e
 - II. o prazo máximo de classificação em grau de sigilo ou o evento que defina seu termo final.
- Art. 6º. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação pela UFRA nos graus de confidencialidade reservado ou secreto, as informações cuja divulgação ou acesso irrestrito possam:
- I. pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
 - II. pôr em risco a vida, a segurança ou a saúde da população;

- III. 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;
- IV. pôr em risco a segurança da Universidade ou demais instituições da Administração Pública, suas autoridades e seus familiares.

Parágrafo único. Os prazos máximos de restrição de acesso à informação, conforme a classificação prevista no caput, vigoram a partir da data de sua produção e são os seguintes:

- I. secreta: 15 (quinze) anos; e
- II. reservada: 5 (cinco) anos.

Art. 7º. A classificação de informação em qualquer grau de sigilo deverá ser formalizada por meio de decisão que conterà, no mínimo, os seguintes elementos:

- I. assunto sobre o qual versa a informação;
- II. fundamento da classificação, observados os critérios estabelecidos no art. 6º;
- III. indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, conforme limites previstos no parágrafo único do art. 6º; e
- IV. identificação da autoridade que a classificou.

Parágrafo único. A decisão referida no caput será mantida no mesmo grau de sigilo da informação classificada.

Art. 8º. A decisão que classificar a informação em qualquer grau de sigilo deverá ser formalizada no Termo de Classificação de Informação - TCI, conforme modelo contido no Anexo II, e conterà o seguinte:

- I. código de indexação de documento;
- II. grau de sigilo;
- III. categoria na qual se enquadra a informação;
- IV. tipo de documento;
- V. data da produção do documento;
- VI. indicação de dispositivo legal que fundamenta a classificação de acordo com os incisos de I a IV do art. 6º;
- VII. razões da classificação, observados os critérios estabelecidos no art. 5º;
- VIII. indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no parágrafo único do art. 6º;
- IX. data da classificação; e
- X. identificação da autoridade que classificou a informação.

§ 1º O TCI seguirá anexo à informação.

§ 2º As informações previstas no inciso VII do caput deverão ser mantidas no mesmo grau de sigilo que a informação classificada.

Art. 9º. Na hipótese de documento que contenha informações classificadas em diferentes graus de sigilo, será atribuído ao documento tratamento do grau de sigilo mais elevado, ficando assegurado o acesso às partes não classificadas por meio de certidão, extrato ou cópia, com ocultação da parte sob sigilo.

Art. 10. A UFRA poderá constituir Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS, com as seguintes atribuições:

- I. opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo;
- II. assessorar a autoridade classificadora ou a autoridade hierarquicamente superior quanto à desclassificação, reclassificação ou reavaliação de informação classificada em qualquer grau de sigilo;
- III. propor o destino final das informações desclassificadas, indicando os documentos para guarda permanente, observado o disposto na Lei nº 8.159, de 8 de janeiro de 1991; e

IV. subsidiar a elaboração do rol anual de informações desclassificadas e documentos classificados em cada grau de sigilo, a ser disponibilizado na Internet.

Art. 11. A classificação das informações será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, com vistas à sua desclassificação ou à redução do prazo de sigilo;

§ 1º A reavaliação a que se refere o caput deverá considerar as peculiaridades das informações produzidas por autoridades ou agentes públicos.

§ 2º Na reavaliação a que se refere o caput, deverão ser examinadas a permanência dos motivos do sigilo e a possibilidade de danos decorrentes do acesso ou da divulgação da informação.

§ 3º Na hipótese de redução do prazo de sigilo da informação, o novo prazo de restrição manterá como termo inicial a data da sua produção.

Art. 12. Orientações complementares e eventuais casos omissos atinentes à classificação da informação deverão ser esclarecidos através dos dispositivos legais e normativos que norteiam esta norma.

Art. 13. Este documento passa a compor a Política de Segurança da Informação e Comunicação - PoSIC da UFRA.

Belém, 30 de março de 2021.

ANEXO I – ITENS DA NORMA COMPLEMENTAR NO 14/IN01/DSIC/SCS/GSIPR



MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Item da NC 14	Nível de classificação	Detalhamento
5.2.1	Informação sem restrição de acesso	Pode ser tratada, a critério do órgão ou entidade da APF , em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC.
5.2.2	Informação sigilosa	Como regra geral, deve ser evitado o tratamento em ambiente de computação em nuvem, conforme disposições a seguir:
5.2.2.1	Informação classificada	É vedado o tratamento em ambiente de computação em nuvem
5.2.2.2	Conhecimento e informação contida em material de acesso restrito	É vedado o tratamento em ambiente de computação em nuvem
5.2.2.3	Informação com restrição de acesso prevista em legislação vigente	A critério do órgão ou entidade da APF , pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a disponibilidade, integridade, confidencialidade e autenticidade (DICA)
5.2.2.4	Documento Preparatório * * Documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas. Lei 7.724, Art. 3º, XII.	A critério do órgão ou entidade da APF , pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA.
5.2.2.5	Documento preparatório que possa originar informação classificada	Deve ser tratado conforme o item 5.2.2.1. É vedado o tratamento em ambiente de computação em nuvem
5.2.2.6	Informação pessoal relativa à intimidade, vida privada, honra e imagem	A critério do órgão ou entidade da APF , pode ser tratado em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de SIC. O órgão ou entidade da APF deve adotar medidas que assegurem a DICA.



MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL RURAL DA AMAZÔNIA

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO	
UNIDADE: (Informar a unidade classificadora. Ex: STIC)	
CÓDIGO DE INDEXAÇÃO: (de acordo com os arts. 51 e 52 do Decreto nº 7.845, de 14 de novembro de 2012) ¹	
GRAU DE SIGILO: (indicar o grau de classificação de sigilo da informação – reservado ou secreto)	
CATEGORIA: (identificar o código numérico da categoria na qual se enquadra a informação que está sendo classificada) ²	
TIPO DE DOCUMENTO: (descrever o documento, identificando-o. Exemplos: <ul style="list-style-type: none"> • Memorando nº 1/STIC/UFRA, de 5 de janeiro de 2020; • Processo nº 23084.001280/2020-01.) 	
DATA DE PRODUÇÃO: (identificar a data em que o documento/processo foi produzido)	
FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO: (indicar um dos incisos de I a IV do art. 6º da Norma complementar nº 01/2021)	
RAZÕES PARA A CLASSIFICAÇÃO: (demonstrar como a informação se enquadra à hipótese legal, ou seja, a motivação do ato administrativo de acordo com o entendimento expresso no art. 5º da Norma nº complementar 01/2021)	
PRAZO DA RESTRIÇÃO DE ACESSO: (indicar o prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu término, conforme limites previstos no parágrafo único do art. 6º da Norma complementar 01/2021)	
DATA DE CLASSIFICAÇÃO: (identificar a data em que o documento/processo foi classificado com grau de sigilo)	
AUTORIDADE CLASSIFICADORA (identificar (nome e cargo) a autoridade competente para classificar, de acordo com o grau de sigilo, conforme estabelecido no art. 30 do Decreto nº 7.724, de 2012)	Nome:
	Cargo:
AUTORIDADE RATIFICADORA (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 – quando aplicável)	Nome:
	Cargo:
DESCLASSIFICAÇÃO em ____/____/____ (informar a data, bem como nome e cargo da autoridade competente, mediante decisão de desclassificação da informação – quando aplicável)	Nome:
	Cargo:

<p>RECLASSIFICAÇÃO em ____/____/____ (informar a data, bem como nome e cargo da autoridade competente, mediante decisão de reclassificação da informação – quando aplicável)</p>	<p>Nome: Cargo:</p>
<p>REDUÇÃO DE PRAZO em ____/____/____ (informar a data, bem como nome e cargo da autoridade competente, mediante decisão de redução de prazo de classificação da informação – quando aplicável)</p>	<p>Nome: Cargo:</p>
<p>PRORROGAÇÃO DE PRAZO em_____/_____ (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 – quando aplicável)</p>	<p>Nome: Cargo:</p>
<p>_____ ASSINATURA DA AUTORIDADE CLASSIFICADORA</p>	
<p>_____ ASSINATURA DA AUTORIDADE RATIFICADORA (quando aplicável)</p>	
<p>_____ ASSINATURA DA AUTORIDADE responsável por DESCLASSIFICAÇÃO (quando aplicável)</p>	
<p>_____ ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO (quando aplicável)</p>	
<p>_____ ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO (quando aplicável)</p>	
<p>_____ ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO (quando aplicável)</p>	

mento¹ “(...)

Art. 51. A primeira parte do CIDIC será composta pelo Número Único de Protocolo -NUP, originalmente cadastrado conforme legislação de gestão documental.

§ 1º A informação classificada em qualquer grau de sigilo ou o documento que a contenha, quando de sua desclassificação, manterá apenas o NUP.

§ 2º 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 em qualquer grau de sigilo, sob pena de pôr em risco sua proteção e confidencialidade.

Art. 52. A segunda parte do CIDIC será composta dos seguintes elementos:

I - grau de sigilo: indicação do grau de sigilo, ultrassecreto (U), secreto (S) ou reservado (R), com as iniciais na cor vermelha, quando possível;

II - categorias: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme Anexo II do Decreto nº 7.845, de 14 de novembro de 2012; * Ver quadro nota (2);

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

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

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

a) reclassificação da informação resultante de reavaliação; ou

b) primeiro registro da classificação; e

VI - indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ultrassecreto, de acordo com a seguinte composição:

dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível. (...)”

² Categorias – de acordo com o Anexo II do Decreto nº 7.845, de 14 de novembro de 2012:

Categoria	Código Numérico	Categoria	Código Numérico
Agricultura, Extrativismo e Pesca	01	Indústria	10
Ciência, Informação e Comunicação	02	Justiça e Legislação	11
Comércio, Serviços e Turismo	03	Meio Ambiente	12
Cultura, Lazer e Esporte	04	Pessoa, Família e Sociedade	13
Defesa e Segurança	05	Relações Internacionais	14
Economia e Finanças	06	Saúde	15
Educação	07	Trabalho	16
Governo e Política	08	Transportes e Trânsito	17
Habitação, Saneamento e Urbanismo	09		