DIÁRIO OFICIAL DA UNIÃO

Publicado em: 16/12/2022 | Edição: 236 | Seção: 1 | Página: 94

Órgão: Ministério da Educação/Gabinete do Ministro

PORTARIA Nº 1.008, DE 13 DE DEZEMBRO DE 2022

Dispõe sobre procedimentos relacionados ao tratamento, à segurança e à classificação da informação no âmbito do Ministério da Educação - MEC.

O MINISTRO DE ESTADO DA EDUCAÇÃO, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II, da Constituição, tendo em vista o disposto na Lei nº 12.527, de 18 de novembro de 2011, na Lei nº 13.460, de 26 de junho de 2017, na Lei nº 13.709, de 14 de agosto de 2018, no Decreto nº 7.724, de 16 de maio de 2012, no Decreto nº 7.845, de 14 de novembro de 2012, resolve:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Os procedimentos relacionados ao tratamento, à segurança e à classificação da informação, no âmbito do Ministério da Educação - MEC, observarão as disposições desta Portaria.

CAPÍTULO II

DOS CONCEITOS E DAS DEFINIÇÕES

Art. 2º Para os efeitos desta Portaria, considera-se:

I - Algoritmo de Estado: função matemática utilizada na cifração e na decifração, desenvolvida pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal;

II - Alta Administração do MEC: Ministro de Estado, Secretário-Executivo, Secretário-Executivo Adjunto e Secretários titulares dos Órgãos específicos singulares do MEC;

III - Autoridade Classificadora: aquela que tem competência para classificar os documentos nos graus de sigilo reservado, secreto e ultrassecreto;

IV - Conhecimento Sensível: todo conhecimento, sigiloso ou estratégico, cujo acesso não autorizado pode comprometer a consecução dos objetivos nacionais e resultar em prejuízos ao País, necessitando de medidas especiais de proteção;

V - Documento Preparatório: documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas;

VI - Gestor de Segurança da Informação: responsável pelas ações de Segurança da Informação no âmbito do MEC;

VII - Gestor de Segurança e Credenciamento - GSC: responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle;

VIII - Informação Classificada: informação sigilosa em poder do MEC, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada, conforme procedimentos específicos de classificação estabelecidos na legislação vigente;

IX - Informação ou Dado Pessoal: informação ou dado relacionados à pessoa natural identificada ou identificável, relativa à intimidade, à vida privada, à honra e à imagem;

X - Informação ou Dado Pessoal Sensível: informação ou 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;

XI - Informação Sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo;

XII - Informação ou Dado Pessoal Anonimizado: informação ou dado relativos à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

XIII - Necessidade de Conhecer: é a condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para que uma pessoa tenha acesso à informação classificada, em qualquer grau de sigilo;

XIV - Núcleo de Segurança e Credenciamento: órgão de registro central, instituído no Gabinete de Segurança Institucional da Presidência da República - GSI/PR, nos termos do art. 37 da Lei nº 12.527, de 18 de novembro de 2011;

XV - Órgão de registro nível 1 - ORN1: ministério ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento;

XVI - Órgão de registro nível 2 - ORN2: órgão ou entidade pública vinculada a órgão de registro nível 1 e por este habilitado;

XVII - Posto de Controle: unidade do MEC, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo;

XVIII - Quebra de Segurança: ação ou omissão que implica comprometimento ou risco de comprometimento de informação classificada em qualquer grau de sigilo;

XIX - Sanitização: eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não sejam reconstruídos ou recuperados;

XX - Subcomitê de Segurança da Informação e Proteção de Dados do MEC - SSIP/MEC: colegiado subordinado ao Comitê de Governança Digital - CGD-MEC responsável por tratar de assuntos relacionados à segurança da informação, a privacidade e a proteção de dados pessoais no âmbito do MEC, conforme competências estabelecidas na Portaria MEC nº 10.012, de 25 de novembro de 2021, considerado como estrutura equivalente àquela prevista no art. 20 da Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020;

XXI - Tratamento da Informação: 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 da informação; e

XXII - Tratamento de Dados Pessoais: toda operação realizada com dados pessoais, como as que se referem à coleta, à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, à transmissão, à distribuição, ao processamento, ao arquivamento, ao armazenamento, à eliminação, à avaliação ou ao controle da informação, à modificação, à comunicação, à transferência, à difusão ou à extração.

CAPÍTULO III

DO ACESSO À INFORMAÇÃO

Art. 3º O acesso à informação pública será assegurado em conformidade com a Lei nº 12.527, de 2011, com o Decreto nº 7.724, de 16 de maio de 2012, e com o Decreto nº 7.845, de 14 de novembro de 2012.

Parágrafo único. As normas e os procedimentos relacionados ao Serviço de Informações ao Cidadão do MEC estão dispostas nos termos da Portaria nº 992, de 6 de dezembro de 2021.

Art. 4º A Política Corporativa de Segurança da Informação e Proteção de Dados do MEC - PSI/MEC, instituída pela Portaria nº 495, de 18 de julho de 2022, é constituída pelo conjunto de objetivos, princípios, diretrizes, políticas, normas, práticas, estruturas organizacionais e competências para orientar o uso e o compartilhamento de ativos de informação durante todo o seu ciclo de vida, sob a ótica da segurança física e virtual, da defesa cibernética e da proteção da informação, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade, bem como a proteção de dados pessoais e a privacidade de indivíduos.

Seção I

Do Comitê de Governança Digital

Art. 5º O Comitê de Governança Digital, instituído pela Portaria nº 565, de 28 de julho de 2021, é um órgão colegiado de natureza deliberativa e de caráter permanente, de cunho estratégico e executivo, para deliberar sobre assuntos relativos à Governança Digital e às ações, aos programas, às políticas e aos projetos de Tecnologia da Informação e Comunicação - TIC no âmbito do MEC.

Parágrafo único. O Subcomitê de Segurança da Informação e Proteção de Dados do MEC - SSIP-MEC, vinculado ao Comitê de Governança Digital - CGD/MEC, foi criado por meio da Portaria nº 1.012, de 25 de novembro de 2021, para tratar de assuntos relacionados à segurança da informação, à privacidade e à proteção de dados pessoais no âmbito do MEC.

Art. 6º Para estruturar a gestão da segurança da informação no MEC, serão designados e/ou instituídos:

I - um Gestor de Segurança da Informação (Portaria nº 1.110, de 24 de dezembro de 2021);

II - um Subcomitê de Segurança da Informação e Privacidade de Dados - SSIP/MEC (Portaria nº 1.012, de 2021); e

III - uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, conforme norma específica do MEC.

§ 1º Compete ao Subcomitê de Segurança da Informação e Proteção de Dados do MEC a edição de ato para dispor sobre a composição da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR cuja atuação será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos de Governo, sem prejuízo das demais metodologias e dos padrões conhecidos.

§ 2º O MEC deverá se fazer representar, por meio de sua ETIR, junto à Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC e ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov, atuando nas relações necessárias para o aprimoramento contínuo da Segurança e Privacidade.

Seção II

Do Gestor de Segurança da Informação

Art. 7º O Gestor de Segurança da Informação será designado dentre os servidores públicos ocupantes de cargo efetivo, com formação ou capacitação técnica compatível às suas atribuições.

Art. 8º As competências do Gestor de Segurança da Informação do MEC são apresentadas na Portaria nº 1.110, de 2021.

CAPÍTULO IV

DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 9º Serão consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação, 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 - 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 estratégicos 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 - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou

VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

§ 1º Estarão igualmente sujeitos à restrição de acesso:

I - as informações pessoais;

II - as informações sigilosas protegidas por legislação específica; e

III - os documentos preparatórios enquadrados no art. 3º, inciso XII, do Decreto nº 7.724, de 2012.

§ 2º O acesso ao teor de documento preparatório será assegurado a partir da edição do ato ou de decisão, em conformidade com o disposto no art. 20 do Decreto nº 7.724, de 2012.

Art. 10. No âmbito do MEC, a classificação da informação será realizada pelas seguintes autoridades classificadoras, conforme os graus determinados a seguir:

I - ultrassecreto e secreto: Ministro de Estado da Educação; e

II - reservado: Ministro de Estado da Educação e ocupantes de cargos de chefia do Grupo Direção e Assessoramento Superiores - DAS, nível 5 ou superior, ou seus equivalentes.

Art. 11. A decisão de classificar a informação deverá ser formalizada mediante a elaboração do Termo de Classificação de Informação - TCI (Anexo A), previsto no art. 31 do Decreto nº 7.724, de 2012.

§ 1º Tão logo ocorra a classificação da informação, o respectivo TCI deverá ser anexado, de forma analógica ou digital, com a informação original e ambos deverão ser encaminhados ao Gestor de Segurança e Credenciamento, para controle e arquivamento.

§ 2º No caso de informação classificada nos graus de sigilo ultrassecreto ou secreto, deverá ser enviada, no prazo de 30 (trinta) dias, contados a partir da respectiva classificação, cópia do TCI à Comissão Mista de Reavaliação de Informações, instituída no âmbito da Administração Pública federal, nos termos do art. 35, § 1º, da Lei nº 12.527, de 2011.

Art. 12. As autoridades referidas no art. 10, desta Portaria, serão consideradas credenciadas ex officio no exercício de seu cargo, dentro de suas competências e nos seus respectivos graus de sigilo, respeitada a necessidade de conhecer.

§ 1º As autoridades referidas no art. 10, inciso II, que tenham necessidade de conhecer informação classificada em grau de sigilo superior àquele para o qual já são credenciadas ex officio, deverão possuir credencial de segurança no respectivo grau de sigilo.

§ 2º Considera-se que aquele que tenha a competência para classificar em determinado grau de sigilo seja habilitado, de ofício, ao acesso às informações classificadas naquele grau de sigilo ou inferiores, observada a necessidade de conhecer preconizada no art. 37 desta Portaria.

CAPÍTULO V

DO TRATAMENTO DA INFORMAÇÃO CLASSIFICADA

Seção I

Das etapas do ciclo de vida da informação classificada

Art. 13. O sigilo da informação classificada deverá ser resguardado durante todas as etapas de seu ciclo de vida, quais sejam:

I - produção e recepção: refere-se à fase inicial do ciclo de vida, e compreende a produção, recepção ou custódia, e à classificação da informação;

II - organização: refere-se ao armazenamento, arquivamento e controle da informação;

III - uso e disseminação: refere-se à utilização, ao acesso, à reprodução, ao transporte, à transmissão e à distribuição da informação; e

IV - destinação: refere-se à fase final do ciclo de vida da informação, e compreende a avaliação, destinação ou eliminação da informação.

Seção II

Da produção e da recepção

Art. 14. Por ocasião da produção de documentos, os servidores deverão realizar prévia e criteriosa análise acerca do teor da matéria tratada, no sentido de, pontualmente, avaliar a sua sensibilidade, conferindo-lhe tratamento particularizado, à luz do contido no art. 9 da presente Portaria.

Parágrafo único. Considerando suas atribuições, e os assuntos a elas relacionados, os setores deverão mapear e definir os processos que usualmente ensejam informações sensíveis, disseminando, no âmbito do setor, uma rotina para seu tratamento.

Art. 15. Somente servidores que exerçam funções de direção ou chefia do Grupo Direção e Assessoramento - DAS, nível 5 ou superior, ou seus equivalentes, serão competentes para proceder a classificação do sigilo da informação.

Parágrafo único. É de responsabilidade do servidor que produziu informação passível de classificação dar ciência à sua chefia imediata, e esta, se necessário, a outras autoridades de forma subsequente, até que a informação chegue a um dos servidores com competência para sua classificação, previstos no caput.

Art. 16. Documentos produzidos no âmbito do MEC contendo informações passíveis de classificação, de acordo com o caput do art. 9 desta Portaria, deverão exibir, na parte central do cabeçalho e do rodapé, inclusive nas suas capas, marcação própria que indique o grau de sigilo atribuído: R E S E R V A D O, S E C R E T O ou U L T R A S E C R E T O, de forma a possibilitar a sua rápida visualização.

§ 1º Para a padronização das marcações referidas no caput deste artigo, deverá ser utilizada a fonte calibri em letras maiúsculas, tamanho 12, cor vermelha, com um espaço entre cada letra.

§ 2º Documentos cuja restrição de acesso decorra das situações dispostas no § 1º do artigo referenciado no caput deverão ser produzidos com a identificação de SIGILOSO, utilizando-se o modelo previsto no Anexo B desta Portaria.

Art. 17. As páginas de documentos sensíveis produzidos (classificados ou não) deverão ser numeradas de forma sequencial, com numeração exibida nos respectivos rodapés, observando-se formatação padronizada "XX/YY", em que XX é o número da página, e YY é o quantitativo total de páginas do documento.

Art. 18. O material utilizado como insumo para a elaboração de documento sensível ou classificado, como por exemplo minutas, rascunhos e anotações, deverá receber tratamento específico por ocasião da sua eliminação, sendo fragmentado ou adequadamente guardado para posterior descarte de forma apropriada, a fim de evitar a recuperação irregular e indevida de seu conteúdo.

Art. 19. O recebimento de processos ou documentos externos que contenham informações classificadas deverá ser protocolizado no Protocolo Central ou no Protocolo do Gabinete do Ministro de Estado da Educação, conforme o caso, à luz do destinatário e da sensibilidade do assunto.

Parágrafo único. Nos casos dos documentos classificados como secreto e ultrassecreto, deverão ser protocolizados pelo Protocolo do Gabinete do Ministro de Estado da Educação.

Art. 20. Quando do recebimento de processos ou documentos neste Ministério, deverá ser mantido o sigilo da informação já classificada por outro órgão ou entidade.

Art. 21. Ao receber processo ou documento classificado de origem externa, caberá à unidade de protocolo:

I - informar ao remetente, imediatamente, o recebimento da informação; e

II - efetuar a verificação da integridade do meio de recebimento e registrar indícios de violação ou de irregularidade, cientificando, com brevidade, o destinatário no MEC.

§ 1º Na hipótese dos casos previstos no inciso II do caput deste artigo, caberá ao destinatário do documento informar, imediatamente, o fato ao remetente.

§ 2º Quando não houver indicação expressa do destinatário, o encaminhamento deverá ocorrer à Chefia de Gabinete do Ministro.

§ 3º O envelope interno somente será aberto pelo destinatário, representante autorizado pelo Gestor de Segurança e Credenciamento, excetuando-se aqueles identificados com a marca PESSOAL, os quais somente poderão ser abertos pelo próprio destinatário.

Art. 22. A autoridade destinatária deverá atestar o recebimento do documento classificado.

§ 1º Após tomar conhecimento do conteúdo do processo ou do documento classificado, o destinatário elaborará o Formulário de Registro de Documento Classificado - FRDC (Anexo C) e o encaminhará ao Protocolo Central, para a sua inclusão no Sistema de Processo Eletrônico - SEI do MEC.

§ 2º Após elaboração do FRDC referenciado no parágrafo anterior, a autoridade recebedora do documento encaminhará cópia do Termo de Classificação de Informação - TCI recebido ao Gestor de Segurança e Credenciamento, para controle e arquivo.

§ 3º No sentido de viabilizar a identificação da localização física do documento/processo classificado a qualquer momento, o FRDC deverá ser tramitado eletronicamente, e de forma concomitante, aos mesmos destinatários do documento/processo físico.

Art. 23. Nas hipóteses em que o servidor receba documento não classificado quanto ao sigilo na sua origem, mas que ao tomar conhecimento do seu teor identifique a presença de dados ou informações que, na sua avaliação, justificariam a classificação do documento, deverá ser observado o procedimento previsto no parágrafo único do art. 15 desta Portaria para tal fim, cabendo ao servidor com competência a elaboração do correspondente TCI (Anexo A).

§ 1º Se o documento recebido já estiver inserido no Sistema de Processo Eletrônico, o processo eletrônico, com os respectivos TCI e FRDC, deverá retornar à unidade de protocolo central para a adoção dos procedimentos necessários à segurança da informação, seguido do envio de cópia do TCI ao Gestor de Segurança e Credenciamento.

§ 2º No caso de eventual identificação de registro e armazenamento indevido de arquivo classificado no Sistema de Processo Eletrônico, a pessoa credenciada deverá comunicar ao Gestor de Segurança e Credenciamento e este deverá solicitar à STIC a exclusão definitiva de todo e qualquer registro da base de dados.

§ 3º Procedimento idêntico ao previsto no caput deste artigo deverá ser observado se o servidor responsável pela instrução de um processo eletrônico identificar a necessidade de inserir ou elaborar um novo documento que contenha informação classificada.

Seção III

Da organização

Art. 24. É obrigatório o cadastro de todo processo ou documento que contenha informação classificada no Sistema de Processo Eletrônico do MEC, utilizando-se o Formulário de Registro de Documento Classificado - FRDC (Anexo C), com observância, no que for aplicável, às normas e aos procedimentos de protocolização e organização processual, sendo vedada a inserção no Sistema de Processo Eletrônico do conteúdo do documento contendo a informação classificada.

Parágrafo único. Na hipótese de o processo ou o documento não ter sido recebido originalmente pelo Protocolo Central ou Protocolo do Gabinete do Ministro de Estado da Educação, o servidor que o recebeu deverá encaminhá-lo a uma dessas duas unidades para a elaboração do Formulário de Registro de Documento Classificado - FRDC e, consequentemente, ser efetuado seu cadastramento no Sistema.

Art. 25. A informação classificada deverá ser mantida e arquivada em condições especiais de segurança em Postos de Controle - PC, separada de acordo com o grau de sigilo atribuído.

§ 1º Cada PC deverá definir local adequado para a guarda dessas informações, devendo ser observada a utilização de cofre ou armário com chave, em compartimento com acesso restrito às pessoas credenciadas.

§ 2º Para a manutenção e o arquivamento de informação classificada no grau de sigilo ultrassecreto e secreto, é obrigatório o uso de equipamento, ambiente ou estrutura que ofereça segurança compatível com o grau de sigilo.

§ 3º Documentos em suporte físico ou digital (mídia removível) armazenados podem possuir cópia de segurança armazenada no PC, sendo obrigatório o uso de equipamento, ambiente ou estrutura que ofereça segurança compatível com o grau de sigilo.

Art. 26. Os Titulares das unidades do MEC deverão designar, no âmbito dos respectivos setores, servidor responsável pelo armazenamento e controle dos documentos sensíveis em suporte físico, bem como os digitais em mídia removível (HD externo, pen drive).

Parágrafo único. Compete aos servidores designados no caput providenciar a entrega das cópias de segurança exigidas no § 3º do artigo anterior.

Art. 27. Nos Postos de Controle, os documentos em meio físico recebidos para guarda deverão ser segregados e armazenados conforme a sua classificação de sigilo e a sua sensibilidade, observando-se as medidas adequadas para fins de organização, preservação e acesso.

Art. 28. Para o armazenamento em meio eletrônico de documento com informação classificada em qualquer grau de sigilo, é obrigatória a utilização de sistemas de tecnologia da informação atualizados, de forma a prevenir ameaças de quebra de segurança, observado o disposto no art. 38 do Decreto nº 7.845, de 2012.

§ 1º As mídias para armazenamento poderão estar integradas a equipamentos conectados à internet, desde que por canal seguro e com níveis de controle de acesso adequados ao tratamento da informação classificada, admitindo-se também a conexão a redes de computadores internas, desde que seguras e controladas.

§ 2º Os meios eletrônicos de armazenamento de informação classificada em qualquer grau de sigilo, inclusive os dispositivos móveis, devem utilizar recursos criptográficos adequados ao grau de sigilo, conforme normativos em vigor.

Seção IV

Do uso e da disseminação

Art. 29. A utilização, o acesso, a reprodução, o transporte, a transmissão e a distribuição da informação devem seguir os princípios da disponibilidade, integridade, confidencialidade e autenticidade, conforme normativos de segurança da informação e a legislação vigente, bem como as orientações específicas que garantam a salvaguarda de informação sigilosa e pessoal.

Art. 30. Durante seu trâmite, a guarda e o armazenamento de documentos que contenham informações classificadas são de responsabilidade daquele que detém a sua posse.

Art. 31. O acesso, a divulgação e o tratamento de informações classificadas são restritos a pessoas com necessidade de conhecê-las e que estejam credenciadas, em conformidade com o art. 18 do Decreto nº 7.845, de 2012.

Parágrafo único. Os servidores que tiverem acesso a qualquer informação sigilosa ficam proibidos de divulgar o seu conteúdo, durante o período correspondente à classificação da informação, ainda que venham a ser dispensados ou exonerados.

Art. 32. O acesso à informação classificada por pessoa não credenciada, ou não autorizada ex officio, poderá ser permitido excepcionalmente, mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS (Anexo D).

Art. 33. 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.

§ 1º 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.

§ 2º Os sistemas de informação de que trata o caput deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos graus de sigilo, bem como 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.

Art. 34. Os equipamentos e sistemas utilizados para o acesso a 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.

Parágrafo único. A cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado, conforme legislação em vigor.

Art. 35. A reprodução do todo ou de parte de documento com informação classificada em qualquer grau de sigilo terá o mesmo grau de sigilo do documento.

Parágrafo único. A reprodução referenciada no caput condiciona-se à autorização expressa da autoridade competente ou autoridade hierarquicamente superior com igual prerrogativa, devendo as cópias serem autenticadas por essas autoridades.

Art. 36. A impressão de documentos com conteúdo sensível ou sigiloso, quando realizada em equipamentos de uso comum, só deverá ser liberada com a presença do usuário que os enviou, mediante a apresentação do crachá ou senha.

Art. 37. A expedição e a tramitação de documentos em meio físico classificados deverão observar os seguintes procedimentos:

I - serão acondicionados em envelopes duplos;

II - não constará indicação do grau de sigilo ou do teor do documento no envelope externo;

III - constarão o destinatário e o grau de sigilo do documento no envelope interno, de modo a serem identificados logo que removido o envelope externo;

IV - o envelope interno será fechado, lacrado e expedido mediante recibo, que indicará remetente, destinatário e número ou outro indicativo que identifique o documento; e

V - será inscrita a palavra PESSOAL no envelope que contiver documento de interesse exclusivo do destinatário.

Art. 38. A expedição de documento com informação classificada em grau de sigilo secreto ou reservado será feita pelos meios de comunicação disponíveis, com recursos de criptografia compatíveis com o grau de sigilo, ou, se for o caso, por via diplomática, sem prejuízo da entrega pessoal.

Art. 39. A expedição, a condução e a entrega de documento com informação classificada em grau de sigilo ultrassecreto serão efetuadas pessoalmente, por agente público autorizado, ou transmitidas por meio eletrônico, desde que sejam usados recursos de criptografia compatíveis com o grau de classificação da informação, vedada sua postagem.

Art. 40. No transporte, na transmissão e na distribuição de mídias que contenham informação sigilosa deverá ser aplicado controle de acesso e uso de criptografia baseada em algoritmo de Estado.

Art. 41. No transporte, na transmissão e na distribuição de documentos em suporte físico que forem realizados por empresa terceirizada, caberá à Subsecretaria de Assuntos Administrativos - SAA efetuar o processo licitatório e assinar o Contrato, cabendo ao Gestor de Segurança e Credenciamento estabelecer, por ocasião da elaboração do Termo de Referência, as regras que visem a seleção da empresa, zelando também pela observância das medidas e procedimentos de segurança da informação previstos nos normativos em vigor.

Seção V

Da destinação da informação

Art. 42. A avaliação e a seleção de documento com informação desclassificada, para fins de guarda permanente ou eliminação, observarão o disposto na Lei nº 8.159, de 8 de janeiro de 1991, e no Decreto nº 4.073, de 3 de janeiro de 2002.

Parágrafo único. Quando da desclassificação, o documento que contiver informação classificada em qualquer grau de sigilo será encaminhado ao Arquivo Central do Ministério. A destinação final de documentos contendo informações desclassificadas é de competência da Comissão Permanente de Avaliação de Documentos - CPAD, conforme proposição da Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS.

Seção VI

Da desclassificação e da reavaliação da informação sigilosa

Art. 43. A desclassificação ou a redução do prazo de sigilo da informação classificada poderá ser reavaliada pela autoridade competente ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, observando-se a legislação em vigor sobre o assunto.

Art. 44. A decisão da desclassificação, reclassificação ou redução do prazo de sigilo de informações classificadas deverá constar das capas dos processos, se houver, e de campo apropriado no TCI.

Art. 45. A desclassificação de informações, sua reclassificação, ou a redução do prazo de seu sigilo, deverá ser prontamente informada ao Gestor de Segurança e Credenciamento pela autoridade que a procedeu.

Art. 46. Periodicamente, de acordo com rotina estabelecida pela Comissão Permanente de Avaliação de Documentos Sigilosos, referenciada na Seção VII desta Portaria, deverá ser procedida a eliminação segura de documentos sensíveis em suporte físico e/ou digital, observando-se os procedimentos e os necessários registros previstos nos normativos sobre o tema.

Art. 47. Na eliminação de informação em meio eletrônico deverá ser realizada sanitização dos dados nas mídias de armazenamento, tais como dispositivos móveis, discos rígidos, memórias das impressoras, scanners, multifuncionais, entre outros dispositivos, antes do descarte, a fim de evitar a recuperação irregular e indevida de dados.

Seção VII

Da Comissão Permanente de Avaliação de Documentos Sigilosos

Art. 48. Constituir, no âmbito do MEC, uma Comissão Permanente de Avaliação de Documentos Sigilosos com as seguintes competências:

I - assessorar a classificação quanto ao grau de sigilo, a desclassificação, a reclassificação ou a reavaliação da informação;

II - propor o destino final da informação desclassificada; e

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

§ 1º Regulamento da SAA disporá sobre a composição, a organização e o funcionamento da Comissão Permanente de Avaliação de Documentos Sigilosos.

§ 2º Compete ao Gestor de Segurança e Credenciamento coordenar os trabalhos da Comissão Permanente de Avaliação de Documentos Sigilosos.

CAPÍTULO VI

DO TRATAMENTO DA INFORMAÇÃO PESSOAL

Art. 49. Independentemente de classificação de sigilo, as informações pessoais relativas à intimidade, à vida privada, à honra e à imagem terão seu acesso restrito, pelo prazo máximo de 100 (cem) anos, a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem (conforme exposto no inciso I do § 1º do art. 31 da Lei 12.527, de 18 de novembro de 2011).

§ 1º O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, à vida privada, à honra e à imagem das pessoas, bem como às liberdades e garantias individuais, e em estrita observância ao estabelecido na Lei Geral de Proteção de Dados - LGPD.

§ 2º As informações mencionadas no caput poderão ter autorizados a divulgação ou o acesso por terceiros, diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem, desobrigando-se esse consentimento nos casos específicos previstos na legislação em vigor sobre o assunto.

Art. 50. O acesso à informação pessoal por terceiros será condicionado à assinatura de um Termo de Responsabilidade (Anexo E), que disporá sobre a finalidade e a destinação que fundamentaram sua autorização, bem como sobre as obrigações a que se submeterá o requerente.

Parágrafo único. A utilização de informação pessoal por terceiros vincula-se à finalidade e à destinação que fundamentaram a autorização do acesso, vedada sua utilização de maneira diversa.

Art. 51. Para a identificação e a classificação de dados pessoais no âmbito do MEC, deverá ser observado, como orientação, o disposto no "Guia de Elaboração de Inventário de Dados Pessoais", disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf/view, elaborado com o intuito de auxiliar os órgãos e as entidades da Administração Pública Federal, direta, autárquica e fundacional a realizar o levantamento e o registro dos dados pessoais tratados no âmbito institucional.

Art. 52. Dados anonimizados não serão considerados dados pessoais para os fins desta Portaria, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.

Parágrafo único. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

Seção I

Do tratamento de dados pessoais sensíveis

Art. 53. O tratamento de dados pessoais sensíveis somente poderá ocorrer quando houver o consentimento do titular ou de seu responsável legal, de forma específica e destacada, e para finalidades específicas.

Parágrafo único. É permitido o tratamento dos dados citados no caput sem o fornecimento de consentimento do titular, desde que observadas as hipóteses previstas no art. 11, inciso II, da LGPD, e as vedações estabelecidas no mesmo artigo.

Seção II

Do tratamento de dados de crianças e adolescentes

Art. 54. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos da legislação em vigor, e mediante o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Parágrafo único. O consentimento citado no caput não será exigido quando a coleta de dados for necessária para sua proteção ou para contatar os pais ou o responsável legal, podendo os dados serem utilizados uma única vez e sem armazenamento, sendo vedado, entretanto, o seu repasse a terceiros sem o consentimento de que trata caput.

CAPÍTULO VII

DO CREDENCIAMENTO DE SEGURANÇA

Seção I

Do Gestor de Segurança e Credenciamento

Art. 55. O Gestor de Segurança e Credenciamento do MEC e seu substituto serão servidores lotados na Secretaria-Executiva e/ou no Gabinete do Ministro, conforme a conveniência do serviço e a devida indicação, ambos designados formalmente pelo Secretário-Executivo do MEC.

Art. 56. Caberá ao Gestor de Segurança e Credenciamento:

I - manter a qualificação técnica necessária à segurança de informação classificada, em qualquer grau de sigilo, no âmbito do MEC;

II - controlar os documentos classificados;

III - garantir a formalidade e o sigilo dos processos de credenciamento e de habilitação dentro da competência do MEC;

IV - propor normas à Alta Administração, no âmbito do MEC, para o tratamento da informação classificada e para o acesso às áreas, às instalações e aos materiais de acesso restritos;

V - gerir os recursos criptográficos, as Credenciais de Segurança e os materiais de acesso restrito, com o auxílio do Posto de Controle;

VI - assessorar a Alta Administração do MEC para o tratamento de informações classificadas, em qualquer grau de sigilo;

VII - promover a capacitação dos agentes públicos responsáveis pelo tratamento de informação classificada, em qualquer grau de sigilo;

VIII - controlar e manter arquivo atualizado dos TCI;

IX - definir as áreas de acesso restrito para efeito de segurança das informações classificadas, informando-as à SAA;

X - providenciar anualmente, junto à Assessoria de Comunicação Social - ACS/MEC, a disponibilização do rol das informações desclassificadas e dos documentos classificados em cada grau de sigilo na página do MEC na internet; e

XI - responder, no âmbito do MEC, pelas ações necessárias ao desempenho das atribuições de competência do Órgão de Registro Nível 1 - ORN1 previstas nos normativos em vigor.

Parágrafo único. O Gestor de Segurança e Credenciamento e o Gestor de Segurança da Informação adotarão as providências para que os agentes públicos do MEC conheçam as normas e observem os procedimentos de segurança e de tratamento de informação sigilosa classificada, de acordo com o grau de sigilo atribuído.

Seção II

Da concessão de credencial

Art. 57. O MEC, mediante prévia habilitação junto ao Gabinete de Segurança Institucional da Presidência da República, exercerá as atribuições institucionais de competência do Órgão de Registro Nível 1 - ORN1, conforme disposto no art. 7º do Decreto nº 7.845, de 2012.

Art. 58. A concessão de credencial de segurança pelo Gestor de Segurança e Credenciamento realizar-se-á em três fases: indicação, investigação de segurança e credenciamento.

Art. 59. A fase de indicação para o processo de credenciamento se inicia com a solicitação formal, ao Gestor de Segurança e Credenciamento, por autoridade que exerça função de direção, comando ou chefia do Grupo Direção e Assessoramento Superiores - DAS, nível 5 ou superior, ou seus equivalentes, à qual o servidor esteja subordinado, com a identificação da pessoa para a qual deseja a credencial.

Parágrafo único. Além do Formulário Individual de Dados para Credenciamento - FIDC (Anexo F), devidamente preenchido e assinado, a solicitação de indicação referenciada no caput deverá informar:

I - o grau de acesso à informação classificada pretendido;

II - as atividades/funções a serem desenvolvidas pelo indicado que demandem o acesso à informação classificada;

III - o prazo estimado de exercício;

IV - a justificativa da autoridade indicadora para a necessidade de conhecer documentos classificados por parte da pessoa a ser credenciada; e

V - outras informações julgadas pertinentes.

Art. 60. A fase de investigação de segurança tem como objetivo identificar o nível do risco potencial de quebra de segurança ao se permitir que a pessoa indicada acesse informação classificada no grau de sigilo indicado, e será realizada pela Secretaria Executiva e/ou Gabinete do Ministro, por solicitação formal do Gestor de Segurança e Credenciamento.

Parágrafo único. O MEC poderá firmar ajustes, convênios ou termos de cooperação com outros órgãos ou entidades públicas, habilitados, para:

I - credenciamento de segurança e tratamento de informação classificada; e

II - realização de inspeção e investigação para credenciamento de segurança.

Art. 61. O relatório de investigação será anexado ao processo de credenciamento de segurança, no qual constará parecer do responsável, identificando, em função do nível do risco potencial de quebra de segurança constatado, se o indicado está apto ou não para o credenciamento de segurança no grau solicitado.

§ 1º Os autos e as peças componentes da investigação serão elaborados por: servidor público ocupante de cargo efetivo, com competência profissional comprovada para atuar na área de inteligência; por policial ou por perito criminal.

§ 2º O relatório de investigação e os autos da investigação deverão ser tratados como documento pessoal, sendo arquivados no órgão encarregado da investigação e compondo o processo de credenciamento.

§ 3º A investigação deverá avaliar, no mínimo, dados dos seguintes aspectos pessoais do indicado:

I - envolvimento com pessoas ou organizações associadas ao crime, terrorismo, tráfico, sabotagem e espionagem;

II - situação fiscal;

III - dados relacionados à situação criminal, cível e administrativa; e

IV - situação eleitoral e do serviço militar.

Art. 62. A fase do credenciamento se caracteriza pela homologação da permissão para o tratamento da informação classificada no grau solicitado, não eximindo o credenciado das responsabilidades administrativas, cíveis e penais quanto à manutenção da segurança dos ativos de informação classificados, tratados conforme legislação pertinente.

Art. 63. A credencial de segurança terá prazo de validade máximo de 2 (dois) anos, observada eventual restrição temporal contida no art. 59, parágrafo único, inciso III, desta Portaria, e poderá ser renovada ao término de sua validade, sem limite de renovações, desde que observado o processo preconizado nesta Portaria para sua concessão, sendo vedada a prorrogação.

Seção III

Do descredenciamento de segurança

Art. 64. O descredenciamento dar-se-á de forma automática, independentemente de solicitação ou processo, nos seguintes casos:

I - término de validade de credencial de segurança;

II - transferência de órgão ou entidade;

III - cessação da necessidade de conhecer;

IV - aposentadoria;

V - falecimento; e

VI - exoneração de cargo comissionado ou função de confiança.

Parágrafo único. Excetuando-se o previsto no inciso I acima, em qualquer dos demais casos cabe à chefia imediata do servidor, via autoridade que solicitou o credenciamento de segurança (se não for a mesma), informar ao Gestor de Segurança e Credenciamento a ocorrência do fato, para que seja providenciado o respectivo descredenciamento.

Art. 65. O descredenciamento poderá ocorrer, a qualquer tempo, a critério da Alta Administração do MEC, ou ainda, em caso de suspeita ou quebra de segurança.

Seção IV

Do posto de controle

Art. 66. Os Postos de Controle do MEC atuarão sob a responsabilidade e subordinação ao Gestor de Segurança e Credenciamento, observando as disposições que normatizam o seu funcionamento.

Art. 67. Caberá ao Posto de Controle do MEC:

I - armazenar e controlar as informações classificadas, inclusive as credenciais de segurança, sob sua responsabilidade;

II - manter a segurança lógica e física das informações classificadas, sob sua guarda;

III - encaminhar, anualmente, ao Órgão de Registro que o credenciou relatórios de suas atividades; e

IV - notificar o Órgão de Registro que o credenciou, imediatamente, quando da quebra de segurança das informações classificadas por ele custodiadas.

Art. 68. Quando cessada a tramitação de documentos que contenham informação sigilosa classificada em grau de sigilo, estes serão encaminhados pela área responsável ao Posto de Controle do MEC para fins de guarda.

Parágrafo único. Até que sejam transferidos ao Posto de Controle, tais documentos deverão ser armazenados de modo que impossibilite o acesso por pessoas não credenciadas, conforme o disposto no art. 25 desta Portaria.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 69. Caberá à Subsecretaria de Tecnologia da Informação e Comunicação - STIC/MEC e à SAA/MEC auxiliar o Gestor de Segurança da Informação e o Gestor de Segurança e Credenciamento na proposição e implementação de soluções e no estabelecimento de requisitos de proteção física e lógica para o adequado tratamento das informações, inclusive as classificadas, no âmbito do MEC.

Art. 70. Os agentes públicos respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou da utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso, nos termos do art. 34, parágrafo único, da Lei nº 12.527, de 2011.

Parágrafo único. O disposto no caput aplica-se, no que couber, à pessoa física ou à entidade privada que, em virtude de vínculo de qualquer natureza com órgãos ou entidades, tenha acesso a informação sigilosa ou pessoal e a submeta a tratamento indevido.

Art. 71. Os usuários da informação são responsáveis pela segurança dos ativos da informação do MEC que estejam sob sua responsabilidade e por todos os atos praticados com sua identificação, tais como: login, crachá, carimbo, endereço de correio eletrônico ou assinatura digital e outros.

Art. 72. Toda quebra de segurança de informação classificada, em qualquer grau de sigilo, deverá ser informada, tempestivamente, pelo Gestor de Segurança e Credenciamento, à Alta Administração do Órgão, que informará ao Gabinete de Segurança Institucional da Presidência da República, relatando as circunstâncias com o maior detalhamento possível.

Art. 73. O Secretário-Executivo poderá expedir atos complementares necessários ao cumprimento desta Portaria.

Art. 74. Os casos omissos serão tratados pelo Secretário-Executivo, assessorado pelo Gestor de Segurança da Informação e pelo Gestor de Segurança e Credenciamento do MEC, conforme o caso, e, ainda, no que couber, pela Autoridade de Monitoramento a que se refere o art. 40 da Lei nº 12.527, de 2011.

Art. 75. Esta Portaria entra em vigor em 2 de janeiro de 2023.

VICTOR GODOY VEIGA

ANEXO A

MINISTÉRIO DA EDUCAÇÃO

GRAU DE SIGILO: _____ (idêntico ao grau de sigilo do documento)

TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO - TCI
ÓRGÃO/ENTIDADE:
CÓDIGO DE INDEXAÇÃO:
GRAU DE SIGILO:

CATEGORIA:		
TIPO DE DOCUMENTO:		
DATA DE PRODUÇÃO:		
FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO:		
RAZÕES PARA A CLASSIFICAÇÃO: (observando-se o 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)		

ANEXO B

(SIGILOSO)

MINISTÉRIO DA EDUCAÇÃO

Este modelo destina-se ao registro de informações que se enquadrem em alguma das situações abaixo:

A) Informações Pessoais, observado o disposto na Lei Geral de Proteção de Dados - LGPD;

B) Informações sigilosas protegidas por legislação específica; ou

C) Documento Preparatório: utilizado como fundamento de tomada de decisão ou de ato administrativo, conforme o disposto no art. 3º, inciso XII, do Decreto nº 7.724, de 16 de maio de 2012.

ANEXO C

MINISTÉRIO DA EDUCAÇÃO

	FORMULÁRIO DE REGISTRO DE DOCUMENTO CLASSIFICADO - FRDC
	. (1) Órgão/Entidade responsável pela classificação do documento:
	. (2) NUP:
	. (1) Código de Indexação do Documento Classificado (TCI):
	. (1) Grau de Sigilo:
	. (1) Data da Produção do Documento Classificado:

	. (1) Data de Classificação:		
	. (1) Fundamentação Legal:		
	. (1) Identificação do Documento:		
	. (1) Prazo da Restrição de Acesso:		
	. (1) Autoridade Classificadora		Nome:
. (3) Registro do Destinatário do Documento no Ministério da Educação:			
. (4) Responsável pela Elaboração do FRDC			Nome:
			Cargo:

(1) Informações extraídas do Termo de Classificação de Informação - TCI.

(2) Preencher com o NUP atribuído ao Processo no SEI.

(3) Unidade Destinatária Original do Documento no Ministério da Educação.

(4) Identificação do Responsável pela Elaboração da FRDC no Protocolo.

ANEXO D

MINISTÉRIO DA EDUCAÇÃO

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO - TCMS

Eu, _____, CPF nº _____, identidade nº, _____ solicito, em caráter excepcional, acesso ao documento/processo _____ (1) _____, em decorrência da _____(2) _____.

Declaro ter pleno conhecimento das obrigações a mim impostas em decorrência do teor e da classificação dos dados e das informações acima especificados, e comprometo-me a agir no sentido de resguardar o conteúdo disseminado pelo prazo estabelecido.

Declaro ter conhecimento dos dispositivos constantes na Lei de Acesso à Informação - LAI, mormente o contido no § 2º do seu artigo 25, o qual estabelece a obrigação de resguardar o sigilo àquele que obtiver acesso à informação classificada como sigilosa; e no parágrafo único do seu artigo 34, o qual submete a pessoa física ou entidade privada que tenha acesso a informação sigilosa a responder pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida da mesma.

Declaro ainda autorizar o tratamento dos dados pessoais fornecidos neste documento, para a finalidade de registro da concessão do acesso, conforme o previsto no inciso I do art. 7º da lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD).

_____, _____, em _____ de _____ de 20_____.

_____

(assinatura)

(1) Preencher com a identificação clara do documento/processo que deseja ter acesso.

(2) Apresentar a motivação que justifique o acesso ao documento/processo desejado.

ANEXO E

MINISTÉRIO DA EDUCAÇÃO

TERMO DE RESPONSABILIDADE PELO USO E PELA DIVULGAÇÃO DE INFORMAÇÕES PESSOAIS

Eu, _____, identidade nº _____, expedido pelo órgão _____, e CPF nº _____, residente na rua/avenida _____, CEP nº _____, cidade _____, UF _____, telefone nº (_____) _____ e correio eletrônico _____, declaro, nos termos da Lei nº 12.527, de 18 de novembro de 2011, e de sua regulamentação, que é de minha inteira responsabilidade o acesso à(s) cópia(s) do(s) documento(s) nº (s) _____, certifico que a utilização do(s) referido(s) documento(s) tem como finalidade e destinação: _____.

Responsabilizo-me integralmente pela adequada utilização das informações a que tiver acesso.

Autorizo o tratamento dos dados pessoais fornecidos neste termo, para a finalidade de registro da concessão de acesso aos aludidos documentos, conforme o previsto no inciso I do art. 7º da Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD).

Estou ciente de que posso vir a ser responsabilizado civil, criminal e administrativamente pelos danos morais ou materiais decorrentes da utilização, reprodução ou divulgação indevida, conforme as legislações:

I - Lei nº 12.527, de 2011, art. 31, § 2º (uso indevido de informação);

II - Decreto nº 7.724, de 16 de maio de 2012, art. 56 (transparência e respeito às informações pessoais);

III - Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), art. 20 (divulgação autorizada ou necessária); e

IV - Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), arts. 138 a 145 (crimes contra a honra), 297, 299 e 304 (crimes de falsidade documental).

_____, _____, em _____ de _____ de 20 _____.

_____

(assinatura)

ANEXO F

(SIGILOSO)

MINISTÉRIO DA EDUCAÇÃO

FORMULÁRIO INDIVIDUAL DE DADOS PARA CREDENCIAMENTO - FIDC

ÓRGÃO DE REGISTRO NÍVEL 1

INSTRUÇÕES PARA O PREENCHIMENTO: responda de forma precisa às questões apresentadas; digite os dados diretamente no Formulário ou utilize letras de forma para preenchê-lo, com caneta azul ou preta; se não houver resposta a dar a alguma(s) questão(ões), escreva a expressão NADA A RELATAR; e os dados informados são considerados pessoais.	Foto 3x4 Rosto Frontal e Fundo Branco

1. DADOS PESSOAIS:

. Nome completo:
. Data de nascimento: / /
. Local de nascimento: UF: País:
. Nacionalidades:
. Estado civil:
. Documento de identificação: Tipo:
. Data de expedição: Local de expedição:
. Identidade Funcional: Órgão:
. Cadastro de Pessoas Físicas: Cadastro INSS:
. Título de Eleitor: Zona: Seção:
. Carteira Nacional de Habilitação: Emissão: UF:
. Passaporte nº: País Emissor:

2. RESIDÊNCIA HABITUAL:

. Endereço:
. CEP nº: Cidade: UF: País:
. Telefones residenciais:
. Telefones celulares:
. Telefones Funcionais:

. E-mails:

3. DADOS PROFISSIONAIS:

. Cargo/Função/Emprego:
. Órgão/Empresa:
. Endereço:
. CEP nº: Cidade: UF: País:
. Data de admissão: / /

4. DADOS DO PAI:

. Nome completo:	
. Data de nascimento: / /	Local de nascimento:
. UF: País:	Nacionalidades:
. Endereço:	
. CEP nº: Cidade:	UF : País:
. Convive atualmente: Sim [ ] Não [ ]	

5. DADOS DA MÃE:

. Nome completo:	
. Data de nascimento: / /	Local de nascimento:
. UF: País:	Nacionalidades:
. Endereço:	
. CEP nº: Cidade:	UF: País:
. Convive atualmente: Sim [ ] Não [ ]	

6. DADOS DO CÔNJUGE OU COMPANHEIRO(A):

.Nome completo:		
.Data de nascimento: / /	Local de nascimento:	
.UF: País:	Nacionalidades:	
.Endereço:		
.CEP nº: Cidade:	UF:	País:
.Convive atualmente: Sim [ ] Não [ ]		

7. RESIDÊNCIAS ANTERIORES (Endereços residenciais do solicitante nos últimos dez anos):

Desde (mês/ano)	Até (mês/ano)	Endereço: ____ CEP: _____________ Cidade: _______________ UF: __________ País: __________________
Desde (mês/ano)	Até (mês/ano)	Endereço: ____ CEP: _____________ Cidade: _______________ UF: __________ País: __________________
Desde (mês/ano)	Até (mês/ano)	Endereço: ____ CEP: _____________ Cidade: _______________ UF: __________ País: __________________
Desde (mês/ano)	Até (mês/ano)	Endereço: ____ CEP: _____________ Cidade: _______________ UF: __________ País: __________________
Desde (mês/ano)	Até (mês/ano)	Endereço: ____ CEP: _____________ Cidade: _______________ UF: __________ País: __________________

8. VIAGENS: Se visitou algum País estrangeiro nos últimos 10 anos, preencha o quadro abaixo:

Data		País	Motivo
Início	Fim		

9. Pessoas de seu convívio que tenham residido no exterior por mais de 2 anos, nos últimos dez anos:

Nome	De/Até (mês/ano)	País	Motivo

10. Possui alguma enfermidade? Sim [ ] Não [ ]

10.1 Caso positivo, qual?

----

11. Faz uso de algum medicamento controlado? sim [ ] não [ ]

11.1 Caso positivo, relacione:

----

12. FORMAÇÃO PROFISSIONAL (Relacionar os cursos realizados após o ensino médio):

Data de Conclusão	Instituição e País	Título

13. DADOS SOBRE EMPREGOS ANTERIORES (Relacionar os empregos anteriores ao que está sendo exercido atualmente):

Período	Empresa ou Entidade	Endereço	Cargo/Emprego

14. RELAÇÕES INTERNACIONAIS (Relatar se manteve relações com governos estrangeiros, organismos ou programas internacionais, esclarecendo as funções desempenhadas ou tipo de relação mantida):

Organismo/Programa	Tipo de Relação e Período	País

15. REFERÊNCIAS PESSOAIS:

Nome	Telefone

16. OBSERVAÇÕES FINAIS (Relate qualquer fato que julgue necessário e oportuno para o processo de credenciamento):

----

17. DECLARAÇÃO PESSOAL:

EU _____, DEVIDAMENTE QUALIFICADO NO ITEM 1 (UM) DESTE FORMULÁRIO, DECLARO PARA OS FINS DESTE CREDENCIAMENTO DE SEGURANÇA, QUE:

A) TUDO QUE FOI MANIFESTADO POR MIM, NESTE QUESTIONÁRIO, É PURA EXPRESSÃO DA VERDADE;

B) RECONHEÇO QUE QUALQUER FALSIDADE DECLARADA (POR OMISSÃO, ENGANO, INEXATIDÃO OU TERGIVERSAÇÃO DE ALGUM DADO) SERÁ MOTIVO PARA NEGAÇÃO OU ANULAÇÃO DA CREDENCIAL DE SEGURANÇA, SEM PREJUÍZO DE OUTRAS RESPONSABILIDADES;

C) COMPROMETO-ME A COMUNICAR IMEDIATAMENTE AO ÓRGÃO CREDENCIADOR, DURANTE A INVESTIGAÇÃO OU DURANTE O PERÍODO DE VALIDADE DA CREDENCIAL DE SEGURANÇA, QUALQUER ALTERAÇÃO POSTERIOR DOS DADOS ASSINALADOS NESTE QUESTIONÁRIO;

D) DECLARO CONHECER A LEGISLAÇÃO EM VIGOR E AS NORMAS RELACIONADAS À SEGURANÇA DA INFORMAÇÃO E DE COMUNICAÇÕES, ESPECIALMENTE, AQUELAS RELATIVAS ÀS INFORMAÇÕES CLASSIFICADAS;

E) A PARTIR DOS DADOS DESTE FORMULÁRIO, ATENDENDO AO PRESCRITO NO INCISO II DO ART. 55 DO DECRETO Nº 7.724, DE 16 DE MAIO DE 2012, AUTORIZO A INVESTIGAÇÃO PARA CREDENCIAMENTO SOBRE MINHA PESSOA, A FIM DE VERIFICAR SE EXISTE ALGUM REGISTRO QUE POSSA INDICAR RISCO À SEGURANÇA DA INFORMAÇÃO, EM ESPECIAL ÀS INFORMAÇÕES CLASSIFICADAS;

F) ACEITO A CONDIÇÃO DE SER OU NÃO APROVADO NA INVESTIGAÇÃO DE SEGURANÇA, RECONHECENDO QUE O MEU CREDENCIAMENTO, PARA TRATAMENTO DE INFORMAÇÕES CLASSIFICADAS, DEPENDERÁ DESSE RESULTADO; E

G) AUTORIZO O TRATAMENTO DOS DADOS PESSOAIS FORNECIDOS NESTE DOCUMENTO PARA A FINALIDADE DE INVESTIGAÇÃO PARA CREDENCIAMENTO, CONFORME O PREVISTO NO INCISO I DO ART. 7º DA LEI 13.709, DE 14 DE AGOSTO DE 2018 (Lei Geral de Proteção de Dados - LGPD).

_____, _____ de _____ de _____

(Local) (Data)

_____

(Nome e assinatura do declarante)