PORTARIA NORMATIVA Nº 6/GM/MME, DE 8 DE ABRIL DE 2021.

Dispõe sobre procedimentos relacionados ao tratamento, segurança e classificação da informação no âmbito do Ministério de Minas e Energia.

O MINISTRO DE ESTADO DE MINAS E ENERGIA, no uso das atribuições 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, no art. 4º, parágrafo único, do Decreto nº 10.139, de 28 de novembro de 2019, e o que consta do Processo nº 48300.000370/2021-21, resolve:

Art. 1º Os procedimentos relacionados ao tratamento, segurança e classificação da informação, no âmbito do Ministério de Minas e Energia, observarão as disposições desta Portaria.

CAPÍTULO I
CONCEITOS E DEFINIÇÕES

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

I - 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;

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

III - Alta Administração do Ministério de Minas e Energia - Ministro de Estado, Secretário-Executivo, Secretário-Executivo Adjunto e Secretários titulares dos Órgãos específicos singulares do Ministério de Minas e Energia;

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 órgão ou entidade da Administração Pública Federal;

VII - Gestor de Segurança e Credenciamento - responsável por promover a gestão da segurança e do credenciamento dos órgãos de registros, dos postos de controle e das pessoas naturais sob sua responsabilidade, no que se refere às informações classificadas;

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

IX - Informação ou Dado Pessoal - informação ou dado relacionados à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e 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 a 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 - Posto de Controle - Unidade do Ministério de Minas e Energia, habilitada, responsável pelo armazenamento de informação classificada em qualquer grau de sigilo;

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

XVII - Sanitização - eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados; e

XVIII - SEI - Sistema Eletrônico de Informações do Ministério de Minas e Energia.

CAPÍTULO II
DO ACESSO À INFORMAÇÃO

Art. 3º Observadas as normas e procedimentos específicos aplicáveis, mormente o contido no art. 7º da Lei nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI), serão asseguradas, no âmbito do Ministério de Minas e Energia:

I - a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;

II - a proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e

III - a proteção da informação sigilosa e da informação pessoal, observando-se o disposto na legislação específica sobre o tema, mormente o contido na Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo único. Normativos internos estabelecerão diretrizes voltadas para identificar e assegurar a proteção de dados pessoais, de dados pessoais sensíveis, bem como de dados de crianças e adolescentes, inclusive em relação à previsão de eventual compartilhamento, observando-se a legislação em vigor e o disposto pela Autoridade Nacional de Proteção de Dados.

Art. 4º As informações de interesse coletivo ou geral, produzidas ou custodiadas no âmbito das competências do Ministério de Minas e Energia, deverão ser divulgadas em local de fácil acesso, observando-se o conteúdo mínimo, a forma e os requisitos estabelecidos na LAI.

Art. 5º Qualquer interessado poderá apresentar pedido de acesso a informações, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação

requerida, sendo vedadas exigências relativas aos motivos determinantes da solicitação de informações de interesse público.

Art. 6º Deverá ser autorizado ou concedido o acesso imediato à informação disponível. Em caso de impossibilidade, o setor do Ministério de Minas e Energia instado a disponibilizar a informação demandada deverá prontamente:

I - comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão;

II - indicar as razões de fato ou de direito da recusa, total ou parcial, do acesso pretendido; ou

III - comunicar que não possui a informação, e indicar, se for do seu conhecimento, o órgão ou a entidade que a detém, ou, ainda, remeter o requerimento a esse órgão ou entidade, cientificando o interessado da remessa de seu pedido de informação.

§ 1º Por estar incumbida da intermediação das relações com os cidadãos, caberá à Ouvidoria-Geral do Ministério de Minas e Energia repassar a demanda recebida aos diversos setores do Ministério responsáveis pelo seu atendimento, fixando, à luz dos prazos legais estabelecidos, datas-limite que viabilizem a tempestiva resposta ao demandante.

§ 2º A resposta completa à solicitação deverá ser repassada pelos setores instados à Ouvidoria-Geral do Ministério de Minas e Energia até a data-limite estabelecida, cabendo a esta o contato e o encaminhamento da resposta ao demandante.

§ 3º Quando não for possível autorizar o acesso por se tratar de informação total ou parcialmente sigilosa, deverá a negação de acesso ser devidamente fundamentada pelo Chefe do setor incumbido da resposta. A Ouvidoria informará ao requerente sobre a possibilidade de recurso, prazos e condições para sua interposição, devendo, ainda, ser-lhe indicada a autoridade competente para sua apreciação.

CAPÍTULO III
DA SEGURANÇA DA INFORMAÇÃO

Art. 7º A Política de Segurança da Informação e Comunicações do Ministério de Minas e Energia (POSIC/MME) estabelecerá diretrizes, responsabilidades, competências e subsídios para a gestão da segurança da informação, e será elaborada considerando a natureza e a finalidade do Ministério, estando alinhada ao seu planejamento estratégico.

Art. 8º A POSIC/MME será elaborada/revista sob a coordenação do Gestor de Segurança da Informação, com a participação dos Integrantes do Subcomitê de Tecnologia e Segurança da Informação e Comunicações do Ministério de Minas e Energia (STSIC), e será submetida à apreciação do Comitê de Governança Digital e Segurança da Informação (CGDSI) do Ministério, para sua posterior aprovação pelo Ministro de Estado de Minas e Energia.

Seção I
Do Comitê de Governança Digital e Segurança da Informação

Art. 9º Será instituído, no âmbito do Ministério de Minas e Energia, um Comitê de Governança Digital e Segurança da Informação (CGDSI), ou estrutura similar, para, dentre outras atribuições, deliberar sobre os assuntos relativos à Política Nacional de Segurança das Informações (PNSI), a implementação das ações de governo digital e o uso de recursos de tecnologia da informação e comunicação.

Parágrafo único. Normativo interno disporá sobre a composição, organização e funcionamento do Comitê de Governança Digital e Segurança da Informação do Ministério de Minas e Energia - CGDSI/MME.

Art. 10. Compete ao CGDSI/MME a governança da segurança da informação, bem como:

I - promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à segurança da informação;

II - monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política de segurança da informação e das normas internas de segurança da informação;

III - propor alterações na Política de Segurança da Informação e Comunicações - POSIC/MME;

IV - incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar o comportamento dos agentes públicos, em consonância com as funções e as atribuições de seus órgãos e de suas entidades;

V - planejar a execução de programas, de projetos e de processos relativos à segurança da informação;

VI - estabelecer diretrizes para o processo de gestão de riscos de segurança da informação;

VII - observar as normas que estabelecem requisitos e procedimentos para a segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

VIII - implementar controles internos fundamentados na gestão de riscos da segurança da informação;

IX - instituir um sistema de gestão de segurança da informação;

X - implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados pelos órgãos da Administração Pública Federal;

XI - apreciar a proposição de recursos necessários às ações de segurança da informação, adotando as providências necessárias para assegurá-los e propiciar a execução da POSIC/MME; e

XII - observar as normas e os procedimentos específicos aplicáveis, implementar e manter mecanismos, instâncias e práticas de governança da segurança da informação em consonância com os princípios e as diretrizes estabelecidos nesta Portaria e na legislação.

Parágrafo único. O sistema de gestão de segurança da informação de que trata o inciso IX do **caput** identificará as necessidades do Ministério de Minas e Energia quanto aos requisitos de segurança da informação e implementará o processo de gestão de riscos de segurança da informação.

Art. 11. Para estruturar a gestão da segurança da informação no Ministério de Minas e Energia, deverão ser designados e/ou instituídos:

I - um Gestor de Segurança da Informação Interno - GSI;

II - um Subcomitê de Tecnologia e Segurança da Informação e Comunicações - STSIC/MME; e

III - uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

§ 1º Compete ao Presidente do Comitê de Governança Digital e Segurança da Informação do Ministério de Minas e Energia a edição de ato para dispor sobre a composição e o funcionamento do Subcomitê de Segurança da Informação e Comunicações do Ministério de Minas e Energia (STSIC/MME), observado o disposto na legislação.

§ 2º Compete ao GSI (Coordenador do Subcomitê de Segurança da Informação e Comunicações do MME) 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 padrões conhecidos.

Seção II
Do Gestor de Segurança da Informação

Art. 12. O Gestor de Segurança da Informação será designado dentre os servidores públicos ocupantes de cargo efetivo no Ministério de Minas e Energia, com formação ou capacitação técnica compatível às suas atribuições.

Art. 13. Compete ao Gestor de Segurança da Informação do Ministério de Minas e Energia:

I - coordenar o Subcomitê de Tecnologia e Segurança da Informação e Comunicações (STSIC) do Ministério de Minas e Energia;

II - coordenar a elaboração/revisão da Política de Segurança da Informação e das normas internas de segurança da informação do Ministério de Minas e Energia;

III - assessorar o CGDSI/MME na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da política e das normas internas de segurança da informação do Ministério de Minas e Energia a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor os recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

XI - implementar a gestão de risco de segurança das informações tratadas em ambiente de computação em nuvem; e

XII - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

CAPÍTULO IV
DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 14. São 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 Estão 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 16 de maio de 2012.

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

Art. 15. No âmbito do Ministério de Minas e Energia, a classificação das informações será realizada pelas seguintes autoridades competentes, conforme os graus determinados a seguir:

I - ultrassecreto e secreto: Ministro de Estado de Minas e Energia; e

II - reservado: Ministro de Estado de Minas e Energia, e ocupantes de cargos de chefia do Grupo Direção e Assessoramento Superiores (DAS), nível DAS 101.5 ou superior.

Art. 16. 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 do documento, cópia do respectivo TCI deverá ser encaminhada ao Gestor de Segurança e Credenciamento (GSC), para controle e arquivo.

§ 2º No caso de informações classificadas nos graus de sigilo ultrassecreto ou secreto, além da cópia encaminhada ao GSC, deverá ser enviada, no prazo de 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. 17. As autoridades referidas no art. 15, nos incisos I e II, desta Portaria são 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. 15, 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. 18. O sigilo da informação classificada deve 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 a classificação da informação;

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

III - uso e disseminação: refere-se à utilização, acesso, reprodução, transporte, transmissão e 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 Recepção

Art. 19. 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. 14 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. 20. Somente servidores que exerçam funções de direção ou chefia do Grupo-Direção e Assessoramento Superiores - DAS, nível DAS 101.5 ou superiores, são 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. 21. Documentos produzidos no âmbito do Ministério de Minas e Energia contendo informações passíveis de classificação de acordo com o contido no **caput** do art. 14 desta Portaria, deverão exibir, na parte central do cabeçalho e rodapé, inclusive nas suas capas, marcação própria que indique o grau de sigilo atribuído: "RESERVADO", "SECRETO" ou "ULTRASECRETO", 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. 22. 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”, onde XX é o número da página, e YY é o quantitativo total de páginas do documento.

Art. 23. 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. 24. O recebimento de processos ou documentos externos que contenham informações classificadas deverá ser protocolizado no Protocolo Geral ou no Protocolo do Gabinete do Ministro de Estado de Minas e Energia, conforme o caso, à luz do destinatário e da sensibilidade do assunto.

Art. 25. Quando do recebimento de processos ou documentos neste Ministério, deverá ser mantido o sigilo da informação já classificada por outro órgão ou entidade.

Art. 26. Ao receber processo ou documento classificado de origem externa, cabe à unidade de protocolo:

I - informar ao remetente, no prazo mais curto possível, 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 Ministério de Minas e Energia.

§ 1º Na hipótese dos casos previstos no inciso II do **caput**, cabe 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 ou aos titulares das unidades administrativas quando identificadas, conforme o caso.

§ 3º O envelope interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior, excetuando-se aqueles identificados com a marca "PESSOAL", os quais somente poderão ser abertos pelo próprio destinatário.

Art. 27. A autoridade destinatária deverá atestar o recebimento do documento classificado.

§ 1º Após tomar conhecimento do conteúdo do processo ou documento classificado, o destinatário elaborará o Formulário de Registro de Documento Classificado - FRDC (Anexo C) e o encaminhará à unidade setorial de protocolo, para a sua inclusão no Sistema Eletrônico de Informações do Ministério de Minas e Energia (SEI).

§ 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 (GSC), 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. 28. 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. 20 desta Portaria para tal fim, cabendo ao servidor com competência a elaboração do correspondente Termo de Classificação da Informação - TCI (Anexo A).

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

§ 2º 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. 29. É obrigatório o cadastro de todo processo ou documento que contenha informação classificada no Sistema Eletrônico de Informações do Ministério de Minas e Energia (SEI), utilizando-se o Formulário de Registro de Documento Classificado - FRDC (Anexo C), com observância, no que for aplicável, às normas e procedimentos de protocolização e organização processual, sendo vedada a inserção no SEI do conteúdo do documento contenho informação classificada.

Parágrafo único. Na hipótese de o processo ou documento não ter sido recebido originalmente pelo Protocolo Geral ou Protocolo-GM, 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. 30. A informação classificada deverá ser mantida e arquivada em condições especiais de segurança, separada de acordo com o grau de sigilo atribuído. Cada setor 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 autorizadas.

§ 1º Para a manutenção e 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.

§ 2º Documentos em suporte físico ou digital (mídia móvel) armazenados nos setores deverão possuir cópia de segurança armazenada no Arquivo Central do Ministério de Minas e Energia e em local a ser definido pelo CGTI/SPOA, respectivamente.

Art. 31. Os Titulares das unidades do Ministério de Minas e Energia 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 móvel (HD externo, pen drive, etc.).

Parágrafo único. Compete aos servidores designados no **caput** providenciar a entrega das cópias de segurança exigidas no § 2º do artigo anterior.

Art. 32. No Arquivo Central, 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. 33. 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 14 de novembro 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.

Seção IV
Do Uso e Disseminação

Art. 34. 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. 35. Durante seu trâmite, a guarda e o armazenamento de documentos que contenham informações classificadas são de responsabilidade daquele que detém a sua posse.

Art. 36. Documentos sigilosos em suporte físico (classificados ou não) deverão ter as suas tramitações, interna e externa, controladas por meio de sistema de protocolo, de forma a possibilitar conhecer, a qualquer momento, a sua localização e o responsável pela sua custódia.

Art. 37. 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 ser dispensados ou exonerados.

Art. 38. 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. 39. 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. 40. 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.

Art. 41. 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 classificadora ou autoridade hierarquicamente superior com igual prerrogativa, devendo as cópias serem autenticadas por essas autoridades.

Art. 42. 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. 43. Caso a preparação, impressão ou reprodução de informação classificada em qualquer grau de sigilo seja efetuada em tipografia, impressora, oficina gráfica ou similar, essa operação deverá ser acompanhada por pessoa oficialmente designada, responsável pela garantia do sigilo durante a confecção do documento.

Art. 44. A expedição e a tramitação de documentos em meio físico classificados deverão observar os seguintes procedimentos:

I - serão acondicionados em envelopes duplos;

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

III - no envelope interno constarão o destinatário e o grau de sigilo do documento, 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. 45. 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. 46. 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. 47. No transporte, transmissão e distribuição de mídias que contenham informação sigilosa deve ser aplicado controle de acesso e uso de criptografia baseada em algoritmo de Estado.

Art. 48. No transporte, transmissão e distribuição de documentos em suporte físico que forem realizados por empresa terceirizada, cabe à Subsecretaria de Planejamento, Orçamento e Administração efetuar o processo licitatório e assinar o Contrato, cabendo ao GSC 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. 49. 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
Desclassificação e Reavaliação da Informação Sigilosa

Art. 50. A desclassificação ou redução do prazo de sigilo da informação classificada poderá ser reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, observando-se a legislação em vigor sobre o assunto.

Art. 51. 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 Termo de Classificação de Informação - TCI.

Art. 52. 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. 53. Periodicamente, de acordo com rotina estabelecida pela Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS), 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. 54. Na eliminação de informação em meio eletrônico deve 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 (CPADS)

Art. 55. Será constituída, no âmbito do Ministério de Minas e Energia, uma Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) com as seguintes competências:

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

II - propor o destino final da informação desclassificada; e

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

Parágrafo único. Regulamento disporá sobre a composição, organização e funcionamento da Comissão Permanente de Avaliação de Documentos Sigilosos.

CAPÍTULO VI
DO TRATAMENTO DA INFORMAÇÃO PESSOAL

Art. 56. Independentemente de classificação de sigilo, as informações pessoais relativas à intimidade, vida privada, honra e 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.

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

§ 2º As informações mencionadas no **caput** poderão ter autorizados sua divulgação ou 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. 57. 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, e 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. 58. Para a identificação e a classificação de dados pessoais no âmbito do Ministério de Minas e Energia, 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/governanca-de-dados/GuiaInventario.pdf*, elaborado com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a realizar o levantamento e registro dos dados pessoais tratados no âmbito institucional.

Seção I
Do Tratamento de Dados Pessoais Sensíveis

Art. 59. 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.

Art. 60. 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 II
Do Tratamento de Dados de Crianças e Adolescentes

Art. 61. 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. 62. O Gestor de Segurança e Credenciamento (GSC) do Ministério de Minas e Energia, 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 Ministério de Minas e Energia.

Art. 63. Cabe ao Gestor de Segurança e Credenciamento (GSC):

I - a manutenção da qualificação técnica necessária à segurança de informação classificada, em qualquer grau de sigilo, no âmbito do Ministério de Minas e Energia;

II - a implantação, controle e funcionamento dos protocolos de Documentos Controlados, se houver, e dos documentos classificados;

III - a conformidade administrativa e sigilo dos processos de credenciamento e habilitação dentro da competência do Ministério de Minas e Energia;

IV - a proposição à Alta Administração de normas no âmbito do Ministério de Minas e Energia, para o tratamento da informação classificada e para o acesso às áreas, instalações e materiais de acesso restritos;

V - a gestão dos recursos criptográficos, das Credenciais de Segurança e dos materiais de acesso restrito, com o auxílio do Posto de Controle;

VI - o assessoramento à Alta Administração do Ministério de Minas e Energia para o tratamento de informações classificadas, em qualquer grau de sigilo;

VII - a promoção da capacitação dos agentes públicos ou militares responsáveis pelo tratamento de informação classificada, em qualquer grau de sigilo;

VIII - controlar e manter arquivo atualizado dos Termos de Classificação de Informação - TCI;

IX - coordenar os trabalhos da Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS);

X - definir as áreas de acesso restrito para efeito de segurança das informações classificadas, informando-as à Subsecretaria de Planejamento, Orçamento e Administração;

XI - providenciar, até 31 de maio de cada exercício, junto à CGTI, a disponibilização do rol das informações desclassificadas e o de documentos classificados em cada grau de sigilo na página do Ministério de Minas e Energia na internet; e

XII - responder, no âmbito do Ministério de Minas e Energia, pelas ações necessárias ao desempenho das atribuições de competência do Órgão de Registro Nível 1 (ORN1) previstas nos normativos em vigor.

§ 1º O Gestor de Segurança e Credenciamento adotará as providências para que os agentes públicos do Ministério de Minas e Energia conheçam as normas e observem os procedimentos de segurança e de tratamento de informação sigilosa classificada, de acordo com o grau de sigilo atribuído.

§ 2º A gestão de segurança e credenciamento no que se refere ao tratamento de informação classificada, em qualquer grau de sigilo, abrange ações e métodos que visam à integração das atividades de gestão de risco e de continuidade das ações de controle, acesso, credenciamento e suas capacitações.

Art. 64. Em conformidade com o disposto no item 5.5.3.2 da Norma Complementar nº 01/IN02/NSC/GSI/PR, de 27 de junho de 2013, fica delegado o ato de concessão da credencial de segurança para o Gestor de Segurança e Credenciamento, sendo vedada a subdelegação.

Seção II
Da Concessão de Credencial

Art. 65. O Ministério de Minas e Energia, mediante prévia habilitação junto ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), 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. 66. 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. 67. A fase de indicação para o processo de credenciamento se inicia com a solicitação formal, ao GSC, por autoridade que exerça função de direção, comando ou chefia do Grupo-Direção e Assessoramento Superiores - DAS, nível DAS 101.5 ou superior, e 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 - 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. 68. 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 Assessoria Especial de Acompanhamento de Políticas, Estratégias e Desempenho Setoriais (AEPED), por solicitação formal do GSC.

Art. 69. 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 peças componentes da investigação serão elaborados por: servidor público ocupante de cargo efetivo ou militar de carreira, 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. 70. 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 classificada tratados, conforme legislação pertinente.

Art. 71. A credencial de segurança terá prazo de validade máximo de dois anos, observada eventual restrição temporal contida no art. 67, parágrafo único, inciso III, 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
Descredenciamento de Segurança

Art. 72. 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, quando a necessidade de conhecer for decorrente do exercício do referido cargo.

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. 73. O descredenciamento poderá ocorrer, a qualquer tempo, a critério da Alta Administração do Ministério de Minas e Energia, ou ainda, em caso de suspeita ou quebra de segurança.

Seção IV
Do Posto de Controle

Art. 74. O Posto de Controle do Ministério de Minas e Energia atuará sob a responsabilidade e subordinação ao Gestor de Segurança e Credenciamento, observando as disposições que normatizam o seu funcionamento.

Art. 75. Caberá ao Posto de Controle do Ministério de Minas e Energia:

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, periodicamente, 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. 76. 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 Ministério de Minas e Energia 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. 30 desta Portaria.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 77. Caberá à Subsecretaria de Planejamento, Orçamento e Administração (SPOA), por meio da Coordenação-Geral de Recursos Logísticos e da Coordenação-Geral de Tecnologia da Informação, auxiliar o Gestor de Segurança da Informação (GSI) e o Gestor de Segurança e Credenciamento (GSC) na proposição e implementação de soluções e o estabelecimento de requisitos de proteção física e lógica para o adequado tratamento das informações, inclusive as classificadas, no âmbito do Ministério de Minas e Energia.

Art. 78. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou 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, também, à pessoa física ou 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. 79. Os usuários da informação são responsáveis pela segurança dos ativos da informação do Ministério de Minas e Energia 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. 80. De acordo com art. 24 da Instrução Normativa GSI/PR nº 2, de 5 de fevereiro de 2013, toda quebra de segurança de informação classificada, em qualquer grau de sigilo, deverá ser informada, tempestivamente, pelo Gestor de Segurança e Credenciamento (GSC), à Alta Administração do Órgão, que informará ao GSI/PR, relatando as circunstâncias com o maior detalhamento possível.

Art. 81. Os documentos não classificados, ou não identificados como de acesso restrito, estão automaticamente disponíveis para acesso público e imediato, em conformidade com o art. 11 da Lei nº 12.527, de 2011.

Art. 82. A solicitação de acesso externo a processos não sinalizados no SEI como de acesso público, deverá ser, obrigatoriamente, submetida à apreciação prévia do responsável pela classificação e/ou ao GSIC do Ministério, antes de sua concessão.

Art. 83. O Secretário-Executivo poderá expedir atos complementares necessários ao cumprimento desta Portaria.

Art. 84. Os casos omissos serão tratados pelo Secretário-Executivo assessorado pelo Gestor de Segurança da Informação e Gestor de Segurança e Credenciamento do Ministério de Minas e Energia, 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. 85. Esta Portaria entra em vigor na data de sua publicação.

BENTO ALBUQUERQUE

ANEXO A
MINISTÉRIO DE MINAS E ENERGIA
GRAU DE SIGILO: _____ (idêntico ao grau de sigilo do documento)

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: (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 DE MINAS E ENERGIA

Este modelo destina-se ao registro de informações que se enquadrem em alguma das situações abaixo:
A) Informações Pessoais, observado o disposto na 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 DE MINAS E ENERGIA

FORMULÁRIO DE REGISTRO DE DOCUMENTO CLASSIFICADO	
(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:
	Cargo:
(3) Registro do Destinatário do Documento no Ministério de Minas e Energia:	
(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 de Minas e Energia.

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

ANEXO D

MINISTÉRIO DE MINAS E ENERGIA

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

_____ , 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 13.709/2018 - 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 DE MINAS E ENERGIA
TERMO DE RESPONSABILIDADE PELO USO E DIVULGAÇÃO DE INFORMAÇÕES PESSOAIS

Eu, _____, identidade nº _____, expedido pelo órgão _____, e CPF nº _____, residente na rua/avenida _____, CEP_____, 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 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 13.709/2018 - 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 12.527/2011, art. 31 § 2º (uso indevido de informação);

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

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

IV - Decreto-Lei nº 2.848/1940 (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 DE MINAS E ENERGIA
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 preencha o mesmo em letras de forma com caneta azul ou preta; • Se não tiver 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_____Cidade_____UF_____País_____
Telefones residenciais: _____
Telefones celulares: _____
Telefones Funcionais:_____
Emails:_____

3. DADOS PROFISSIONAIS:

Cargo/Função/Emprego: _____
Órgão/Empresa: _____
Endereço:_____
CEP_____ Cidade _____ UF _____ País _____
Data de admissão: _____ / _____ / _____

4. DADOS DO PAI:

Nome completo: _____
Data de nascimento: _____ / _____ / _____ Local de nascimento: _____
UF: _____ País: _____ Nacionalidades: _____
Endereço: _____
CEP_____ Cidade _____ UF _____ País _____
Convive atualmente: Sim [ ] Não [ ]

5. DADOS DA MÃE:

Nome completo: _____
Data de nascimento: _____ / _____ / _____ Local de nascimento: _____
UF: _____ País: _____ Nacionalidades: _____
Endereço: _____
CEP_____ 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_____ Cidade _____ UF _____ País _____
Convive atualmente: Sim [ ] Não [ ]

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

Desde	Até	Endereço: _____
		CEP_____ Cidade _____ UF____ País_____
Desde	Até	Endereço: _____
		CEP_____ Cidade _____ UF____ País_____
Desde	Até	Endereço: _____
		CEP_____ Cidade _____ UF____ País_____
Desde	Até	

		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	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 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 13.709/2018 LGPD.

_____, ___ de _____ de ____
(Local) (Data)

_____

(Nome e assinatura do declarante)