



DECRETO Nº 35.382, DE 29 DE ABRIL DE 2014.(*)

Publicado no DODF nº 86, de 30/04/2014. Págs. 36 a 39.

Republicado no DODF nº 90, de 08/05/2014. Págs. 27 a 30.

Regulamenta o art. 42, da [Lei nº 4.990](#), de 12 de dezembro de 2012, dispõe sobre os procedimentos para credenciamento de segurança, sobre o Núcleo de Segurança e Credenciamento, institui o Comitê Gestor de Credenciamento de Segurança, e dá outras providências.

O GOVERNADOR DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o artigo 100, inciso VII, da Lei Orgânica do Distrito Federal, considerando o disposto no artigo 42, da [Lei nº 4.990](#), de 12 de dezembro de 2012, e tendo em vista o que consta nos autos do Processo nº 0428-000.085/2014, **DECRETA**:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º O credenciamento de segurança e o tratamento de informações ou dados classificados em qualquer grau de sigilo, ou previstos na legislação como sigilosos no âmbito do Poder Executivo respeitarão os procedimentos previstos neste Decreto.

Art. 2º Para os efeitos do disposto neste Decreto considera-se:

I – Acesso: possibilidade ou oportunidade de obter conhecimento sobre assunto sigiloso;

II – Assunto sigiloso: é aquele que, por sua natureza, deva ser de conhecimento restrito e, portanto, requeira medidas especiais para sua segurança;

III – Classificação: atribuição, pela autoridade competente, do grau de sigilo a dado, informação, documento, material, área ou instalação;

IV – Credencial de segurança: certificado que autoriza pessoa para o tratamento de informação classificada;

V – Credenciamento de segurança: processo utilizado para habilitar órgão ou entidade pública ou privada, e para credenciar pessoa para o tratamento de informação classificada;

VI – Comprometimento: perda de segurança resultante de obtenção, por pessoa não autorizada, do conhecimento sobre assunto sigiloso;

VII – Custódia: responsabilidade pela segurança de assunto sigiloso, decorrente da posse de material ou documento sigiloso;

VIII – Desclassificação: cancelamento da classificação, pela autoridade competente ou pelo transcurso de prazo, tornando ostensivos dados ou informações;

IX – Documento controlado: são informações ou dados classificados em qualquer grau de sigilo ou previstos na legislação como sigilosos;



- X – Gestor de segurança e credenciamento: responsável pela segurança de documento controlado no órgão de registro e posto de controle;
- XI – Grau de sigilo: gradação atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo;
- XII – Investigação para credenciamento: investigação feita com o propósito de verificar se determinada pessoa possui os requisitos indispensáveis para receber Credencial de Segurança;
- XIII- Material sigiloso: toda matéria, substância ou artefato que, por sua natureza, deva ser do conhecimento restrito, por conter ou utilizar assunto sigiloso;
- XIV – Órgão de registro nível 1: secretaria ou órgão de nível equivalente habilitado pelo Núcleo de Segurança e Credenciamento;
- XV – Órgão de registro nível 2: órgão ou entidade pública vinculada ao órgão de registro nível 1 e por este habilitado;
- XVI – Posto de controle: unidade de órgão ou entidade pública ou privada, habilitada, responsável pelo armazenamento de documento controlado;
- XVII – Reclassificação: alteração, pela autoridade competente, da classificação de dado, informação, área ou instalação sigilosos; e
- XVIII – Tratamento de informação classificada: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de documento controlado.

CAPÍTULO II
DO CREDENCIAMENTO DE SEGURANÇA
SEÇÃO I
DOS ÓRGÃOS

Art. 3º O Núcleo de Segurança e Credenciamento – NSC, de que trata o art. 42 da [Lei nº 4.990](#), de 12 de dezembro de 2012, é o órgão central de credenciamento de segurança e é composto pelos titulares dos seguintes órgãos:

- I – Casa Militar do Distrito Federal;
- II – Casa Civil, da Governadoria do Distrito Federal;
- III – Secretaria de Estado de Transparência e Controle do Distrito Federal;
- IV – Secretaria de Estado de Administração Pública do Distrito Federal; e
- V – Consultoria Jurídica do Distrito Federal.

§ 1º Cada integrante do Núcleo de Segurança e Credenciamento – NSC indicará seu respectivo suplente.

§ 2º O credenciamento do suplente ficará condicionado ao preenchimento dos requisitos previstos nos incisos II, III e IV, do artigo 13 deste Decreto e a sua indicação somente será efetivada após a investigação social.

Art. 4º Compete ao Núcleo de Segurança e Credenciamento:

- I – Habilitar os órgãos de registro nível 1 para o credenciamento de segurança de órgãos e entidades públicas e privadas, e pessoas para o tratamento de informação classificada;
- II – Habilitar postos de controle dos órgãos de registro nível 1 para armazenamento de documento controlado;
- III – Fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada;

IV – Habilitar entidade privada que mantenha vínculo de qualquer natureza com a Casa Militar do Distrito Federal para o tratamento de informação classificada;

V – Credenciar pessoa que mantenha vínculo de qualquer natureza com a Casa Militar do Distrito Federal para o tratamento de informação classificada; e

VI – Realizar inspeção e investigação para credenciamento de segurança necessária à execução do previsto nos incisos III a V deste artigo.

Art. 5º O Núcleo de Segurança e Credenciamento contará com um Comitê Gestor de Credenciamento de Segurança, integrado por representantes, titular e suplente, dos órgãos que integram o Núcleo de Segurança e Credenciamento.

§ 1º Os membros titulares e suplentes de que trata este artigo serão indicados pelos dirigentes máximos dos órgãos integrantes do NSC, e designados pelo Secretário de Estado Chefe da Casa Militar do Distrito Federal, nos termos disposto no artigo 13 deste Decreto, caso não sejam contraindicados após a investigação social.

§ 2º A participação no Comitê será considerada prestação de serviço público relevante, não remunerada.

§ 3º Poderão ser convidados para as reuniões do Comitê representantes de órgãos e entidades públicas e privadas, ou especialistas, para emitir pareceres e fornecer informações.

Art. 6º Compete ao Comitê Gestor de Credenciamento de Segurança do NSC:

I – Propor diretrizes gerais de credenciamento de segurança para tratamento de informação classificada;

II – Definir parâmetros e requisitos mínimos para:

a) qualificação técnica de órgãos e entidades públicas e privadas, para credenciamento de segurança, nos termos do disposto nos artigos 11 e 12 deste Decreto;

b) concessão de credencial de segurança para pessoas, nos termos do artigo 13 deste Decreto;

III – Avaliar periodicamente o cumprimento do disposto neste Decreto.

Art. 7º Compete à Casa Militar do Distrito Federal, no âmbito do NSC:

I – Expedir atos complementares e estabelecer procedimentos para o credenciamento de segurança e para o tratamento de informação classificada;

II – Acompanhar averiguações e processos de avaliação e recuperação dos danos decorrentes de quebra de segurança;

III – Assessorar o Governador do Distrito Federal nos assuntos relacionados com credenciamento de segurança para o tratamento de informação classificada;

IV – Propor e promover a regulamentação do credenciamento de segurança de pessoas físicas, empresas, órgãos e entidades para tratamento de informações sigilosas; e

V – Garantir a segurança de informações sigilosas.

Art. 8º Compete aos órgãos de registro nível 1:

I – Habilitar órgãos de registro nível 2 para credenciar pessoa para o tratamento de informação classificada;

II – Habilitar posto de controle dos órgãos e entidades públicas ou privadas, que com ele mantenham vínculo de qualquer natureza, para o armazenamento de documento controlado;

III – Credenciar pessoa que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada;

IV- Realizar inspeção e investigação para credenciamento de segurança necessária à execução do previsto no inciso anterior; e



V – Fiscalizar o cumprimento das normas e procedimentos de credenciamento de segurança e tratamento de informação classificada, no âmbito de suas competências.

Art. 9º Compete aos órgãos de registro nível 2, investigar e credenciar pessoa que com ele mantenha vínculo de qualquer natureza para o tratamento de informação classificada.

Parágrafo único. A competência para realização de inspeção de que trata o inciso IV, do artigo anterior poderá ser delegada a órgão de registro nível 2.

Art. 10. Compete ao posto de controle:

I – Realizar o controle das credenciais de segurança das pessoas que com ele mantenham vínculo de qualquer natureza;

II – Garantir a segurança de documento controlado sob sua responsabilidade.

SEÇÃO II

DOS PROCEDIMENTOS

Art. 11. A habilitação dos órgãos e entidades públicas para o credenciamento de segurança fica condicionada aos seguintes requisitos:

I – Comprovação de qualificação técnica necessária à segurança de documento controlado;

II – Designação de gestor de segurança e credenciamento, e de seu substituto.

Art. 12. A concessão de habilitação de entidade privada como posto de controle fica condicionada aos seguintes requisitos:

I – Regularidade fiscal;

II – Comprovação de qualificação técnica necessária à segurança de documento controlado;

III – Expectativa de assinatura de contrato sigiloso;

IV – Designação de gestor de segurança e credenciamento, e de seu substituto; e

V – Aprovação em inspeção para habilitação de segurança.

Art. 13. A concessão de credencial de segurança a uma pessoa fica condicionada aos seguintes requisitos:

I – Solicitação do órgão ou entidade pública ou privada em que a pessoa exerce atividade;

II – Preenchimento de formulário com dados pessoais e autorização para investigação social;

III – Aptidão para o tratamento da informação classificada, verificada na investigação social; e

IV – Declaração de conhecimento das normas e procedimentos de credenciamento de segurança e de tratamento de informação classificada.

Art. 14. A habilitação para credenciamento de segurança e a concessão de credencial de segurança resultarão da análise objetiva dos requisitos previstos neste Decreto.

Art. 15. Os órgãos de registro nível 1 e nível 2 poderão 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. 16. Cada órgão de registro terá, no mínimo, um posto de controle habilitado.



CAPÍTULO III
DA SEGURANÇA DE INFORMAÇÃO CLASSIFICADA

SEÇÃO I

DISPOSIÇÕES GERAIS

Art. 17. Os órgãos e entidades da administração direta e indireta do Poder Executivo do Distrito Federal adotarão providências para que os agentes públicos conheçam as normas e observem os procedimentos de credenciamento de segurança e de tratamento de informação classificada.

Parágrafo único. O disposto no caput deste artigo se aplica à pessoa ou entidade privada que, em razão de qualquer vínculo com o Poder Público, execute atividade de credenciamento de segurança ou de tratamento de informação classificada.

Art. 18. A publicação de atos normativos relativos a documento controlado ou protegido por sigilo legal ou judicial poderá limitar-se, quando necessário, aos seus respectivos números, datas de expedição e ementas, redigidos de modo a não comprometer o sigilo.

SEÇÃO II

DA SEGURANÇA E RESPONSABILIDADE

Art. 19. Compete ao dirigente dos órgãos, das empresas e das entidades credenciados para tratamento de informações sigilosas se assegurar de que as pessoas, sob suas ordens e credenciadas para tratamento de assuntos sigilosos, conheçam perfeitamente as medidas de segurança em vigor.

Art. 20. Qualquer pessoa que tome conhecimento de assunto sigiloso fica, automaticamente, responsável pela manutenção de seu sigilo.

Art. 21. Verificando-se qualquer ocorrência que possa implicar o comprometimento de assunto sigiloso, a autoridade competente tomará as providências necessárias para verificar a extensão do comprometimento e apurar as responsabilidades.

Art. 22. Qualquer pessoa que tenha conhecimento de situação na qual um assunto sigiloso possa estar ou venha a ser comprometido deverá comunicar tal fato ao seu Chefe imediato e ou à autoridade responsável.

Art. 23. Qualquer pessoa que tenha extraviado documento ou material sigiloso deverá comunicar essa ocorrência ao seu Chefe imediato ou à autoridade responsável pela custódia do documento ou material.

Parágrafo Único. Idêntica providência deverá ser tomada por qualquer pessoa que venha a encontrar ou tenha conhecimento de que foi achado documento ou material sigiloso.

SEÇÃO III

DO ACESSO

Art. 24. O acesso, a divulgação e o tratamento de documento controlado somente poderão ser concedidos à pessoa que tenha necessidade de conhecê-lo e que possua Credencial de Segurança no grau apropriado e na forma deste Decreto.

§ 1º A necessidade de conhecer, de que trata este artigo, decorre do efetivo exercício de cargo, função ou atividade.

§ 2º O acesso, concedido à determinada pessoa, deverá ser continuamente reavaliado pelo dirigente, que o cancelará tão logo deixe de ser preenchida qualquer condição estabelecida para sua concessão.

Art. 25. O acesso ao assunto sigiloso depende da função desempenhada pela pessoa e não de seu grau hierárquico, posição ou precedência dentro do órgão, da empresa ou da entidade, sendo, contudo, obrigatório o credenciamento de segurança compatível, de acordo com as normas estabelecidas para concessão de Credencial de Segurança.



Art. 26. O acesso à informação, classificada em qualquer grau de sigilo, por pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo – TCMS, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

SEÇÃO IV

DO DOCUMENTO CONTROLADO

Art. 27. Para o tratamento de documento controlado, o órgão ou entidade poderá adotar os seguintes procedimentos adicionais de controle:

- I – Identificação dos destinatários em protocolo e recibo específicos;
- II – Lavratura de termo de custódia e registro em protocolo específico;
- III – Lavratura anual de termo de inventário, pelo órgão ou entidade expedidor e pelo órgão ou entidade receptor; e
- IV – lavratura de termo de transferência de custódia ou guarda.

§ 1º O termo de inventário previsto no inciso III deste artigo deverá conter, no mínimo, os seguintes elementos:

- a) numeração sequencial e data;
- b) órgãos produtor e custodiante do documento controlado;
- c) lista de documentos controlados; e
- d) local e assinatura.

§ 2º O termo de transferência previsto no inciso IV deste artigo deverá conter, no mínimo, os seguintes elementos:

- a) numeração sequencial e data;
- b) agentes públicos substituto e substituído;
- c) identificação dos documentos ou termos de inventário a serem transferidos; e
- d) local e assinatura.

Art. 28. O documento ultrassecreto é considerado documento controlado desde sua classificação ou reclassificação.

SEÇÃO V

DA MARCAÇÃO

Art. 29. A marcação será feita nos cabeçalhos e rodapés das páginas que contiverem informação classificada e nas capas do documento.

§ 1º As páginas serão numeradas seguidamente, devendo cada uma conter indicação do total de páginas que compõe o documento.

§ 2º A marcação deverá ser feita de modo a não prejudicar a compreensão da informação.

Art. 30. O Documento Controlado possuirá a marcação de que trata o artigo 29 deste Decreto e conterà, na capa e em todas as páginas, a expressão em diagonal “Documento Controlado (DC)” e o número de controle, que indicará o agente público custodiante.

Art. 31. A indicação do grau de sigilo em mapas, fotocartas, cartas, fotografias e em quaisquer outros tipos de imagens e meios eletrônicos de armazenamento obedecerá aos procedimentos complementares adotados pelos órgãos e entidades.

SEÇÃO VI

DA EXPEDIÇÃO, TRAMITAÇÃO E COMUNICAÇÃO



Art. 32. A expedição e a tramitação de documentos 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 for 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. 33. A expedição, a condução e a entrega de documento com informação classificada em grau de sigilo ultrassecreto serão realizadas, 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 a sua postagem.

Art. 34. 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.

Art. 35. Cabe aos responsáveis pelo recebimento de documento controlado, independentemente do meio e formato:

I – Registrar o recebimento do documento;

II – Verificar a integridade do meio de recebimento e registrar indícios de violação ou de irregularidade, comunicando ao destinatário, que informará imediatamente ao remetente; e

III – Informar ao remetente o recebimento da informação, no prazo mais curto possível.

§ 1º Caso a tramitação ocorra por expediente ou correspondência, o envelope interno somente será aberto pelo destinatário, seu representante autorizado ou autoridade hierarquicamente superior.

§ 2º Envelopes internos contendo a marca “PESSOAL” somente poderão ser abertos pelo destinatário.

Art. 36. Os documentos ultrassecretos e secretos serão manuseados pelo menor número possível de pessoas, a fim de tornar mais efetiva a sua segurança.

SEÇÃO VII

DA REPRODUÇÃO

Art. 37. A reprodução total ou parcial de documento controlado terá o mesmo grau de sigilo do documento.

§ 1º Qualquer reprodução de Documento Controlado condiciona-se à autorização expressa da autoridade classificadora ou autoridade hierarquicamente superior com igual prerrogativa.

§ 2º As cópias serão autenticadas pela autoridade classificadora ou autoridade hierarquicamente superior com igual prerrogativa.

Art. 38. Caso a preparação, a impressão ou a reprodução de documento controlado seja efetuada em tipografia, impressora, oficina gráfica ou similar, essas operações serão acompanhadas por pessoa oficialmente designada, que ficará responsável pela garantia do sigilo durante a confecção do documento.

SEÇÃO VIII

DA SEGURANÇA NO ARQUIVAMENTO E NA PRESERVAÇÃO



Art. 39. Os Documentos Controlados serão guardados em arquivos que ofereçam condições especiais de segurança, cabendo às empresas, às entidades e aos órgãos credenciados para tratamento de informações sigilosas adotarem as medidas necessárias para a salvaguarda dos documentos.

§ 1º Para 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 seu grau de sigilo.

§ 2º Para a guarda de documentos reservados é necessário, no mínimo, o uso de arquivo com chave.

§ 3º Para armazenamento em meio eletrônico de documento controlado é obrigatória a utilização de sistemas de tecnologia da informação atualizados, de forma a prevenir ameaças de quebra de segurança, observado o disposto no artigo 46 deste Decreto.

§ 4º 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.

Art. 40. Os originais dos documentos controlados deverão ser mantidos e preservados em arquivo nos órgãos, nas empresas e nas entidades que os produziu ou que os recebeu.

Art. 41. Os meios eletrônicos de armazenamento de documento controlado, inclusive os dispositivos móveis, devem utilizar recursos criptográficos adequados ao seu manuseio.

Art. 42. Os agentes responsáveis pela guarda ou custódia de documento controlado o transmitirá a seus substitutos, devidamente conferido, quando da passagem ou transferência de responsabilidade.

Parágrafo único. Aplica-se o disposto neste artigo aos responsáveis pela guarda ou custódia de material de acesso restrito.

Art. 43. Para a avaliação e a seleção de documento com informação desclassificada, para fins de guarda permanente ou eliminação, deverá ser observado o disposto no Decreto nº 8.530, de 14 de março de 1985, na Lei nº 2.545, de 28 de abril de 2000 e no Decreto nº 24.205, de 10 de novembro de 2003.

Art. 44. O documento de guarda permanente que contiver informação ou dado classificado em qualquer grau de sigilo será encaminhado, em caso de desclassificação, ao Arquivo Público do Distrito Federal, para fins de organização, preservação e acesso.

Art. 45. O documento de guarda permanente não pode ser desfigurado ou destruído, ficando o autor sujeito à responsabilização penal, civil e administrativa, na forma da lei.

SEÇÃO IX

DOS SISTEMAS DE INFORMAÇÃO

Art. 46. 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.

§ 1º A transmissão de documento controlado 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 A autenticidade da identidade do usuário da rede deverá ser garantida, no mínimo, pelo uso de certificado digital.

§ 3º Os sistemas de informação de que trata o caput deverão ter níveis diversos de controle de acesso e utilizar recursos criptográficos adequados aos respectivos graus de sigilo.



§ 4º Os sistemas de informação de que trata o caput deverão manter controle e registro dos acessos autorizados e não autorizados e das transações realizadas por prazo igual ou superior ao de restrição de acesso à informação.

Art. 47. Os equipamentos e sistemas utilizados para a produção de documento controlado 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.

Art. 48. A cifração e a decifração de documento controlado deverão utilizar recurso criptográfico baseado em algoritmo.

Art. 49. Os procedimentos de tratamento de documento controlado aplicam-se aos recursos criptográficos, atendidas as seguintes exigências:

I – Realização de vistorias periódicas, com a finalidade de assegurar a execução das operações criptográficas;

II – Manutenção de inventários completos e atualizados do material de criptografia existente;

III – Designação de sistemas criptográficos adequados a cada destinatário;

IV – Comunicação, ao superior hierárquico ou à autoridade competente, de anormalidade relativa ao sigilo, à inviolabilidade, à integridade, à autenticidade, à legitimidade e à disponibilidade de informações criptografadas; e

V – Identificação de indícios de violação, de interceptação ou de irregularidades na transmissão ou recebimento de informações criptografadas.

SEÇÃO X

DAS ÁREAS, INSTALAÇÕES E MATERIAIS

Art. 50. As áreas e instalações que contenham documento controlado ou que, por sua utilização ou finalidade exigir proteção, terão seu acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Art. 51. Os órgãos e entidades públicas adotarão medidas para definição, demarcação, sinalização, segurança e autorização de acesso às áreas restritas sob sua responsabilidade.

Parágrafo único. As visitas às áreas ou às instalações de acesso restrito serão disciplinadas pelo órgão ou entidade responsável pela sua segurança.

Art. 52. Os materiais que, por sua utilização ou finalidade, exigirem proteção, terão acesso restrito às pessoas autorizadas pelo órgão ou entidade.

Art. 53. São considerados materiais de acesso restrito qualquer matéria, produto, substância ou sistema que contenha, utilize ou veicule conhecimento ou documento controlado, cuja divulgação implique risco ou dano aos interesses da sociedade e do Estado, tais como:

I – Equipamentos, máquinas, modelos, moldes, maquetes, protótipos, artefatos, aparelhos, dispositivos, instrumentos, representações cartográficas, sistemas, suprimentos e manuais de instrução;

II – Veículos terrestres, aquaviários e aéreos, suas partes, peças e componentes;

III – Armamentos e seus acessórios, as munições e os aparelhos, equipamentos, suprimentos e insumos correlatos;

IV – Aparelhos, equipamentos, suprimentos e programas relacionados à tecnologia da informação e comunicações e à inteligência de sinais e imagens;

V – Recursos criptográficos; e

VI – Explosivos, líquidos e gases.



Art. 54. Os órgãos ou entidades públicas encarregadas da preparação de planos, pesquisas e trabalhos de aperfeiçoamento ou de elaboração de projeto, prova, produção, aquisição, armazenagem ou emprego de material de acesso restrito expedirão instruções adicionais necessárias à salvaguarda dos assuntos a eles relacionados.

Art. 55. O meio de transporte utilizado para deslocamento de material de acesso restrito é de responsabilidade do custodiante e deverá considerar o grau de sigilo das informações.

§ 1º O material de acesso restrito poderá ser transportado por empresas contratadas, adotadas as medidas necessárias à manutenção do sigilo das informações.

§ 2º As medidas necessárias para a segurança do material transportado serão prévia e explicitamente estabelecidas em contrato.

SEÇÃO XI

DA CELEBRAÇÃO DE CONTRATOS SIGILOSOS

Art. 56. A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto ou execução envolva documento classificado é condicionada à assinatura de TCMS e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

I – Obrigação de manter sigilo relativo ao objeto e à sua execução;

II – Possibilidade de alteração do objeto para inclusão ou alteração de cláusula de segurança não estipulada previamente;

III – Obrigação de adotar procedimentos de segurança adequados para a manutenção do sigilo relativo ao objeto e à execução;

IV – Identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a documento classificado e material sigiloso;

V – Obrigação de receber inspeções para habilitação de segurança e sua manutenção; e

VI – Responsabilidade quanto aos procedimentos de segurança na subcontratação, no todo ou em parte.

Art. 57. Aos órgãos e entidades públicas com os quais os contratantes mantêm vínculo de qualquer natureza, caberá adotar procedimentos de segurança do documento controlado ou do material de acesso restrito em poder dos contratados ou subcontratados.

CAPÍTULO IV

DA INDEXAÇÃO DE DOCUMENTO COM INFORMAÇÃO CLASSIFICADA

Art. 58. A informação classificada em qualquer grau de sigilo ou o documento que a contenha receberá o Código de Indexação de Documento que contém Informação Classificada – CIDIC.

Parágrafo único. O CIDIC será composto por elementos que garantirão a proteção e a restrição temporária de acesso à informação classificada, e será estruturado em duas partes.

Art. 59. A primeira parte do CIDIC será composta pelo Número Único de Protocolo–NUP, originalmente cadastrado conforme legislação de gestão documental.

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

§ 2º Não serão usadas tabelas de classificação de assunto ou de natureza do documento, em razão de exigência de restrição temporária de acesso à informação classificada em qualquer grau de sigilo, sob pena de pôr em risco sua proteção e confidencialidade.



Art. 60. A segunda parte do CIDIC será composta dos seguintes elementos:

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

II – Categorias: indicação, com dois dígitos, da categoria relativa, exclusivamente, ao primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), conforme Anexo Único;

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

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

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

a) reclassificação da informação resultante de reavaliação; ou

b) primeiro registro da classificação.

VI – Indicação da data de prorrogação da manutenção da classificação: indicação, exclusivamente, para informação classificada no grau de sigilo ultrassecreto, de acordo com a seguinte composição: dia (dois dígitos)/mês (dois dígitos)/ano (quatro dígitos), na cor vermelha, quando possível.

Art. 61. Para fins de gestão documental, deverá ser guardado o histórico das alterações do CIDIC.

CAPÍTULO V

DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 62. Os órgãos e entidades públicas e privadas poderão expedir instruções complementares, no âmbito de suas competências, que detalharão os procedimentos relativos ao credenciamento de segurança e ao tratamento de documento classificado ou material sigiloso.

Art. 63. Os órgãos e entidades públicas e privadas exigirão termo de compromisso de manutenção de sigilo dos seus servidores, funcionários e empregados que direta ou indiretamente tenham acesso a documento classificado ou material sigiloso.

Parágrafo único. Os agentes de que trata o caput deste artigo comprometem-se, após o desligamento, mediante a assinatura de termo próprio, a não revelar ou divulgar informações ou dados sigilosos dos quais tenham tido conhecimento no exercício de cargo, função ou emprego público ou privado.

Art. 64. Os agentes responsáveis pela custódia de documentos e materiais e pela segurança de áreas, instalações ou sistemas de informação de natureza sigilosa sujeitam-se às normas referentes ao sigilo profissional, em razão do ofício, e ao seu código de ética específico, sem prejuízo de outras sanções.

Art. 65. Este Decreto entra em vigor na data de sua publicação.

Art. 66. Revogam-se as disposições em contrário, em especial os artigos 56 e 57, ambos do [Decreto nº 34.276](#), de 11 de abril de 2013.

Brasília, 29 de abril de 2014.

126º da República e 55º de Brasília

AGNELO QUEIROZ

() Republicado por ter sido encaminhado com incorreção no original, publicado no DODF nº 86, de 30 de abril de 2014.*

ANEXO ÚNICO

CÓDIGO DE INDEXAÇÃO DE DOCUMENTO QUE CONTÉM INFORMAÇÃO CLASSIFICADA - CIDIC – CATEGORIAS

CATEGORIAS	CÓDIGO NUMÉRICO
Agricultura, extrativismo e pesca	01
Ciência, Informação e Comunicação	02
Comércio, Serviços e Turismo	03
Cultura, Lazer e Esporte	04
Defesa e Segurança	05
Economia e Finanças	06
Educação	07
Governo e Política	08
Habitação, Saneamento e Urbanismo	09
Indústria	10
Justiça e Legislação	11
Meio ambiente	12
Pessoa, família e sociedade	13
Relações internacionais	14
Saúde	15
Trabalho	16
Transportes e trânsito	17

Obs.:

1. Categorias: representam os aspectos ou temas correlacionados à informação classificada em grau de sigilo, e serão indicadas pela Autoridade Classificadora. Para tanto deverá ser usado, exclusivamente, o primeiro nível do Vocabulário Controlado do Governo Eletrônico (VCGE), definidos no Padrão de Interoperabilidade do Governo Eletrônico (e-Ping), conforme quadro acima.
2. Composição no CIDIC: 2 dígitos = código numérico

