Ministério da Saúde

FIOCRUZ - Fundação Oswaldo Cruz

Vice-Presidência de Gestão e Desenvolvimento Institucional

Coordenação de Gestão de Tecnologia da Informação

NORMA INSTITUCIONAL DE CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÃO CLASSIFICADA

ORIGEM

VPGDI/CGTI/Serviço de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

- Decreto nº 3.505, de 13 de junho de 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Portaria nº 3.207, de 20 de outubro de 2010, que institui a Política de Segurança da Informação e Comunicações no Ministério da Saúde.
- Portaria nº 69, de 21 de fevereiro de 2011, que institui a Política de Segurança da Informação e Comunicações da Fundação Oswaldo Cruz.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todos no âmbito da Fiocruz.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não se aplica.

1. OBJETIVO

Este documento estabelece as diretrizes para classificação e tratamento das informações quanto ao seu grau de sigilo nos aspectos referentes à segurança da informação e comunicações no âmbito da Fiocruz.

2. PÚBLICO-ALVO

Esta norma aplica-se a todos que manipulam informações institucionais e pessoais no âmbito da Fiocruz.

3. DEFINIÇÕES E TERMINOLOGIAS

- Algoritmo de Estado: função matemática utilizada na cifração e na decifração, Desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável;
- Autenticidade - qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
- Chave Criptográfica: valor que trabalha com um algoritmo criptográfico para cifração ou decifração;
- Cifração: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la;
- Credencial de Segurança: certificado que autoriza pessoa para o tratamento de informação classificada;
- Dados processados - dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;
- Decifração: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;
- Disponibilidade - qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
- Documento - unidade de registro de informações, qualquer que seja o suporte ou formato;
- Informação - dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
- 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;

- Informação pessoal - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;
- Informação sigilosa - informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;
- Integridade - qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
- 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;

4. DOCUMENTOS DE REFERÊNCIA DA NORMA

- Lei nº 12.527, de 18 de novembro de 2011
- Decreto nº 7.724, de 16 de maio de 2012
- Decreto nº 7.845, de 14 de novembro de 2012
- Norma Complementar 09/IN01/DSIC/GSIPR, de 15 de fevereiro de 2013
- Instrução Normativa 02 GSIPR, de 5 de fevereiro de 2013
- Norma Complementar 01/IN02/DSIC/GSIPR, de 27 de junho de 2013
- ISO/IEC 27001/2008

5. REGRAS

5.1. Disposições gerais

5.1.1 Deve-se classificar a informação em termos de seu valor, requisitos legais, sensibilidade e criticidade para a Fiocruz.

5.1.2 O nível de proteção deve ser avaliado analisando a confidencialidade, a integridade e a disponibilidade da informação.

5.1.3 Os procedimentos de rotulação da informação precisam abranger tanto os ativos de informação no formato eletrônico quanto no formato físico.

5.1.4 O disposto nesta norma não exclui as demais hipóteses legais de sigilo e de segredo de justiça, nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

5.2. Classificação da informação quanto ao grau de sigilo

5.2.1 Deve-se classificar toda informação que possa vir a colocar em risco a segurança do estado ou da sociedade, como por exemplo:

5.2.1.1 Pôr em risco a vida, a segurança ou a saúde da população;

5.2.1.2 Oferecer elevado risco à estabilidade financeira do país, econômica ou monetária do país;

5.2.1.3 Prejudicar ou causar riscos a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;

5.2.1.4 Pôr em risco a segurança das instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares.

5.2.2 Observando-se o teor e em razão a imprescindibilidade à segurança da sociedade ou do Estado, a informação poderá ser classificada como ultrassecreta, secreta e reservada.

5.2.3 Os prazos máximos de restrição de acesso à informação vigoram a partir da sua data de produção e são os seguintes:

5.2.3.1 A informação classificada como ultrassecreta terá o prazo de restrição de 25 (vinte e cinco) anos e sua classificação será de competência das seguintes autoridades: Presidente da República, Vice-presidente da República, Ministros de Estado e autoridades com as mesmas prerrogativas (Comandantes da Marinha, Comandantes do Exército, Comandantes da Aeronáutica, Chefes de Missões Diplomáticas e Consulares permanentes no exterior).

5.2.3.2 A informação classificada como secreta terá o prazo de restrição de 15 (quinze) anos e sua classificação será de competência das autoridades supracitadas no item “a” e: titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista.

5.2.3.3 A informação classificada como reservada terá o prazo de restrição de 5 (cinco) anos e sua classificação será de competência das autoridades supracitadas nos itens “a” e “b” e: autoridades que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo-Direção e Assessoramento Superiores, ou hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade;

5.2.4 Transcorrido o prazo de classificação ou consumado algum evento que defina o seu termo final, a informação torna-se automaticamente de acesso público.

5.2.5 Para a classificação da informação em determinado grau de sigilo, deve ser observado o interesse público das informações e utilizado o critério menos restritivo possível.

5.2.6 A informação classificada deve ser formalizada e conter minimamente o assunto sobre o qual versa a informação, fundamento da classificação, indicação do prazo de sigilo, identificação da autoridade que a classificou.

5.3. Da proteção e do controle de informações sigilosas

5.3.1 É dever da Fiocruz assegurar a proteção e controlar o acesso e a divulgação de informações sigilosas produzidas por suas unidades.

5.3.2 Entidades públicas ou privadas que tiverem algum vínculo com a Fiocruz para o tratamento ou o uso de informações sigilosas deverão observar as regulamentações das leis vigentes, inclusive instruir seus empregados, prepostos ou representantes a observarem as medidas e procedimentos de segurança das informações classificadas quanto ao seu grau de sigilo.

5.3.3 Aquele que tiver acesso à informação classificada cria a obrigação de resguardar o sigilo.

5.3.4 O acesso, a divulgação e o tratamento de informações classificadas como sigilosas ficarão restritos a pessoas que tenham necessidade de conhecê-la e que sejam devidamente credenciadas na forma das regulamentações das leis vigentes.

5.4. Tratamento das Informações Pessoais

5.4.1 O tratamento das informações pessoais deve respeitar à intimidade, a honra, a vida privada e a imagem das pessoas.

5.4.2 As informações pessoais terão seu acesso restrito, independente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos, a contar da sua data de produção.

5.4.3 Terceiros poderão ter acessos às informações pessoais mediante previsão legal ou consentimento expresso da pessoa a que se refere às informações.

5.4.4 Não haverá a necessidade de consentimento da pessoa nos casos que a informação for necessária para:

5.4.4.1 A prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico.

5.4.4.2 Realização de pesquisas e estatísticas cientificas de evidente interesse público ou geral, previsto em lei, sendo vedada a identificação da pessoa a que as informações se referirem.

5.4.4.3 Ao cumprimento de ordem judicial, à defesa de direitos humanos, ou à proteção do interesse público e geral preponderante, requisição de autoridade policial no exercício da investigação policial com fim de apuração de infrações penais, aos membros do Ministério Público no exercício de suas atividades para a instrução do Inquérito civil e procedimentos administrativos.

5.5. Dos sistemas de informação

5.5.1 Devem ser utilizados sistemas de informação e canais de comunicação seguros.

5.5.2 As informações, classificadas em qualquer grau de sigilo, contidas em sistemas de informação, devem ser transmitidas através da rede corporativa por meio de um canal seguro.

5.5.3 De forma a garantir a autenticidade, a identidade do usuário da rede deve ser garantida minimamente pelo uso de certificado digital.

5.5.4 Os sistemas de informação devem prever níveis de controle de acesso e recursos criptográficos adequados aos graus de sigilo.

5.5.5 Os sistemas de informação devem manter controle e registro dos acessos autorizados e não-autorizados e das transações realizadas por um prazo igual ou superior ao de restrição da informação.

5.5.6 Os equipamentos e sistemas utilizados para a produção de documento com informação classificada em qualquer grau de sigilo deverão estar isolados ou ligados a canais de comunicação seguros, que estejam fisicamente ou logicamente isolados de qualquer outro, e que possuam recursos criptográficos e de segurança adequados à sua proteção.

5.5.7 Toda a informação, classificada em qualquer grau de sigilo, produzida, armazenada ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deve ser protegida com recurso criptográfico baseado em algoritmo de Estado.

5.5.8 A cifração e decifração de informações classificadas, em qualquer grau de sigilo, utilizará exclusivamente recurso criptográfico baseado em algoritmo de Estado em conformidade com os parâmetros e padrões mínimos conforme as legislações vigentes.

5.5.9 Todo recurso criptográfico constitui material de acesso restrito e requer procedimentos especiais para sua criação, controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte, em conformidade com a legislação vigente.

5.5.10 O recurso criptográfico, baseado em algoritmo de Estado, deve ser de desenvolvimento próprio ou por órgãos e entidades da APF, direta ou indireta, mediante acordo ou termo de cooperação, vedada a participação e contratação de empresas e profissionais externos à APF, para tal finalidade.

5.5.11 Com anuência da Alta Administração do órgão ou entidade, o previsto no item 5.5.10 poderá ser terceirizado, desde que sejam atendidas obrigatoriamente as seguintes condições:

5.5.11.1 Seja realizado exclusivamente por meio de contrato sigiloso, conforme as legislações vigentes.

5.5.11.2 Seja previsto em contrato que fica vedado ao contratado os direitos de propriedade e exploração comercial do recurso criptográfico com algoritmo de estado.

5.6. Das áreas, instalações e materiais

5.6.1 As áreas e instalações que contenham documento com informação classificada em qualquer grau de sigilo, ou que, por sua utilização ou finalidade, demandarem proteção, terão seu acesso restrito.

5.6.2 Devem ser adotadas medidas para definição, demarcação, sinalização, segurança e autorização de acessos às áreas restritas.

5.6.3 Qualquer matéria, produto, substância ou sistema que contenha, utilize e veicule conhecimento ou informação classificada em qualquer grau de sigilo, informação econômica ou informação científico-tecnológica, cuja divulgação implique em risco ou danos aos interesses da sociedade e do estado, como por exemplo: recursos criptográficos,

equipamentos, máquinas, protótipos, sistemas, entre outros, devem receber o devido tratamento.

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

5.6.5 O material de acesso restrito poderá ser transportado por empresas contratadas, desde que sejam adotadas as medidas necessárias à manutenção do sigilo das informações. Tais medidas de manutenção de sigilo devem ser estabelecidas em contratos.

5.7. Da celebração de contratos sigilosos

5.7.1 A celebração de contrato, convênio, acordo, ajuste, termo de cooperação ou protocolo de intenção cujo objeto contenha informação classificada em qualquer grau de sigilo, ou cuja execução envolva informação classificada, é condicionada à assinatura do Termo de Compromisso de Manutenção de Sigilo (TCMS) e ao estabelecimento de cláusulas contratuais que prevejam os seguintes requisitos:

5.7.1.1 Obrigação de manter sigilo relativo ao objeto e a sua execução;

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

5.7.1.3 Obrigação de adotar procedimentos de segurança adequados, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto;

5.7.1.4 Identificação, para fins de concessão de credencial de segurança e assinatura do TCMS, das pessoas que poderão ter acesso a informação classificada em qualquer grau de sigilo e material de acesso restrito;

5.7.1.5 Obrigação de receber inspeções para habilitação de segurança e sua manutenção; e

5.7.1.6 Responsabilidade em relação aos procedimentos de segurança, relativa à subcontratação, no todo ou em parte.

5.8. Dos procedimentos para classificação de informação

5.8.1 A Comissão Permanente de Acesso à Informação da Fiocruz (CPAI) definirá metodologia de trabalho e estabelecerá critérios para a classificação, desclassificação ou reavaliação de documentos, dados e informações sigilosas no âmbito da instituição.

5.8.2 A informação que for classificada em qualquer grau de sigilo deve ser formalizada no Termo de Classificação de Informação (TCI).

5.8.3 O TCI deve conter as seguintes informações: código de indexação do documento, grau de sigilo, categoria na qual se enquadra a informação, tipo de documento, data da produção do documento, indicação de dispositivo legal que fundamenta a classificação, razões da classificação, indicação do prazo de sigilo, data da classificação e identificação da autoridade que classificou a informação.

5.8.4 A informação classificada no grau ultrassecreto ou secreto deve encaminhar cópia do TCI à Comissão Mista de Reavaliação de Informações no prazo de trinta dias, contado da decisão de classificação ou de ratificação.

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

5.9. Da Desclassificação e Reavaliação da Informação Classificada em Grau de Sigilo

5.9.1 A classificação das informações será reavaliada pela autoridade classificadora ou por autoridade hierarquicamente superior, mediante provocação ou de ofício, para desclassificação ou redução do prazo de sigilo.

5.9.2 Para toda informação classificada que sofrer desclassificação ou reavaliação devem ser observados:

5.9.2.1 O prazo máximo de restrição de acesso à informação;

5.9.2.2 O prazo máximo de quatro anos para revisão de ofício das informações classificadas no grau ultrassecreto ou secreto;

5.9.2.3 A permanência das razões da classificação;

5.9.2.4 A possibilidade de danos ou riscos decorrentes da divulgação ou acesso irrestrito da informação; e

5.9.2.5 A peculiaridade das informações produzidas no exterior por autoridades ou agentes públicos.

5.9.3 O pedido de desclassificação e reavaliação das informações classificadas será endereçado a autoridade classificadora, que decidirá no prazo de trinta dias.

5.9.4 Negado o pedido de desclassificação ou de reavaliação pela autoridade classificadora, o requerente poderá apresentar recurso no prazo de dez dias, contando da ciência negativa, ao Ministro de Estado ou à autoridade com as mesmas prerrogativas, que decidirá no prazo de trinta dias.

6. DISPOSIÇÕES FINAIS

6.1. Os usuários devem comunicar e/ou reportar os incidentes que afetam a segurança dos ativos ou o descumprimento desta norma à área de TI correlata.

6.2. Em casos de quebra de segurança da informação por meio de recursos de TI, o Serviço de Segurança da Informação e Comunicações da CGTI deve ser imediatamente acionado pela área de TI correlata para adotar as providências necessárias.

6.3. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações da Fiocruz.

7. VIGÊNCIA E ATUALIZAÇÃO

Esta norma operacional entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.