PORTARIA Nº 3.207, DE 20 DE OUTUBRO DE 2010

Institui a Política de Segurança da Informação e Comunicações do Ministério da Saúde.

O MINISTRO DE ESTADO DA SAÚDE, no uso da atribuição que lhe conferem os incisos I e II do parágrafo único do art. 87 da Constituição, e

Considerando a necessidade de estabelecer os direcionamentos e os valores adotados para a gestão de segurança da informação e comunicações no âmbito do Ministério da Saúde;

Considerando a importância que deve ser dada à garantia da integridade, à disponibilidade, à confidencialidade e à autenticidade dos dados e das informações nos mais diversos suportes utilizados por este Ministério;

Considerando as diretrizes do Governo Federal, representado pelo Gabinete de Segurança Institucional da Presidência da República, que recomenda a implantação, o no âmbito de cada órgão da Administração Pública Federal (APF), de processos e de metodologias de segurança da informação e comunicações;

Considerando o Decreto Nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

Considerando o 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;

Considerando a Lei Nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei Nº 2.848, de 7 de setembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

Considerando que segundo o art. 1.016 da Lei Nº 10.406, de 10 de janeiro de 2002 (Código Civil), os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;

Considerando o Decreto Nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

Considerando a Política Nacional de Informação e Informática em Saúde - Proposta versão 2.0 que inclui as deliberações de 12ª Conferência Nacional de Saúde, de 2003;

Considerando o acórdão do Tribunal de Contas da União Nº 461/2004, de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;

Considerando a Portaria Nº 66/SVS/MS, de 10 de dezembro de 2004, que dispõe sobre procedimentos e responsabilidades relativas à divulgação técnico-cientifica de dados e informações da Secretaria de Vigilância em Saúde;

Considerando a Norma NBR ISO/IEC 17799:2005 – Código de Práticas para a Gestão da Segurança da Informação;

Considerando a Instrução Normativa Nº 1, de 13 de junho de 2008, do Conselho de Defesa Nacional e da Secretaria-Executiva, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

Considerando a Portaria Nº 2.466/GM/MS, de 14 de outubro de 2009, que institui o Comitê de Informação e Informática em Saúde (CIINFO) no âmbito do Ministério da Saúde, resolve:

Art. 1º Instituir, no âmbito do Ministério da Saúde, a Política de Segurança da Informação e Comunicações do Ministério da Saúde (POSIC/MS), aprovada pelo CIINFO, e regida pelos objetivos e diretrizes estabelecidos nesta Portaria.

Parágrafo único. O Subcomitê de Segurança da Informação e Comunicações, sob orientação do CIINFO deverá disciplinar as seguintes matérias:

I - a criação e manutenção de contas e acesso aos recursos de Tecnologia da Informação e Comunicação (TIC);

II - o uso do correio eletrônico;

III - a segurança para usuários da rede;

IV - a classificação da informação do Ministério da Saúde;

V - a cessão de bases de dados nominais;

VI - o uso da Internet no Ministério da Saúde;

VII - o controle de acesso lógico e remoto;

VIII - a segurança da informação para técnicos;

IX - a segurança para estações de trabalho e equipamentos eletrônicos portáteis;

X - a segurança física de instalações;

XI - a instalação e configuração de aplicações;

XII - o tratamento de mídias e cópia de segurança;

XIII - a segurança para recursos de tecnologia da informação e comunicação;

XIV - a segurança contra código malicioso;

XV - a segurança para acordo de nível de serviço;

XVI - a conformidade legal;

XVII - a segurança em contratos de prestação de serviços;

XVIII - a segregação de função;

XIX - o registro de eventos e trilhas de auditoria;

XX - os procedimentos para custódia de equipamentos; e

XXI - o termo de responsabilidade.

Art. 2º Para efeitos desta Portaria, adotam-se as seguintes conceituações:

I - acesso: possibilidade de consulta ou reprodução de documentos e arquivos;

II - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função no Ministério da Saúde e equipara-se a quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida no âmbito do Ministério da Saúde;

III - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas [Security Officer - 1 guia oficial para formação de gestores em segurança da informação];

IV - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

V - ativo de informação: ativo que guarda informações do órgão;

VI - auditoria: atividade com a finalidade de reconstruir um evento relacionado à segurança para auxiliar no exame de suas causas e efeitos;

VII - autenticar: processo que busca verificar a identidade de uma pessoa no momento em que é requisitado um acesso a determinado ambiente ou recurso de tecnologia da informação;

VIII - cessão de bases de dados: ato de disponibilizar cópia, total ou parcial, de dados do Ministério da Saúde, aprovada pelo gestor competente;

IX - ciclo de vida da informação: compreende as fases de criação, manuseio, armazenamento, transporte e descarte da informação, considerando sua confidencialidade, integridade e disponibilidade;

X - classificação da informação: atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

XI - concedente: responsável pelo fornecimento da base de dados confidenciais pelo Ministério da Saúde;

XII - confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

XIII - conta de acesso: conjunto do "nome de usuário" e "senha" utilizado para acesso aos sistemas informatizados e recursos de TIC;

XIV - controles de segurança: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XV - custodiante: agente público responsável por zelar pelo armazenamento e pela preservação do ativo sob sua propriedade;

XVI - dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XVII - dados confidenciais: dados pessoais que permitam a identificação da pessoa e possam ser associados a outros dados referentes ao endereço, idade, raça, opiniões políticas e religiosas, crenças, ideologia, saúde física, saúde mental, vida sexual, registros policiais,

assuntos familiares, profissão e outros que a lei assim o definir, não podendo ser divulgados ou utilizados para finalidade distinta da que motivou a estruturação do banco de dados, salvo por ordem judicial ou com anuência expressa do titular ou de seu representante legal;

XVIII - dados pessoais: representação de fatos, juízos ou situações referentes a uma pessoa física ou jurídica, passível de ser captada, armazenada, processada ou transmitida por meios informatizados ou não;

XIX - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

XX - documento confidencial: contém informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado;

XXI - evento: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente conhecida que possa ser relevante para a segurança da informação (ISO/IEC TR 18044:2004);

XXII - gestor da informação: agente público do Ministério da Saúde responsável pela administração das informações geridas nos processos de trabalho sob sua responsabilidade;

XIII - grau de sigilo: gradação de segurança atribuída a dados e informações em decorrência de sua natureza ou conteúdo;

XXIV - incidente de segurança: todo e qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação ou de redes de computadores;

XXV - informação custodiada: informação sob a guarda e responsabilidade de alguém;

XXVI - integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

XXVII - logs: arquivos em computador utilizados para manter registros das atividades executadas por programas e usuários nos computadores e sistemas informatizados;

XXVIII - recursos de TIC: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XXIX - rede corporativa: conjunto de todas as redes locais sob a gestão do Ministério da Saúde;

XXX - rede local: conjunto de equipamentos interligados localmente com o objetivo de disponibilizar serviços aos usuários de rede do Ministério da Saúde;

XXXI - segurança da informação: preservação da confidencialidade, da integridade e da disponibilidade da informação e, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

XXXII - senha ou palavra-chave: é uma palavra ou uma ação secreta previamente convencionada entre duas partes como forma de reconhecimento, sendo senhas amplamente utilizadas em sistemas de computação para autenticar usuários e permitir-lhes o acesso a informações personalizadas armazenadas no sistema;

XXXIII - sigilo: segredo de conhecimento restrito a pessoas credenciadas; proteção contra revelação não autorizada;

XXXIV - software: programa de computador desenvolvido para executar um conjunto de ações previamente definidas;

XXXV - usuário da rede: qualquer indivíduo ou instituição que tenha acesso autenticado aos recursos da rede corporativa do Ministério da Saúde;

XXXVI - usuário de sistema: qualquer indivíduo ou instituição que tenha acesso autenticado aos sistemas disponibilizados pelo Ministério da Saúde; e

XXXVII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO I

DOS OBJETIVOS

Art. 3º Constituem objetivos da (POSIC/MS):

I - estabelecer suas diretrizes, a serem seguidas pelo Ministério da Saúde no que diz respeito à adoção de normas e procedimentos relacionados à segurança da informação e comunicações;

II - prover o Ministério da Saúde de normas para a segurança da informação, estabelecendo responsabilidades e diretrizes, bem como atitudes adequadas para manuseio, tratamento, controle e proteção contra a indisponibilidade, a divulgação, a modificação e o acesso não autorizados a dados e informações; e

III - definir um conjunto de instrumentos normativos e organizacionais que capacitem o Ministério da Saúde a assegurar a confidencialidade, a integridade e a disponibilidade dos dados e das informações.

CAPÍTULO II

DAS DIRETRIZES

Art. 4º Política de Informação e Comunicações do Ministério da Saúde (POSIC/MS) rege-se pelas seguintes diretrizes:

I - propriedade da informação:

a) toda informação criada, que for manuseada, armazenada, transportada ou descartada pelos agentes públicos do Ministério da Saúde, no exercício de suas atividades, é de propriedade do órgão e deve ser protegida segundo as diretrizes descritas na POSIC/MS e as regulamentações em vigor;

b) a informação custodiada, que for manuseada, armazenada, transportada ou descartada pelos agentes públicos do Ministério da Saúde, no exercício de suas atividades, deve ser protegida segundo as diretrizes descritas na POSIC/MS e nas demais regulamentações em vigor;

c) quando da obtenção de informação de terceiros, o Gestor da Informação deve providenciar junto ao concedente a documentação formal que atenda aos direitos de acesso antes de seu uso;

d) na cessão de bases de dados nominais custodiadas ou na informação de propriedade do Ministério da Saúde a terceiros, o Gestor da Informação deve providenciar a documentação formal relativa à autorização de acesso às informações

II - classificação da informação:

a) toda informação criada, manuseada, armazenada, transportada ou descartada do Ministério da Saúde deve ser classificada quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita, conforme o Decreto Nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

b) um processo de Classificação da Informação deve ser implementado e mantido, em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade do Ministério da Saúde ao longo do seu ciclo de vida;

c) toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada pelo Ministério da Saúde é de sua responsabilidade e deve ser protegida, adequadamente, conforme a classificação das informações;

d) a classificação da informação é atribuição do Gestor da Informação;

III - permissão de acesso:

a) todos os recurso de Tecnologia da Informação e Comunicação (TIC) sob responsabilidade do Ministério da Saúde deve ter um gestor formalmente designado por autoridade competente;

b) o agente público do Ministério da Saúde que utiliza os recursos de TIC deve ter uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em norma específica;

c) os privilégios de leitura, modificação ou eliminação das informações devem ser definidos pelo Gestor da Informação;

d) a autorização, o acesso, o uso da informação e dos recursos de TIC devem ser controlados e limitados ao cumprimento das atribuições de cada agente público do Ministério da Saúde e qualquer outra forma de uso necessita de prévia autorização formal pelo Gestor da Informação;

e) sempre que houver mudanças nas atribuições de determinado agente público do Ministério da Saúde será de responsabilidade da chefia imediata informar os seus privilégios de acesso às informações e aos recursos de TIC para que sejam adequados imediatamente;

f) no caso de exoneração ou demissão, esses privilégios devem ser cancelados;

IV - Gestão de Continuidade de Negócio:

a) deve ser estabelecida a Gestão de Continuidade de Negócio em segurança da informação e comunicações no âmbito do Ministério da Saúde visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de TIC que suportam as operações do Ministério da Saúde;

b) deve ser estabelecido um processo de gestão de risco com vistas a minimizar possíveis impactos associados aos ativos, processo esse que deve possibilitar a seleção e a priorização dos ativos a serem protegidos, bem como a definição e a implementação de controles para a identificação e o tratamento de possíveis falhas de segurança;

c) as medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança;

d) toda informação institucional, se eletrônica, deve ser armazenada nos servidores de arquivo da rede local e, se não eletrônica, deve ser mantida em local que a salvaguarde adequadamente;

e) no descarte de informações institucionais devem ser observados as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação;

f) os recursos de TIC disponibilizados para criação, manuseio, armazenamento, transporte e descarte da informação no Ministério da Saúde devem dispor de mecanismos que minimizem os riscos inerentes a problemas de segurança, a fim de evitar ocorrências de incidentes, de forma acidental ou intencional, que afetem os princípios da integridade, da disponibilidade e da confidencialidade das informações;

g) os recursos de TIC utilizados pelo Ministério da Saúde devem ser previamente homologados, identificados individualmente e inventariados, além de possuir documentação mínima e atualizada para o seu uso e estar em conformidade com as normas de segurança especificas;

V - monitoramento:

a) o uso dos recursos de TIC disponibilizados pelo Ministério da Saúde é passível de monitoramento e auditoria, conforme o previsto no item 9.1.4 do acórdão do Tribunal de Contas da União Nº 461 de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas, e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso; e

b) a entrada e a saída de ativos de informação nas dependências do Ministério da Saúde devem ser registradas e autorizadas por autoridade competente.

CAPÍTULO III

DA GESTÃO, DO GERENCIAMENTO E DA ABRANGÊNCIA

Art. 5º Compete ao CIINFO aprovar e revisar as diretrizes da POSIC/MS e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações do Ministério da Saúde.

Art. 6º Esta política aplica-se ao ambiente de trabalho e aos recursos de TIC, estabelecendo responsabilidades e obrigações a todos os agentes públicos do Ministério da Saúde que tenham acesso às informações ou aos recursos de TIC deste órgão.

Art. 7º As diretrizes de segurança da informação estabelecidas nesta Portaria aplicam-se às informações armazenadas, bem como às que estão sendo transmitidas e devem ser seguidas pelos agentes públicos do Ministério da Saúde, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Art. 8º A POSIC/MS deve ser difundida a todos os agentes públicos do Ministério da Saúde por um processo permanente de Conscientização em Segurança da Informação.

Art. 9º É dever do agente público do Ministério da Saúde conhecer e cumprir a Política de Segurança da Informação e Comunicações.

Art. 10. É condição para acesso aos ativos de informação do Ministério da Saúde a adesão formal aos termos desta Portaria.

Art. 11. O agente público do Ministério da Saúde é responsável pela segurança dos ativos de informação e processos que estejam sob a sua responsabilidade.

Art. 12. Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação devem receber capacitação especializada.

Art. 13. Os contratos firmados pelo Ministério da Saúde devem conter cláusulas que determinem a observância desta política e normas dela derivadas.

Art. 14. Os recursos de TIC disponibilizados pelo Ministério da Saúde devem ser utilizados estritamente dentro do seu propósito.

Parágrafo único. É vedado, a qualquer agente público do Ministério da Saúde, o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Ministério da Saúde ou para perpetrar ações que, de qualquer modo, venham a constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como àquelas que atentem contra a moral e a ética ou que prejudiquem o cidadão ou a imagem do órgão.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 15. Os agentes públicos do Ministério da Saúde devem reportar ao Departamento de Informática do SUS (DATASUS) os incidentes que afetam a segurança dos ativos ou o descumprimento da POSIC/MS.

Art. 16. Em casos de quebra de segurança da informação por meio de recursos de TIC, o DATASUS deverá ser imediatamente acionado para tomar as providências necessárias a fim de sanar as causas, podendo, inclusive, determinar a restrição temporária do acesso às informações ou ao uso dos recursos de TIC do Ministério da Saúde.

Art. 17. A utilização da POSIC/MS é recomendada aos órgãos vinculados ao Ministério da Saúde.

Art. 18. A violação das normas de segurança da informação resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas administrativas sem prejuízo das demais medidas cíveis e penais cabíveis.

Art. 19. Os casos omissos serão resolvidos pelo Comitê de Informação e Informática em Saúde (CIINFO/MS).

Art. 20. O Subcomitê de Segurança da Informação e Comunicações, sob orientação do CIINFO, deverá revisar, sempre que necessário, a POSIC/MS e todos os atos normativos dela decorrentes, não excedendo o período máximo de 1 (um) ano.

Art. 21. O Ministro de Estado da Saúde providenciará a edição dos atos que integram a POSIC/MS, nos termos do parágrafo único do artigo 1º, no prazo de 180 (cento e oitenta) dias, a partir da publicação desta Portaria.

Art. 22. Esta Portaria entra em vigor na data de sua publicação.

Art. 23. Ficam revogadas as Portarias DATASUS/MS nºs 207, de 9 de julho de 2008, publicada no Diário Oficial da União nº 137, de 18 de julho de 2008, Seção I, página 50.

JOSÉ GOMES TEMPORÃO