Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 21 - DOU de 30/01/17 - Seção 1 - p.83

MINISTÉRIO DA SAÚDE
GABINETE DO MINISTRO

PORTARIA Nº 271, DE 27 DE JANEIRO DE 2017

Dispõe sobre a Política de Segurança da Informação e Comunicações do Ministério da Saúde (POSIC/MS).

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 as diretrizes do Governo Federal, representado pelo Gabinete de Segurança Institucional da Presidência da República, que recomenda a implantação, no âmbito de cada órgão da Administração Pública Federal (APF), de processos e de metodologias de segurança da informação e comunicações, conforme preconiza a Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008;
Considerando o advento da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI), que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;
Considerando as boas práticas em segurança preconizadas pelas normas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011, 27004:2010, 27005:2011 e 27014:2013;
Considerando que a norma ABNT NBR ISO/IEC 27002:2013 recomenda revisões periódicas da política de segurança da informação das instituições;
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 pelo Ministério da Saúde; e
Considerando o Acórdão nº 1.233 - TCU/2012, que trata da adoção dos normativos de Segurança da Informação e Comunicações (SIC), não facultativos, mas obrigação da alta administração, e o Acórdão nº 3.051-TCU/2014, que prevê a estratégia geral de Segurança da Informação, resolve:

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

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A POSIC/MS institui diretrizes, responsabilidades e competências que visam viabilizar a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações no MS.
Parágrafo único - Agentes Públicos que tenham acesso a informações do MS sujeitam-se às diretrizes e objetivos de segurança da informação da Política de que trata esta Portaria, e são responsáveis por garantir a segurança das informações a que tenham acesso.

CAPÍTULO II
DOS OBJETIVOS

Art. 3º Constituem objetivos da POSIC/MS:
I - estabelecer diretrizes, a serem seguidas pelo MS no que diz respeito à adoção de normas e procedimentos relacionados à segurança da informação e comunicações;
II - prover o MS 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 autorizado a dados e informações; e
III - definir um conjunto de instrumentos normativos e organizacionais que capacitem o MS a assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e das informações.

CAPÍTULO III
DA ABRANGÊNCIA

Art. 4º Esta Política aplica-se aos recursos de Tecnologia da Informação e Comunicações (TIC), ambientes e processos de trabalho, estabelecendo responsabilidades e obrigações a todos os agentes públicos do MS que tenham acesso às informações ou aos recursos de TIC deste órgão.

CAPÍTULO IV
CONCEITOS E DEFINIÇÕES
Art. 5º Para fins desta Portaria entende-se por:
I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do órgão;
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 pública e equipara-se a agente público quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida no Ministério da Saúde;
III - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
IV - ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;
V - ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
VI - CIINFO: Comitê de Informação e Informática em Saúde;
VII - Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito deste órgão;
VIII - criticidade: grau de importância da informação;
IX - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;
X - Gestor de Área: responsável pela área funcional onde a informação é criada, comunicada, manuseada, armazenada, custodiada, transportadas ou descartadas;
XI - Gestor de Segurança da Informação e Comunicações: servidor responsável pelas ações de segurança da informação e comunicações no âmbito deste órgão;
XII - incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, de computação ou das redes de computadores;
XIII - informação: é um ativo essencial para os negócios de uma organização e, por conseqüência, necessita ser adequadamente gerenciada e protegida independentemente de seu formato e meio;
XIV - Política de Segurança da Informação e Comunicações (POSIC): documento com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações neste órgão;
XV - Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações neste órgão;
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;
XVII - SGSIC: Subcomitê Gestor de Segurança da Informação e Comunicações;
XVIII - Termo de Responsabilidade: Termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso; e
XIX - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO V
REFERÊNCIAS LEGAIS E NORMATIVAS
Art. 6º As ações de Segurança da Informação e Comunicações do Ministério da Saúde deverão observar os seguintes requisitos legais e normativos:
I - 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;
II - 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;
III - 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;
IV - Art. 1.016 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), que dispõe que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;
V - Portaria nº 589, de 20 de maio de 2015, que Institui a Política Nacional de Informação e Informática em Saúde (PNIIS);
VI - Instrução Normativa nº 01, de 13 de junho de 2008, do Conselho de Defesa Nacional e suas respectivas Normas Complementares publicadas no Diário Oficial da União (DOU) pelo Departamento de Segurança da Informação e

Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR), que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;
VII - Portaria nº 2072, de 31 de agosto de 2011, que redefine o Comitê de Informação e Informática em Saúde (CIINFO) no âmbito do Ministério da Saúde;
VIII - Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações;
IX - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011;
X - Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento; XI - Norma NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação; e
XII - ISO 31.000:2009 - Diretrizes para a implementação da gestão de riscos.

CAPÍTULO VI
PRINCÍPIOS
Art. 7º As ações relacionadas com a Segurança da Informação e Comunicações no MS são norteadas pelos seguintes princípios:
I - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
II - celeridade: as ações de segurança da informação oferecem respostas rápidas a incidentes e falhas;
III - clareza: as regras de segurança dos ativos de segurança da informação e comunicações são precisas, concisas e de fácil entendimento;
IV - confidencialidade: as informações somente estarão disponíveis ou reveladas à pessoa, sistema, órgão ou entidade autorizada e credenciada;
V - disponibilidade: as informações estarão disponíveis e utilizável a quem dela necessita e possua autorização para acessála;
VI - equanimidade: as normas e regras de segurança da informação são obedecidas por todos, sem distinção de cargo ou função;
VII - ética: os direitos dos agentes públicos são preservados sem comprometimento da segurança da informação e comunicações;
VIII - finalidade: as normas e regras de segurança da informação consideram a finalidade dos ativos e das informações a que se referirem;
IX - integridade: as informações não são modificadas ou destruídas de maneira não autorizada ou acidental;
X - menor privilégio: restringir o acesso às informações, ao estritamente necessário ao exercício das funções;
XI - privacidade: informação que fira o respeito, à intimidade, à integridade e a honra dos cidadãos não podem ser divulgadas;
XII - publicidade: dar transparência no trato das informações, observado os critérios legais. Divulgar a todos os agentes públicos do MS as diretrizes e a normas de segurança da informação;
e
XIII - responsabilidade/obediência: os agentes públicos têm o dever de conhecer e respeitar todas as normas de segurança da informação e comunicações do MS.

CAPÍTULO VII
DIRETRIZES GERAIS
Art. 8º É dever do agente público do MS conhecer e cumprir a POSIC/MS.

Art. 9º É condição para acesso aos ativos de informação do MS a adesão formal aos termos desta Portaria, mediante assinatura de Termo de Responsabilidade.

Art. 10 Todos os agentes públicos do MS são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: identificação de usuário da rede (Login), crachá, carimbo, endereço de correio eletrônico ou assinatura digital.

Art. 11 Os recursos de TIC disponibilizados pelo MS devem ser utilizados estritamente dentro do seu propósito.

Art. 12 Os contratos de prestação de serviços, firmados pelo MS conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, devendo ainda, exigir da entidade contratada, a assinatura de Termo de Confidencialidade.

CAPÍTULO VIII
DIRETRIZES ESPECÍFICAS
Art. 13 Esta política aplica-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicaçãoe armazenamento da informação e rege-se pelas eguintes diretrizes:

I - Propriedade da Informação:
a) toda informação criada, armazenada, transportada ou descartada pelos agentes públicos do MS, no exercício de suas atividades, é de propriedade do órgão e é protegida segundo as diretrizes descritas na POSIC/MS e nas regulamentações em vigor;
b) na cessão de bases de dados nominais, informação custodiada ou de propriedade do MS a terceiros, o Gestor da Informação providenciará a documentação formal relativa à cessão ou autorização de acesso às informações antes da sua disponibilização; e
c) nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deverá, se necessário, providenciar junto à concedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.
II - Tratamento da Informação: a) toda informação criada, manuseada, armazenada, transportada,
descartada ou custodiada pelo MS é de sua responsabilidade e são classificadas e protegidas adequadamente, quanto aos aspectos de confidencialidade, integridade, autenticidade e disponibilidade, de forma explícita ou implícita conforme o Decreto nº 7.845, de 14 de novembro de 2012;
b) a classificação da informação é atribuição do Gestor da Informação;
c) toda informação institucional, se eletrônica, estará armazenada nos servidores de arquivo e bases de dados sob gestão e administração da área de TIC e, se não eletrônica, mantida em local que a salvaguarde adequadamente;
d) toda informação institucional, sob a forma eletrônica, estará salvaguardada por meio de cópia de segurança sob administração da área de TIC e mantida em local que a proteja adequadamente e garanta sua recuperação em caso de perda da informação original;
e) no descarte de informações institucionais são observadas as políticas, as normas, os procedimentos internos, a classificação que a informação possui, bem como a temporalidade prevista na legislação;
e
f) as informações classificadas conforme a legislação vigente,
produzida, armazenada e transportada em meios eletrônicos,
utilizará criptografia compatível com o grau de sigilo, em especial as
informações de autenticação dos usuários das aplicações.
III - Tratamento de Incidentes em Rede:
a) cabe ao DATASUS a responsabilidade pela infraestrutura
necessária para fins de registro e resposta aos incidentes de segurança
da informação no âmbito da rede corporativa do MS;
b) a Equipe de Tratamento de Incidentes de Rede (ETIR)
será instituída no Departamento de Informática do SUS (DATASUS); e
c) todo agente público do MS é responsável por notificar, imediatamente, incidentes que afetem a segurança da informação por meio de recursos de TIC ou o descumprimento da POSIC/MS à ETIR, para que as providências necessárias sejam adotadas a fim de sanar as causas.
IV - Gestão de Risco:
a) fica estabelecido o Processo de Gestão de Riscos de Segurança da Informação e Comunicações (PGRSIC), com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações; e
b) o PGRSIC baseia-se nas melhores práticas, na Norma ISSO 31.000:2009 - Diretrizes para a implementação da gestão de riscos e na Norma Complementar nº 04/IN01/DSIC/GSI/PR.
V - Gestão de Continuidade:
a) fica estabelecido o Programa de Gestão de Continuidade de Negócio (PGCN) em segurança da informação e comunicações no âmbito do MS, visando reduzir a possibilidade de interrupção causada por desastres ou falhas nos recursos de TIC que suportam as operações do MS; e
b) todo sistema ou serviço crítico do MS deverá estar suportado pelo PGCN. VI - Auditoria e Conformidade:
a) o uso dos recursos de TIC disponibilizados pelo MS 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 serão implementados e mantidos, sempre que possível, mecanismos que permitam a rastreabilidade desse uso; e
b) serão mantidos procedimentos, tais como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para todos os sistemas corporativos e rede interna do MS.
VII - Controles de Acesso:
a) o agente público do MS que utilizar os recursos de TIC terá uma conta de acesso, única e intransferível, cuja concessão de acesso será regulamentada em norma específica;
b) o gestor da informação é responsável pela concessão e revogação dos privilégios de acesso às informações, considerando sempre o princípio do menor privilégio; e
c) a identificação do agente público, qualquer que seja o meio e a forma, é pessoal e intransferível, e permite o reconhecimento de maneira inequívoca.
VIII - Uso de E-mail:

a) o correio eletrônico do MS tem seu uso exclusivo por agentes públicos no exercício de suas funções. As regras de acesso e utilização são definidas por norma específica, em conformidade com esta POSIC/MS e demais orientações e diretrizes de governo.
IX - Acesso à Internet:
a) o acesso à Internet no ambiente de trabalho do MS está condicionado às necessidades dos agentes públicos no exercício de suas atribuições e será regido por norma específica, em conformidade com esta POSIC/MS e demais orientações governamentais e legislação em vigor.
X - Gestão de Mudança:
a) toda mudança no ambiente, que tenha sido homologada e testada, necessita ser documentada e registrada; e
b) todo processo de gestão de mudanças é composto, no mínimo, pelas fases de Descrição, Avaliação, Aprovação, Implementação e Verificação, de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.
XI - Gestão de Ativos de Informação: a) o MS manterá um processo de Inventário e Mapeamento dos Ativos de Informação objetivando a Segurança das Infraestruturas Críticas que garantem suas Informações; e
b) o processo de Inventário e Mapeamento de Ativos de Informação subsidiará o conhecimento, valoração, proteção e a manutenção de seus ativos de informação, será dinâmico, periódico, e estruturado, para manter a Base de Dados de Ativos de Informação atualizada.
XII - Dispositivos Móveis:
a) o uso dos dispositivos móveis portáteis pelos agentes públicos usuários da rede do MS deverá ser realizado no interesse do órgão;
b) todo dispositivo móvel usado para acessar a rede coorporativa do MS estará submetido aos padrões estabelecidos pelo DATASUS; e
c) O DATASUS proverá uma rede segregada da rede coorporativa para acesso à Internet pelos visitantes.
XIII - Computação em Nuvem:
a) o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SIC, estabelecidas pelo MS, e às legislações vigentes;
b) o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço; e
c) o armazenamento de informação em nuvem deverá estar respaldado por um contrato entre o MS e o provedor de serviço em nuvem, de modo a garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem.
XIV - Redes Sociais:
a) o uso institucional das redes sociais nos aspectos relacionados à Segurança da Informação e Comunicações deverá ser objeto de Norma Interna que, além da SIC, abordará a estratégia de comunicação social, o processo de gestão de conteúdo e outros aspectos relevantes;
b) a normatização interna de uso seguro das redes sociais deverá estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais por usuários que tenham permissão para administrar perfis institucionais ou que possuam credencial de acesso para qualquer rede social a partir da infraestrutura das redes de computadores do MS;
c) perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por servidor, ou estar sob a coordenação e responsabilidade deste; e
d) o MS nomeará um servidor público, ocupante de cargo efetivo, para a função de Agente Responsável pela gestão do uso seguro de cada perfil institucional nas redes sociais.
XV - Desenvolvimento de Software Seguro - DSS: a) deverão ser identificados os responsáveis pela definição e validação dos requisitos de segurança que o software deva atender;
b) deverão ser definidos os requisitos de segurança para aplicação logo no início de qualquer projeto de desenvolvimento ou aquisição de software;
c) deverá ser definida a execução de testes pela contratada e homologação pelo MS antes da instalação do software em ambiente de produção;
d) deverá ser realizado teste de mesa do software desenvolvido por terceiros;
e) fica estabelecida a obrigatoriedade do gerenciamento de monitoração da performance de aplicação ponto a ponto (Análise Dinâmica), antes da implantação de qualquer software ou aplicação, não sendo permitido que passe a operar enquanto perdurar qualquer falha de segurança considerada crítica; e
f) o tratamento das vulnerabilidades constitui um dos requisitos para a aceitação do sistema.
XVI - Preservação de Evidencias:
a) os equipamentos servidores de rede, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (Logs) em formato que permita a completa identificação dos fluxos de dados e das operações de seus administradores;
b) os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos; e

c) os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio de tecnologia aplicável.

CAPITULO IX
COMPETÊNCIAS E RESPONSABILIDADES
Art. 14 Compete ao DATASUS a Gestão da Segurança da Informação e Comunicações eletrônicas.

Art. 15 Compete ao CIINFO a aprovação das diretrizes da POSIC/MS e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações do MS.

Art. 16 O MS nomeará um servidor público que atuará como Gestor de Segurança da Informação e Comunicações (GSIC), com as seguintes competências:
I - promover cultura de segurança da informação e comunicações;
II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III - propor recursos necessários às ações de segurança da informação e comunicações;
IV - coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
VI - manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações; e
VII - propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF.
Art. 17 O Subcomitê Gestor de Segurança da Informação e Comunicações (SGSIC) é constituído por 1 (um) representante, titular e um suplente, das secretarias do MS.
§ 1º O SGSIC terá as seguintes competências:
I - Assessorar na implementação das ações de segurança da informação e comunicações no MS;
II - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
III - Propor normas e procedimentos relativos à segurança da informação e comunicações no âmbito do MS; e
IV - Revisar e analisar periodicamente esta política e as diretrizes e normas dela decorrentes visando a sua aderência e concordância aos objetivos institucionais deste Ministério e às legislações vigentes.
§ 2º Poderão fazer parte deste Subcomitê, como convidados, os órgãos vinculados ao MS.

CAPITULO X
DIVULGAÇÃO E CAPACITAÇÃO
Art. 18 O MS deverá promover ações permanentes de conscientização dos agentes públicos visando à disseminação das diretrizes e normas estabelecidas nesta política.

Art. 19 A POSIC e as normas deverão ser divulgadas no boletim interno do MS e disponíveis na Intranet para todos os agentes públicos.

Art. 20 Todo agente público que acessa a rede corporativa do MS deverá realizar a capacitação básica em Segurança da Informação disponibilizada em ambiente EAD (ensino a distância).
Parágrafo único: Os gestores responsáveis pelos processos inerentes à gestão da segurança da informação devem receber capacitação especializada.

CAPITULO XI
ATUALIZAÇÃO
Art. 21 Esta POSIC/MS e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 2 (dois) anos.

CAPITULO XII
PENALIDADES
Art. 22 O desrespeito, descumprimento ou violação de um ou mais itens constantes nesta POSIC/MS caracteriza infração funcional e 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 administrativas, cíveis e penais cabíveis.

CAPÍTULO XIII
DAS DISPOSIÇÕES FINAIS
Art. 23 Os casos omissos serão resolvidos pelo Comitê de Informação e Informática em Saúde (CIINFO/MS).

Art. 24 O Subcomitê Gestor de Segurança da Informação e Comunicações, em obediência às diretrizes gerais do CIINFO/MS, providenciará propostas de normativos para integrar a POSIC/MS, nos termos do artigo 3º, a partir de sua publicação.

CAPITULO XIV
VIGÊNCIA
Art. 25 Esta Portaria entra em vigor na data de sua publicação.

Art. 26 Fica revogada a Portaria nº 3.207/GM/MS, de 20 de outubro de 2010, publicada no Diário Oficial da União nº 202, de 21 de outubro de 2010, Seção 1, página 52.
RICARDO BARROS