DIÁRIO OFICIAL DA UNIÃO

Publicado em: 18/07/2018 | Edição: 137 | Seção: 1 | Página: 34

Órgão: Ministério da Saúde/Gabinete do Ministro

PORTARIA Nº 1.966, DE 17 DE JULHO DE 2018

Define Normas de Segurança da Informação e Comunicações no âmbito do Ministério da Saúde.

O MINISTRO DE ESTADO DA SAÚDE, SUBSTITUTO, no uso da atribuição que lhe confere o inciso 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 as determinações do Tribunal de Contas da União, expostas no Acórdão nº 2772/2015 - TCU - Plenário;

Considerando a Instrução Normativa n˚ 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; e

Considerando a Portaria nº 271/GM/MS, de 27 de janeiro de 2017, que dispõe sobre a Política de Segurança da Informação e Comunicações do Ministério da Saúde - POSIC/MS, resolve:

Art. 1º Esta Portaria define Normas de Segurança da Informação e Comunicações no âmbito do Ministério da Saúde, conforme Anexos I a VII a esta Portaria, a seguir elencadas:

I - constituição de Equipe de Tratamento e Respostas a Incidentes na Rede Computacional do Ministério da Saúde - ETIR-MS;

II - controle de Acesso;

III - cópias de Salvaguarda;

IV - gerenciamento de Mudanças;

V - inventário e Mapeamento de Ativos de Informação - Gestão de Ativos;

VI - gestão de Riscos de Segurança da Informação e Comunicações; e

VII - uso de Dispositivos Móveis.

Parágrafo Único. O disposto nesta Portaria deverá observar as demais regras definidas na Portaria nº 271/GM/MS, de 27 de janeiro de 2017, que dispõe sobre a Política de Segurança da Informação e Comunicações do Ministério da Saúde - POSIC/MS.

Art. 2º A definição de aspectos técnicos e procedimentais necessários para execução desta portaria será realizada pelas autoridades do Ministério da Saúde, no âmbito de suas competências.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

ADEILSON LOUREIRO CAVALCANTE

ANEXO I

CONSTITUIÇÃO DE EQUIPE DE TRATAMENTO E RESPOSTAS A INCIDENTES NA REDE COMPUTACIONAL DO MINISTÉRIO DA SAÚDE - ETIR-MS

CAPITULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Anexo trata da constituição de Equipe de Tratamento e Resposta a Incidentes na Rede Computacional do Ministério da Saúde - ETIR-MS.

Parágrafo Único. O disposto neste Anexo deverá observar às demais regras definidas na Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, que trata da criação de equipes de tratamento e resposta a incidentes em redes computacionais - ETIR.

Art. 2º Para fins deste Anexo, consideram-se as seguintes definições:

I - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

II - gestor de segurança da informação e comunicações: responsável pelas ações de Segurança da Informação e Comunicações - SIC no âmbito do órgão ou entidade da APF;

III - agente Responsável pela ETIR: servidor público ocupante de cargo efetivo de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a ETIR;

IV - ativo de informação: os meios de armazenamento, transmissão e processamento da informação, bem como os equipamentos, sistemas, locais e recursos humanos relacionados a essas atividades;

V - comunidade ou público alvo: o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

VI - Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR GOV: órgão subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República - GSI, competente para o atendimento aos incidentes em redes de computadores da APF;

VII - gestor do ativo de informação: parte interessada, setor do MS, indivíduo legalmente instituído por sua posição ou cargo, responsável primário pela viabilidade, sobrevivência e administração do ativo de informação;

VIII - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

IX - rede computacional: rede formada por conjunto de computadores e outros dispositivos tecnológicos, interligados entre si por sistema de comunicação, capaz de trocar informações e partilhar recursos físicos e lógicos;

X - serviço: conjunto de procedimentos, estruturados em um processo bem definido, oferecido a outras Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais da APF;

XI - segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;

XII - tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar, classificar e responder as solicitações e alertas e realizar as análises dos incidentes de segurança, extraindo informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências; e

XIII - vulnerabilidade: qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

Art. 3º A ETIR-MS será formada a partir dos membros das equipes de TI do Ministério da Saúde, que, além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança em redes computacionais, conforme modelo descrito no item 7.1 da Norma Complementar 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009.

CAPITULO II

DAS ATRIBUIÇÕES E COMPETÊNCIAS

Art. 4º O Gestor de Segurança da Informação e Comunicações do Ministério da Saúde será o Agente Responsável pela ETIR.

Parágrafo único. O Agente de que trata o caput e seu substituto serão servidores efetivos de carreira, formalmente nomeados para essa função.

Art. 5º Compete ao Gestor de Segurança da Informação e Comunicações do Ministério da Saúde:

I - planejar, coordenar e orientar as atividades de monitoramento, recebimento de alertas, análise, classificação e notificação de incidentes de segurança;

II - propor a implementação da infraestrutura necessária para o funcionamento da ETIR;

III - adotar providências necessárias para a capacitação e o aperfeiçoamento técnico dos membros da ETIR;

IV - garantir que os incidentes de segurança na rede computacional do Ministério da Saúde sejam registrados e analisados;

V - informar às autoridades competentes os assuntos relacionados a incidentes de segurança de redes computacionais;

VI - articular, quando necessário, com autoridades policiais e judiciárias, outros CTIR e outras ETIR, para troca de informações e experiências, com o objetivo de antecipar tendências ou padrões de ataques em massa;

VII - informar ao Centro de Tratamento de Incidentes de Redes do Governo - CTIR Gov a ocorrência e as estatísticas de incidentes de segurança, para manutenção e atualização da base de dados do governo federal; e

VIII - disseminar, no âmbito do Ministério da Saúde, alertas de vulnerabilidades, informativos sobre novas atualizações e incidentes de segurança tratados ou qualquer assunto relacionado à segurança da rede de computadores.

Parágrafo único. A gestão da ETIR será instituída no Núcleo de Segurança da Informação e Comunicações - NSIC/CGGP/DATASUS/SE/MS.

Art. 6º Compete aos membros técnicos da ETIR:

I - monitorar, receber e registrar eventos, elaborar relatórios de incidentes de segurança e alertas;

II - categorizar, priorizar e atribuir eventos e incidentes de segurança;

III - analisar os impactos, ameaças ou danos ocorridos, definindo a reparação e os passos de mitigação a serem seguidos; e

IV - prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicação.

§ 1º Os membros técnicos da ETIR serão indicados pela Coordenação-Geral de Infraestrutura - CGIE/DATASUS/SE/MS e pela Coordenação-Geral de Análise e Manutenção - CGAM/DATASUS/SE/MS.

§ 2º A indicação de que trata o § 1º deverá considerar o perfil profissional adequado às funções elencadas no caput.

Art. 7º Cabe à ETIR monitorar, receber alertas, analisar, classificar e notificar qualquer incidente de segurança, mediante a realização das seguintes atividades:

I - monitoramento de alertas: o monitoramento de incidentes de segurança como parte do processo de reconhecimento de padrões e tendências de atividades maliciosas, que possibilita a produção de informações e conhecimentos que qualificam as respostas a esses incidentes com o objetivo de identificar atividades maliciosas dentre os eventos de segurança e encaminhá-los para tratamento;

II - acompanhamento de alertas: acompanhar os alertas de incidentes de segurança na rede computacional, encaminhá-los para tratamento, registrar as condutas adotadas, identificar tendências e padrões de atividades maliciosas e coletar indicadores estatísticos, com o objetivo de criar base de conhecimento sobre os incidentes de segurança com banco de informações sobre incidentes de segurança na rede do Ministério da Saúde e respectivos tratamentos;

III - registro de incidentes: registro das informações sobre os incidentes de segurança, suas características, danos causados e medidas corretivas e preventivas;

IV - descrição das funções e procedimento do serviço: realização de coleta e registro de informações que permite identificação do escopo do incidente de segurança, sua abrangência, natureza, impactos causados e tratamento adotado;

V - análise e tratamento de incidentes de segurança definição: análise das informações disponíveis sobre os incidentes e indicação dos tratamentos a serem adotados com o objetivo de produzir informações e conhecimentos sobre os incidentes de segurança registrados e adotar as medidas corretivas adequadas;

VI - descrição das funções e procedimento do serviço: análise de todas as informações disponíveis sobre um incidente de segurança, incluindo artefatos, evidências, logs relacionados, sua extensão, natureza e quais os impactos causados, apresentando aos Gestores das áreas envolvidas as informações levantadas referentes ao incidente e as soluções propostas para o tratamento;

VII - comunicação sobre incidentes de segurança: comunicar incidentes de segurança aos órgãos competentes para fins estatísticos, geração de soluções integradas e investigação com objetivo de manter canal de comunicação sobre incidentes de segurança com órgãos competentes;

VIII - comunicação aos órgãos externos competentes: levantar informações sobre incidentes de segurança e comunicar aos órgãos competentes, tais como, CTIR.Gov e autoridades policiais;

IX - disseminação de informações: divulgar, no âmbito do Ministério da Saúde, informações sobre ameaças à rede e respectivas soluções de contenção e prevenção, novas atualizações dos softwares instalados e informações relativas a ataques identificados, com o objetivo de disponibilizar canal com base de conhecimento para tratamento de incidentes de segurança em rede computacional; e

X - a pesquisa de informações sobre ameaças às redes computacionais, soluções de contenção e prevenção, novas atualizações dos softwares instalados na rede e a disseminação de informações relativas a ataques, tendências e medidas preventivas.

CAPITULO III

DA NOTIFICAÇÃO DE INCIDENTES DE SEGURANÇA

Art. 8º A ETIR deve ser notificada sempre que ocorrer a confirmação de um incidente de segurança na rede corporativa de computadores e sistemas do Ministério da Saúde.

Parágrafo único. A notificação dos incidentes de segurança na rede de computadores deve ser feita pelos seguintes meios:

I - central de suporte e atendimento ao usuário: Help Desk, ramal 2222;

II - Ouvidoria Geral do SUS: Disque Saúde 136;

III - e-mail: "abuse@saude.gov.br" e "suporte.rede@saude.gov.br";

IV - correspondências oficiais: memorandos e ofícios; e

V - outros meios tecnológicos, nos casos de eventos detectados pelo monitoramento das áreas de atendimento a usuários e da própria ETIR.

Art. 9º Todo incidente será registrado em software específico, por membro da equipe da ETIR.

Parágrafo único. Membro da equipe da ETIR procederá à consolidação das informações e notificação ao agente responsável da ETIR.

Art. 10. A ETIR terá acesso aos arquivos de registros de atividades (logs), além de evidências coletadas por outras equipes, de forma a realizar a análise e encaminhamento de investigação do incidente de segurança.

Art. 11. Em casos de incidentes e suas recorrências, identificados pelo serviço de monitoramento de incidentes, a ETIR encaminhará as análises das ocorrências aos responsáveis pelas áreas afetadas juntamente com uma proposta de tratamento adequado.

Parágrafo único. Serão informados os impactos que poderão advir caso as recomendações da ETIR não sejam seguidas.

Art. 12. Em conformidade com o item 9.3.2 da Norma Complementar 05/IN01/DSIC/GSIPR, a ETIR não terá autonomia para decidir ou agir no tratamento de incidentes nos termos do escopo de atuação e nível de responsabilidade definidos neste Anexo, no entanto, poderá recomendar procedimentos e medidas preventivas a serem executadas ou ações de contenção e recuperação, baseadas em evidências ou boas práticas.

CAPITULO IV

DAS DISPOSIÇÕES FINAIS

Art. 13. Todas as ações realizadas pela ETIR devem ser documentadas e arquivadas para o acesso de gestores e técnicos envolvidos na investigação e tratamento de incidentes de segurança.

Art. 14. A ETIR-MS manterá contato permanente com o Centro de Tratamento de Incidentes de Redes do Governo - CTIR Gov, para notificação dos incidentes de segurança.

ANEXO II

CONTROLE DE ACESSO AOS ATIVOS DE TI NO ÂMBITO DO MINISTÉRIO DA SAÚDE

CAPITULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Anexo estabelece diretrizes e orientações para o controle de acesso aos ativos de informação.

Parágrafo único. As ações deste Anexo deverão observar as demais regras definidas na:

I - Lei nº 12.527, de 18 de novembro de 2011 - Lei de acesso à Informação;

II - Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 15 de julho de 2014, que define Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF; e

III - ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da Informação.

Art. 2º Para fins deste Anexo, consideram-se as seguintes definições:

I - acesso: possibilidade de comunicar-se com um dispositivo, meio de armazenamento, unidade de rede, memória, registro, arquivo ou ambientes físicos, visando receber ou fornecer dados;

II - ativo 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;

III - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

IV - credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer;

V - custodiante: pessoa ou unidade organizacional responsável pela guarda e transporte de ativos de informação e manutenção das medidas de proteção estabelecidas;

VI - logs: termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional;

VII - perfil de acesso: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

VIII - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

IX - rede corporativa: rede de computadores pertencente a uma empresa ou instituição;

X - smart cards: cartão contendo um chip responsável pela geração e o armazenamento de certificados digitais;

XI - 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

XII - tokens: pequenos dispositivos que podem ser conectados ao computador para autenticar o usuário, gerando uma senha aleatória.

CAPITULO II

DAS DIRETRIZES GERAIS

Art. 3º O acesso lógico e físico às informações, aos recursos de processamento das informações e aos processos de negócios devem ser controlados de forma a considerar:

I - o grau de sigilo;

II - a criticidade dos ativos de informação; e

III - a segurança da informação no âmbito do Ministério da Saúde.

Art. 4º A classificação dos ativos de informação em níveis de criticidade deve considerar:

I - o tipo de ativo;

II - o impacto em caso de quebra de segurança;

III - a gestão de risco; e

IV - a continuidade de negócio.

Art. 5º O acesso aos ativos de informação pelo uso da credencial recebida deve ser precedido da assinatura do Termo de Responsabilidade, conforme Anexo-A.

Parágrafo único. O acesso aos ativos de informação que não estejam classificados como de acesso público deve obrigatoriamente ser precedido de credenciamento.

Art. 6º A implementação do controle de acesso ocorrerá em diferentes níveis, conforme definido pelo gestor da informação.

§ 1º É atribuição do gestor do ativo de informação a concessão de direitos de acesso e a determinação da necessidade de níveis de acesso adicionais.

§ 2º A concessão de direitos de acesso está condicionada à necessidade das atividades do usuário.

CAPITULO III

DO CONTROLE DE ACESSO LÓGICO

Art. 7º O controle de acesso lógico é definido como o procedimento para controlar a concessão e o uso de privilégios especiais de acesso à rede corporativa.

§ 1º O Controle de acesso lógico deve ser implementado conforme definições da Norma de Criação e Manutenção de Contas e Acesso aos Recursos de TIC, descritas nos itens 6.2 e 6.6 do Anexo da Portaria GM/MS nº 85, de 31 de janeiro de 2012.

§ 2º As técnicas de autenticação que permitam validar a identidade do usuário da rede, tais como biometria, tokens e smartcards, devem ser implementadas sempre que se verificar a necessidade, mediante avaliação prévia do Núcleo de Gestão de Segurança da Informação e Comunicações do Ministério da Saúde.

Art. 8º Todo o acesso lógico deverá ser registrado, por meio da gravação em logs, para posterior auditoria e rastreamento.

Parágrafo único. O registro de que trata o caput:

I - conterá, no mínimo, data, hora, serviço utilizado, usuário e informações específicas que facilitem o rastreamento da ação tomada.

II - possuirá mecanismos para garantir a sua integridade; e

III - deverá ser armazenado pelo período mínimo de 1 ano.

Art. 9º As concessões de acesso às informações sigilosas deverão:

I - estar em conformidade com a legislação especifica vigente;

II - utilizar o acesso no âmbito da rede corporativa; e

III - ser providas por meio de canal criptografado, preferencialmente utilizando as recomendações impostas pela ICP-Brasil e protocolos de segurança como SSL/TLS ou IPSEC, para proteger os dados confidenciais durante a transmissão em redes sem fio e públicas.

Art. 10. O acesso à Internet nas dependências do Ministério da Saúde, por visitantes, deverá ser realizado em rede segregada e específica, condicionado a cadastro prévio.

CAPITULO IV

DO ACESSO REMOTO

Art. 11. A permissão para se realizar acesso remoto à rede corporativa deve ser solicitada à área de administração da rede, Coordenação ou área superior à que o usuário da rede está subordinado, com definição do prazo de validade e horários para realizar o acesso.

Parágrafo único. O acesso remoto à rede corporativa deve ter privilégios diferenciados do perfil de acesso local, com serviços explicitamente controlados.

CAPITULO V

DO CONTROLE DE ACESSO FÍSICO

Art. 12. Compete à Subsecretaria de Assuntos Administrativos - SAA/SE/MS atuar no controle de acesso físico, por meio de:

I - estabelecimento de regras para o uso de credenciais físicas, tais como crachá, bóton e cartões; e

II - prestação de orientações sobre o uso de barreiras físicas e mecanismos de controle, quanto ao controle de acesso dos usuários às áreas e instalações; e

III - classificação das áreas e instalações físicas do Ministério da Saúde.

Parágrafo único. A classificação das áreas e instalações físicas do Ministério da Saúde deverá ser realizada conforme Anexo B, considerando os seguintes aspectos das informações tratadas no local:

I - valor;

II - criticidade;

III - tipo de ativo de informação;

IV - classificação; e

V - grau de sigilo.

Art. 13. As áreas e instalações físicas do Ministério da Saúde classificadas com nível de criticidade alto terão:

I - procedimentos específicos para o controle do acesso físico; e

II - análise da necessidade de adoção de sistema de detecção de intrusos e sistemas de vídeo e monitoramento.

CAPITULO VI

DO NÚCLEO DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 14. Os usuários da rede devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da Política de Segurança da Informação e Comunicações ao núcleo de Gestão de Segurança da Informação e Comunicações do Ministério da Saúde.

Art. 15. O núcleo de Gestão de Segurança da Informação e Comunicações deverá ser imediatamente acionado em casos de quebra de segurança da informação por meio de recursos de tecnologia da informação.

Parágrafo único. O núcleo de Gestão de Segurança da Informação e Comunicações, após o acionamento de que trata o caput, tomará as providências necessárias a sanar as causas, com a possibilidade de determinar a restrição temporária do acesso às informações e o uso dos recursos de tecnologia da informação do Ministério da Saúde.

ANEXO A

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em __/__/____, e lotado no(a)_____do Ministério da Saúde, DECLARO, sob pena das sanções cabíveis, nos termos da legislação vigente, ter recebido credenciais de acesso à Rede do Ministério da Saúde, para uso e desempenho das minhas funções profissionais, sendo responsável pelo seu uso e guarda.

Comprometo-me, ainda, a cumprir todas as etapas do curso básico em Segurança da Informação, no prazo máximo de 90 (noventa) dias, estando ciente da Política de Segurança da Informação e Comunicações do Ministério da Saúde e das minhas responsabilidades por:

I - zelar pelos ativos de informação e tratá-los como patrimônio do Ministério da Saúde;

II - utilizar as informações sob minha custódia, exclusivamente, no interesse do serviço do Ministério da Saúde;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Política de Segurança da Informação e Comunicação do Ministério da Saúde, devendo comunicar por escrito à chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou de falhas identificadas nos sistemas;

IV - utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Ministério da Saúde; e

V - responder, perante o Ministério da Saúde, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação eventual dano ou divulgação indevida.

Declaro, ainda, estar plenamente esclarecido e consciente que:

I - o acesso à informação não me garante direito sobre ela, nem me confere autoridade para liberar acesso a outras pessoas;

II - constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos dos sistemas aos quais tenho acesso para outros servidores não envolvidos nos trabalhos executados;

III - devo cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação e Comunicações e das Normas de Segurança estabelecidas, bem como deste Termo de Responsabilidade;

IV - ressalvadas as hipóteses de requisições legalmente autorizadas, constitui infração funcional e penal a revelação de segredo do qual me apropriei em razão do cargo, sendo crime contra a administração pública a divulgação a quem não seja agente público do Ministério da Saúde, das informações do(s) sistema(s) a que tenho acesso, estando sujeito às penalidades previstas em lei;

V - sem prejuízo da responsabilidade penal e civil, e de outras sanções disciplinares, constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro agente público, ainda que habilitado; e

VI - constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da Administração Pública, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano, ficando o infrator sujeito as punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-A; e

VII - constitui infração funcional e penal modificar ou alterar o sistema de informações ou programa de informática sem autorização ou sem solicitação de autoridade competente; ficando o infrator sujeito as punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-B.

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente.

Local, UF, __de _____de ____.

Ass. _____

ANEXO B

CLASSIFICAÇÃO DOS ATIVOS DE INFORMAÇÃO

Grau de criticidade	Ativos de informação	Impacto
Nível 1 Alto	Data-center, servidores, central telefônica, recursos criptológicos, cópias de segurança, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de primeiro escalão.	Interrompe a missão do órgão ou provoca grave dano à imagem institucional, à segurança do estado ou sociedade.
Nível 2 Médio	Computadores com dados e informações únicas, de grande relevância, equipamentos de conectividade ou de armazenamento de informações ou de computação móvel das autoridades de segundo escalão.	Degrada o serviço do órgão ou provoca danos à imagem institucional, à segurança do estado ou sociedade.
Nível 3 Baixo	Os demais ativos de informação.	Compromete planos ou provoca danos aos ativos de informação.

ANEXO III

CÓPIAS DE SEGURANÇA NO ÂMBITO DO MINISTÉRIO DA SAÚDE

CAPITULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Anexo estabelece orientações e requisitos para cópias de salvaguarda no âmbito do Ministério da Saúde.

Parágrafo único. As ações deste Anexo deverão observar o disposto nos seguintes atos:

I - 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;

II - Norma complementar nº 20/IN01/DSIC/GSIPR (Revisão 01), de 15 de dezembro de 2014 - Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

III - ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da Informação; e

IV - ABNT NBR ISO/IEC 27001:2013 - Técnicas de segurança - Sistemas de Gestão de Segurança da Informação - Requisitos.

Art. 2º Para fins deste Anexo, consideram-se as seguintes definições:

I - cópia de segurança ou backup: cópia dos dados de determinado dispositivo de armazenamento para outro, possibilitando sua restauração em caso de perda dos dados originais;

II - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

III - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V - log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional;

VI - mídias: dispositivos de armazenamento utilizados para a cópia dos dados originais quando da realização do backup, tais como fitas, CD-ROM, DVD, cartuchos, HD, entre outros;

VII - gestor da informação: indivíduo da parte interessada do órgão ou entidade da APF, legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência da informação;

VIII - restauração ou restore: ato de recuperar uma versão anterior armazenada em dispositivo específico para retornar ao estado original ou anterior à versão atual;

IX - storage: dispositivo projetado especificamente para armazenamento de dados, que pode-se conectar seu(s) servidor(es) a um storage por meio de conexão via rede, facilitando a expansão da capacidade de armazenamento, sem impacto na produção, garantindo maior flexibilidade e confiabilidade no armazenamento;

X - procedimento de cópias de segurança: procedimento de verificação, por amostragem, para validação das cópias de segurança realizadas; e

XI - cópia de segurança sob demanda: cópia de segurança realizada fora da rotina normal.

CAPITULO II

DOS PROCEDIMENTOS

Art. 3º Deverão ser observados os seguintes procedimentos na gestão de cópias de segurança:

I - verificação, por amostragem, para validação das cópias de segurança realizadas;

II - acompanhamento constante do funcionamento do software de cópia de segurança e das mídias de modo a garantir a geração e a restauração das cópias de segurança quando necessário;

III - verificações para controle da vida útil das mídias de cópias de segurança;

IV - plano de treinamento quanto aos procedimentos de geração e restauração de cópias de segurança para os responsáveis por essas atividades;

V - planejamento dos recursos necessários para geração e restauração de cópias de segurança;

VI - estimativa de tempo necessário para a recuperação dos dados, de modo a não gerar impacto em rotinas de produção; e

VII - formulário e processo específico pelo qual será solicitado a recuperação dos dados.

Art. 4º A geração das cópias de segurança deve observar as seguintes regras:

I - os procedimentos e rotinas de cópias de segurança deverão ser documentados e armazenados em local seguro e com controle de acesso;

II - as tecnologias utilizadas para a realização das cópias de segurança e restauração deverão atender aos requisitos de segurança para preservação da integridade, confidencialidade e disponibilidade das informações;

III - as cópias de segurança deverão ser geradas em dispositivos de armazenamento, tais como fitas, storage, entre outros, conforme as especificações do fabricante e por meio do uso de software homologado pelo DATASUS;

IV - a geração de cópias de segurança ocorrerá em períodos de baixa utilização dos recursos de tecnologia da informação, de modo a não impactar o funcionamento das áreas, preferencialmente fora do horário de expediente;

V - os logs gerados após a realização das cópias de segurança deverão ser analisados, para verificação de falhas ou exceções durante o processo, permitindo a tomada de ações corretivas; e

VI - em situações que demandam confidencialidade, as cópias de segurança deverão ser protegidas por encriptação.

Art. 5º Deverão ser observados os seguintes procedimentos para a restauração das cópias de segurança:

I - as solicitações para restauração de cópias de segurança deverão ser autorizadas pelo gestor da informação e encaminhadas ao servidor de TI responsável por cópias de segurança;

II - a restauração de cópias de segurança deverá ser realizada em ambiente distinto do ambiente de produção original, de forma a não sobrescrever as informações;

III - o gestor da informação deverá verificar e validar a integridade das informações restauradas antes da sua utilização;

IV- a restauração para ambiente de produção ocorrerá apenas nos seguintes casos:

a) para recompor a integridade do ambiente afetado; e

b) por solicitação formal e justificada do gestor da informação à área responsável pelo processo de cópias de segurança.

V - os responsáveis pelo processo de cópias de segurança e recuperação deverão analisar os logs gerados após a restauração das cópias de segurança, a fim de verificar se houve falhas ou exceções durante o processo e providenciar as ações corretivas;

VI - as mídias de cópias de segurança utilizadas no processo de restauração deverão estar previamente protegidas contra escrita, de modo a prevenir a perda das informações armazenadas;

VII - testes de restauração amostral deverão ser periodicamente realizados pela área responsável pelas cópias de segurança, a fim de garantir a disponibilidade das informações armazenadas nas cópias de segurança; e

VIII - no caso dos servidores de banco de dados, deverá haver espaço preparado para receber a base restaurada.

Parágrafo único. O teste de recuperação de dados de que trata o inciso VII do caput será executado com periodicidade máxima de 30 (trinta) dias.

Art. 6º Deverão ser observadas as seguintes regras na identificação das mídias de cópia de segurança:

I - o processo de geração e restauração das cópias de segurança deve prover identificação única das mídias contemplando, no mínimo, as seguintes informações:

a) tipo de cópias de segurança realizado (Full, Differential, Incremental);

b) data de realização das cópias de segurança;

c) periodicidade de realização das cópias de segurança; e

d) serviços ou locais dos quais foram realizadas as cópias de segurança.

II - o responsável de TI pelo processo de cópias de segurança deverá possuir documentação que registre a descrição e versão do software utilizado para geração das cópias de segurança; e

III - as mídias utilizadas na realização de cópias de segurança sob demanda deverão conter identificação diferenciada das demais mídias.

Art. 7º Deverão ser observados os seguintes procedimentos no armazenamento e transporte das cópias de segurança:

I - as cópias de segurança deverão ser duplicadas e gravadas em mídia de contingência, sendo uma armazenada no Ministério da Saúde e outra armazenada em um ambiente remoto, em distância suficiente para não sofrer danos de possível desastre no Ministério da Saúde;

II - o ambiente remoto terá os mesmos requisitos de segurança aplicados ao ambiente principal visando garantir a integridade das mídias e dos dados nelas armazenados;

III - o transporte das mídias para local externo ao Ministério da Saúde deve ser acompanhado por responsável da área de TI devidamente identificado e autorizado;

IV - o transporte das mídias de cópia de segurança será realizado em embalagens apropriadas para cada tipo de mídia;

V - o transporte das mídias será registrado e autorizado pela área responsável pelas cópias de segurança; e

VI - deve-se manter as mídias de cópias de segurança em uso armazenadas de forma a permitir sua rápida localização e recuperação.

Art. 8º Deverão ser observados os seguintes procedimentos no descarte e substituição das mídias de cópia de segurança:

I - a substituição das mídias utilizadas para realização das cópias de segurança deverá observar os critérios definidos pelo fabricante;

II - o descarte das mídias utilizadas para cópia de informações do Ministério da Saúde deverá respeitar a temporalidade prevista na legislação, a política, as normas, os procedimentos de segurança internos e a classificação das informações quanto à confidencialidade;

III - as mídias de cópias de segurança deverão ser descartadas de forma segura, de modo a impossibilitar sua recuperação total ou parcial, por meio de procedimentos formais;

IV - no caso de descarte realizado por empresa especializada, deverão ser verificados os requisitos básicos de segurança para a contratação do serviço, a experiência e os controles adotados pela empresa para garantir a segurança do descarte;

V - nos casos de substituição da solução de cópias de segurança (hardware e software), as informações contidas nas mídias da antiga solução serão transferidas em sua totalidade para as mídias compatíveis com a nova solução; e

VI - a solução de cópias de segurança obsoleta somente poderá ser desativada após a certeza de que todas as informações foram transferidas para a nova solução implementada.

CAPITULO III

DAS DISPOSIÇÕES FINAIS

Art. 9º A definição dos recursos adotados no processo de geração e restauração de cópias de segurança é de responsabilidade da área de Tecnologia da Informação e Comunicações - TIC que custodia a informação.

Art. 10. A geração e restauração de cópias de segurança das informações devem ser precedidas de planejamento e definição de estratégia que preserve a disponibilidade das informações armazenadas.

Art. 11. Os gestores das informações deverão definir os prazos de realização, retenção e descarte das informações do Ministério da Saúde a serem armazenadas nas mídias de cópia de segurança, de forma a respeitar os níveis de classificação atribuídos às informações.

Art. 12. As cópias de segurança de arquivos armazenados em estações de trabalho são de responsabilidade do custodiante da estação.

Art. 13. A inobservância do disposto nesta norma ensejará a aplicação das sanções previstas na legislação em vigor.

Art. 14. Os usuários devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento da POSIC/MS à área responsável por Segurança da Informação e Comunicações do Ministério da Saúde.

Art. 15. A área responsável por Segurança da Informação e Comunicações tem a atribuição de analisar e prestar orientações acerca de questionamentos sobre a POSIC/MS.

Art. 16. As situações não tratadas expressamente neste Anexo serão analisadas pelo Subcomitê Gestor de Segurança da Informação e Comunicação do Ministério da Saúde.

ANEXO IV

GERENCIAMENTO DE MUDANÇAS NO ÂMBITO DO MINISTÉRIO DA SAÚDE

CAPITULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1 º Este Anexo estabelece diretrizes e orientações para o controle e gerenciamento das alterações nos ambientes computacionais, de forma a minimizar o risco de impactos na disponibilidade, integridade e confiabilidade dos sistemas e serviços utilizados.

Parágrafo único. As ações deste Anexo deverão observar o disposto na:

I - Norma Complementar nº 13/IN01/DSIC/GSI/PR, de 30 de janeiro de 2012, que estabelece Diretrizes para Gestão de Mudanças nos Aspectos Relativos à Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal (APF);

II - ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de segurança da Informação; e

III - ITIL - Biblioteca de publicações das melhoras práticas para o gerenciamento de serviços de TI.

Art. 2º Para fins deste Anexo, consideram-se as seguintes definições:

I - Domain Name Service - DNS: serviço de rede responsável pela tradução de endereço físico (IP) para endereço lógico;

II - ativos de informação: os meios de armazenamento, processamento e transmissão, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

III - autenticidade: propriedade da informação referente à sua produção, expedição, modificação ou destruição por determinada pessoa física ou por determinado sistema, órgão ou entidade;

IV - confidencialidade: propriedade de que a informação não esteja disponível ou seja revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

V - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

VI - mudança: introdução, alteração ou exclusão de uma situação atual na infraestrutura computacional, sistemas e serviços de TI, de maneira controlada, autorizada, planejada e aprovada formalmente;

VII - mudança padrão: mudanças que necessitam ser executadas de forma rotineira para garantir a sustentabilidade do ambiente computacional, normalmente pré-aprovadas e com baixo risco para a organização;

VIII - mudança normal: mudanças que necessitam de planejamento prévio elaborado pelo Solicitante para que possam ser executadas, podendo ser categorizadas como importante, significativa ou pequena e devendo seguir os estágios completos de avaliação, autorização e implementação;

IX - mudança emergencial: mudanças altamente críticas que precisam ser implementadas rapidamente, para resolver incidente grave ou implementar patch de segurança;

X - Comitê de Mudança: comitê encarregado de avaliar a necessidade de realização, autorização e priorização de mudanças;

XI - gestão de mudanças: processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito do órgão ou entidade da APF, com objetivo de viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;

XII - gestão de riscos: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XIII - Gestor de Mudanças: responsável pelo processo de mudanças no âmbito do Ministério da Saúde;

XIV - Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do Ministério da Saúde;

XV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XVI - Label: mecanismo utilizado para identificar configuração específica de um ativo de configuração, contemplando um rótulo diferenciado para cada configuração que necessita ser rastreada em um determinado momento, conforme linha de base gerada;

XVII - Patch: evoluções aplicadas a determinado item de configuração para ajustar alguma disfunção identificada após sua implementação ou para otimizar o desempenho e a usabilidade do software definido; e

XVIII - Rollback: terminologia utilizada para definir a necessidade de desfazer uma ou mais ações realizadas durante uma determinada transação.

Art. 3º São diretrizes a serem observadas na Segurança da Informação e Comunicações para Gerenciamento de Mudanças no âmbito do Ministério da Saúde:

I - a integração do processo de gerenciamento de mudanças aos demais processos envolvidos como, gestão de configuração, incidentes, riscos e continuidade do negócio;

II - a utilização de ferramentas e técnicas apropriadas para execução do processo como premissa para a consolidação de lições aprendidas e melhora evolutiva do processo; e

III - a disseminação das normas e do processo estabelecido para as demais unidades do Ministério da Saúde envolvidas com a solicitação e execução da mudança.

CAPITULO III

DAS SOLICITAÇÕES, ANÁLISES E GERENCIAMENTO DE MUDANÇAS

Art. 4º O processo de gerenciamento de mudanças contempla as fases de Registro, Avaliação, Aprovação, Implementação e Verificação, conforme as seguintes definições:

I - registro: consiste no detalhamento do escopo, objetivo e benefícios a serem alcançados com a execução da mudança, podendo abranger todo Ministério da Saúde, ou apenas um segmento ou ativo de informação;

II - avaliação: consiste na identificação e avaliação dos potenciais impactos que possam ocorrer durante a implementação da mudança, de forma a contemplar o planejamento da remediação (rollback) em caso de falha, que conterá a descrição das etapas necessárias para a restauração do objeto a sua situação inicial em caso de falha durante a implementação da mudança;

III - aprovação: consiste na formalização da aprovação ou não das mudanças propostas por meio da reunião periódica do comitê de mudanças;

IV - implementação: consiste no agendamento e implementação das mudanças aprovadas de acordo com os procedimentos descritos na solicitação e aprovadas pelo comitê; e

V - verificação: ocorre paralelamente à fase de implementação e consiste na análise da implementação realizada e do resultado alcançado quanto à viabilização e efetivação da disponibilidade, integridade, confidencialidade e autenticidade da informação.

§ 1º Nenhuma mudança deve ser aprovada sem possuir um plano de remediação.

§ 2º Após aprovada a execução da mudança, os interessados devem ser comunicados para conhecimento e tomada de ações necessárias.

§ 3º Caso necessário, o comitê de mudanças pode solicitar a participação do gestor do negócio para fornecer esclarecimentos adicionais.

§ 4º Nenhuma mudança pode ser executada sem a aprovação do comitê de mudanças.

Art. 4º O Comitê de Mudanças é competente para realizar a análise e apreciação das mudanças relacionadas aos sistemas de informação, e será composto pelo:

I - demandante da mudança;

II - responsável pela infraestrutura;

III - responsável pelo banco de dados;

IV - coordenador da área de desenvolvimento vinculado;

V - responsável pelo sistema;

VI - responsável pela infraestrutura; e

VII - demais envolvidos na mudança.

§ 1º A análise de que trata o caput ocorrerá somente após a homologação prévia das mudanças pelo gestor do negócio.

§ 2º O Comitê de Mudanças possuirá agenda periódica para:

I - a avaliação das mudanças previstas para o período e acompanhamento da execução das mudanças em andamento; e

II - deliberação das solicitações recebidas, priorizadas e com execução aprovadas, com base nos impactos identificados.

Art. 5º As requisições de mudança no ambiente computacional de TI deverão ser registradas por meio do formulário Requisição de Mudanças - RDM.

Parágrafo único. As RDMs terão análise prévia do Gestor de Mudanças, que as encaminhará ao Comitê de Mudanças para apreciação e aprovação.

Art. 6º O Gestor de Mudanças deverá validar o tipo da mudança solicitada inicialmente e tomar as providências necessárias para sua implementação, classificando-as como Padrão, Normal ou Emergencial.

Parágrafo único. Caso a mudança gere impacto em outras unidades organizacionais, deverá ser emitido comunicado formal quanto à ação que será realizada e a previsão de restabelecimento do serviço.

Art. 7º Antes de sua execução, as mudanças solicitadas deverão ser classificadas quanto à abrangência e ao impacto da execução, da seguinte forma:

I - quanto à abrangência:

a) sistemas operacionais;

b) bancos de dados;

c) aplicações/aplicativos;

d) infraestrutura de rede; e

e) infraestrutura física.

II - quanto ao impacto da execução:

a) alto impacto: aquela que impacta mais de um sistema ou estrutura crítica em produção ou treinamento;

b) médio impacto: aquela que ocorre em ativos de tecnologia ou infraestrutura, mas não afeta outras aplicações ou serviços suportados pela área de TI do Ministério da Saúde; e

c) baixo impacto: aquela destinada para um único ativo, não sendo necessária a paralisação ou indisponibilidade significativa dos serviços prestados, tais como atualização de "label" na aplicação, atualização de "patches", implementação de controles de segurança, atualização de antivírus, entre outras.

§ 1º A mudança classificada como de alto impacto deve ser autorizada pelos gestores das áreas responsáveis pelo(s) serviço(s) afetado(s) e pelo respectivo coordenador de desenvolvimento.

§ 2º A mudança classificada como de médio impacto deve ser autorizada pelos gestores das áreas responsáveis pelos serviços afetados.

§ 3º A mudança classificada como de baixo impacto deve ser autorizada pelo responsável do ativo.

CAPITULO IV

DA EXECUÇÃO DAS MUDANÇAS

Art. 8º A atualização de mudança em ambiente de produção deverá ser precedida de homologação pelo gestor em ambiente equivalente ao ambiente de produção, no que tange às características de configuração de software.

Parágrafo único. Os resultados obtidos no procedimento descrito no caput devem ser registrados e mantidos para posterior consulta.

Art. 9º Após executadas em ambiente de produção, as mudanças consideradas de alto impacto deverão ser monitoradas durante período definido pelo Comitê de Mudanças e pelo Gestor do Negócio, para verificação de sua adequada execução.

Art. 10. As mudanças, sempre que possível, deverão ser executadas fora do horário crítico de funcionamento do serviço ou sistema, conforme regras estabelecidas pela equipe responsável, de forma a minimizar o impacto no ambiente computacional.

Art. 11. Após a implementação da mudança, as RDMs somente serão encerradas mediante a atualização dos registros relacionados, tais como inventário de ativos de informação, instruções de trabalho, procedimentos, normas técnicas e materiais de treinamento.

Art. 12. Caso seja identificada situação não planejada e que impacte diretamente no ambiente computacional de TI, o Gestor de Mudanças deve ser acionado para análise e providências necessárias.

CAPITULO V

DAS DISPOSIÇÕES FINAIS

Art. 13. Compete ao Comitê de Informação e Informática do Ministério da Saúde - CIINFO/MS revisar as normas deste Anexo, com auxílio do Subcomitê Gestor de Segurança da Informação e Comunicação.

Art. 14. Compete à área de Gestão de Segurança da Informação monitorar periodicamente a conformidade deste Anexo, por meio do software de gestão de riscos e de lista de verificação, de forma a possibilita a análise comparativa dos resultados obtidos com os resultados.

Art. 15. Compete aos agentes públicos reportar à área de Gestão de Segurança da Informação:

I - incidentes que afetem diretamente o processo de mudança dos ativos de informações; e

II - o descumprimento deste Anexo.

Art. 16. As situações não tratadas expressamente neste Anexo deverão ser encaminhadas ao Subcomitê Gestor de Segurança da Informação e Comunicação do Ministério da Saúde.

ANEXO V

INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO - GESTÃO DE ATIVOS

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Anexo estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação e os requisitos de segurança a serem seguidos, de forma a apoiar a Segurança da Informação e Comunicações e alcançar a proteção adequada dos ativos de informação do Ministério da Saúde.

Parágrafo único. As ações de que trata este Anexo deverão observar o disposto:

I - na Norma Complementar nº 10/IN01/DSIC/GSI/PR, de 30 de janeiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

II - na ABNT NBR ISO/IEC 27002:2013 - Código de Práticas para a Gestão da Segurança da Informação; e

III - no Guia de Referência para a Segurança das Infraestruturas Críticas da Informação - BRASIL/GSIPR, 2010.

Art. 2º O processo de Inventário e Mapeamento de Ativos de Informação tem como objetivos:

I - prover conhecimento amplo, consistente e inequívoco:

a) dos ativos de informação, da identificação clara de seus responsáveis - proprietários e custodiantes;

b) do conjunto completo de informações básicas sobre os requisitos de segurança da informação e comunicações de cada ativo de informação;

c) de descrição do contêiner de cada ativo de informação; e

d) do valor que o ativo de informação representa para as atividades do Ministério da Saúde.

II - subsidiar o conhecimento, valorização, proteção e manutenção do ativos de informação, em conformidade com os requisitos legais e da instituição; e

III - auxiliar a Gestão da Segurança da Informação e Comunicações nas Infraestruturas Críticas de Informação do MS, apoiando:

a) a Gestão de Riscos de Segurança da Informação;

b) a Gestão de Mudanças e a Gestão de Continuidade de Negócios adotados pelo MS; e

c) os procedimentos de avaliação da conformidade, de melhoria contínua, auditoria e de estruturação e geração de base de dados sobre os ativos de informação.

Art. 3º Para fins deste Anexo, consideram-se as seguintes definições:

I - agente responsável: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação;

II - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III - ativos de informação: os meios de armazenamento, transmissão e processamento da informação, incluindo os equipamentos necessários, os sistemas utilizados, os locais onde se encontram e os recursos humanos que a eles têm acesso;

IV - 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.

V - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VI - contêineres dos ativos de informação: local onde o ativo de informação está armazenado e como é transportado ou processado;

VII - continuidade de negócios: capacidade estratégica e tática de planejamento e resposta a incidentes e interrupções de negócios, de forma a minimizar seus impactos e recuperar perdas de ativos da informação das atividades críticas, de modo a manter suas operações em um nível aceitável, previamente definido;

VIII - custodiante do ativo de informação: agente ou estrutura do Ministério da Saúde que tenha a responsabilidade formal pelos contêineres dos ativos de informação e pela aplicação dos controles de segurança em conformidade com os níveis exigidos e comunicados pelos proprietários dos ativos de informação;

IX - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

X - estratégia de continuidade de negócios: abordagem que garanta a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com desastre, interrupção ou outro incidente;

XI - gestão de riscos de segurança da informação e comunicações: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XII - infraestrutura crítica da informação: são os meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade;

XIII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIV - inventário e mapeamento de ativos de informação: processo interativo e evolutivo, que consiste na identificação e classificação de ativos de informação, mapeamento geográfico e inter-relações com sistemas, serviços e outros ativos de informação;

XV - proprietário do ativo de informação (Mantenedor): parte interessada ou setor do Ministério da Saúde, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário (principal) pela viabilidade e sobrevivência (conservação) dos ativos de informação;

XVI - riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XVII - segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XVIII - valor do ativo de informação: valor, tangível e intangível, que reflete a importância do ativo de informação para o alcance dos objetivos estratégicos do Ministério da Saúde, quanto à imprescindibilidade aos interesses da sociedade e do Estado; e

IX - 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.

CAPITULO II

DOS PROCEDIMENTOS

Art. 4º Todo ativo tecnológico instalado deve estar mapeado, identificado e com inventário estruturado mantido, sendo designado, pelo menos, um proprietário e um custodiante para cada ativo de informação.

Parágrafo único. Serão utilizadas, sempre que possível, as bases de inventários já existentes no Ministério da Saúde.

Art. 5º Os ativos de informação em uso considerados importantes possuirão um proprietário e substituto, nomeados por ato publicado no boletim de serviços do Ministério da Saúde.

Art. 6º A identificação e classificação de ativos de informação possuirá 6 (seis) etapas, obedecendo o seguinte procedimento:

I - coleta de informações gerais dos ativos de informação;

II - detalhamento do conteúdo dos ativos de informação;

III - identificação dos responsáveis - proprietários e custodiantes - de cada ativo de informação;

IV - caracterização do contêiner do ativo de informação;

V - definição dos requisitos de segurança dos ativos de informação; e

VI - estabelecimento do valor do ativo de informação.

Art. 7º A coleta de informações gerais dos ativos de informação deve ser:

a) realizada periodicamente por meio de ferramenta automatizada.

b) comunicada e registrada na Base de Dados de Ativos de Informação em caso de qualquer alteração nos ativos de informação.

Art. 8º O detalhamento do conteúdo dos ativos de informação deve:

I - ser definido a partir da necessidade do negócio e dos seus objetivos estratégicos;

II - incluir todas as informações necessárias a partir das necessidades de recuperação ou de substituição eficiente dos ativos de informação, em caso de desastre, bem como a atender aos interesses da sociedade e do Estado;

III - contemplar, no mínimo e quando aplicável, o seguinte conjunto essencial de informações:

a) ativos de tecnologia, identificação do Ativo, tipo de equipamento (servidor, máquina virtual, switch, outros), uso (desenvolvimento, homologação, teste ou produção), descrição/conteúdo; características do equipamento, marca - modelo, número de série, patrimônio, proprietário do ativo, custodiante do ativo, valor do ativo (Relevância) Requisitos de Segurança, sistemas e serviços associados ao ativo; localização: local físico (conteiner), informações de cópia de segurança; informações de licença de uso; sistema operacional/Versão, aplicativos utilizados, data da última atualização; conexões: ID do switch, ID Storage e outras conexões;

b) ativo Pessoas: matricula, nome, cargo/função, e-mail institucional, área/setor telefone/ramal, valor do ativo (Relevância), requisitos de segurança, organização (Proprietário), superior imediato (Custodiante), sistemas e serviços associados ao ativo;

c) ativo ambiente: identificação, localização, valor do ativo (Relevância), requisitos de segurança, custodiante do ativo, proprietário do ativo; e

d) ativo processo: identificação, nome do processo, descrição do processo, localização/setor, valor do ativo (relevância), requisitos de segurança, custodiante do ativo (responsável pela execução), Proprietário do ativo (responsável pela publicação).

Art. 9º Na identificação dos responsáveis - proprietários e custodiantes - de cada ativo de informação, deve constar, no mínimo, as seguintes informações:

a) nome;

b) matrícula;

c) e-mail;

d) local de trabalho; e

e) telefone de contato.

Art. 10. Quanto à caracterização do contêiner do ativo de informação, recomenda-se que contenha, no mínimo, as seguintes informações:

I - lista de todos os recipientes onde o ativo da informação é armazenado, transportado ou processado; e

II - indicação dos responsáveis por manter estes recipientes.

Parágrafo único. Também caracterizam um contêiner os limites do ambiente físico e seus relacionamentos, que devem atender às exigências de segurança da informação e comunicações.

Art. 11. A definição dos requisitos de segurança dos ativos de informação deve ser realizada por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Parágrafo único. Recomenda-se que os requisitos de segurança da informação e comunicações dos ativos de informação sejam indicados, no mínimo, nas 5 (cinco) categorias de controle a seguir elencadas:

I - assegurar tratamento da informação conforme o grau de segurança das informações nele contidas, de acordo com as orientações descritas em legislação específica sobre classificação da informação;

II - assegurar controles de acesso físico e lógico conforme as restrições ao acesso definidas pelo grau de segurança das informações nele contidas, de acordo com as orientações descritas em legislação específica sobre classificação da informação;

III - gestão de risco de segurança da informação e comunicações;

IV - tratamento e respostas a incidentes em redes computacionais; e

V - gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.

Art. 12. No procedimento de estabelecimento do valor do ativo de informação, os proprietários dos ativos de informação devem indicar o valor do ativo para a área de negócio do Ministério da Saúde, considerando:

I - os fatores de riscos aos quais os ativos possam estar expostos como ameaça, vulnerabilidade e impacto decorrente de um incidente;

II - a importância do ativo de informação para que a organização alcance seus objetivos estratégicos; e

III - a tabela constante no Anexo-A, que indica o valor (relevância) do ativo segundo o grau em que afeta os serviços do Ministério Saúde à população.

CAPITULO III

DAS COMPETÊNCIAS

Art. 13. Compete à Coordenação Geral de Infraestrutura de TI do DATASUS:

I - prover os recursos tecnológicos necessários à manutenção da Base de Ativos de Informação utilizada no processo de gerenciamento e mapeamento de ativos tecnológicos de Informação;

II - monitorar os níveis de segurança dos ativos de informação;

III - elaborar relatórios gerenciais;

IV - coordenar as ações em caso de comprometimento da segurança lógica e física do ativo;

V - garantir que sistema operacional e aplicativos estejam sujeitos a controle de mudanças em conformidade com a Norma Complementar Nº 13/IN01/DSIC/GSIPR, que estabelece diretrizes para a VI-Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC);

VI - definir parâmetros para a geração de cópias de segurança (Backup) e sua recuperação (Restore) em um tempo aceitável, e em conformidade com o Decreto Nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos de segurança e tratamento de informações classificadas; e

VII - garantir que os registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzido e mantidos por um período de tempo suficiente para auxiliar em futuras investigações e monitoramento de controle de acesso.

Art. 14. Compete ao proprietário do ativo de informação, como responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumir, no mínimo, as seguintes atividades:

I - descrever o ativo de informação;

II - informar ao custodiante as informações cadastrais sobre o ativo, mantendo-as atualizadas quanto ao hardware, software e serviços disponibilizados por meio do ativo;

III - indicar o valor do ativo para o negócio ou serviço que desempenha, considerando a tabela constante no Anexo A;

IV - definir as exigências de segurança da informação e comunicações do ativo de informação;

V - assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento contínuo;

VI - indicar os riscos de segurança da informação e comunicações que podem afetar os ativos de informação;

VII - delegar para um custodiante, mediante acordo prévio, as tarefas de administração diária dos ativos;

VIII - estabelecer critérios que assegurem a segregação de funções para evitar a detenção do controle de um processo ou sistema na sua totalidade por apenas um agente, de forma a reduzir o risco de mau uso acidental ou deliberado dos ativos de informação; e

IX - comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários.

Parágrafo único. A delegação de que trata o inciso VII do caput não exime a responsabilidade do proprietário do ativo de informação.

Art. 15. Compete ao custodiante dos ativos:

I - manter atualizado o cadastro dos ativos, sob sua custódia, no banco de dados de ativos de informação do ministério da saúde;

II - proteger o ativo de informação quanto ao armazenamento, transporte e processamento, de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação;

III - proteger os contêineres dos ativos de informação, aplicando os níveis de controles de segurança em conformidade com as exigências comunicadas pelo proprietário do ativo;

IV - implementar controles específicos, podendo conforme a necessidade, delegar a um terceiro, sem prejuízo das responsabilidades pela proteção adequada dos ativos;

V - manter as informações cadastrais sobre o ativo atualizadas quanto ao hardware, software e serviços disponibilizados por meio daquele ativo;

VI - atualizar todos os softwares que sejam executados naquele ativo sempre que viável ou solicitado pelo proprietário;

VII - definir e implementar novas funcionalidades, manter o ativo atualizado e configurar novos serviços;

VIII - monitorar o ativo tecnológico diariamente e comunicar ao proprietário qualquer problema ou incidente de segurança envolvendo o ativo, devendo ainda registrar as ações que foram adotadas para sanar ou minimizar o problema;

IX - realizar as modificações necessárias nos ativos, de acordo com o planejamento;

X - garantir que as cópias de segurança estão sendo geradas;

XI - monitorar periodicamente os registros de auditoria (log), avisando imediatamente ao responsável qualquer problema encontrado;

XII - impedir qualquer modificação nos equipamentos, instalação de software de qualquer natureza ou a modificação de qualquer configuração no ativo, sem a autorização por escrito do proprietário do ativo;

XIII - identificar e classificar os ativos de informação; e

XIV - realizar estudos de planejamento de capacidade de forma a evitar sobrecarga.

CAPITULO IV

DISPOSIÇÕES FINAIS

Art. 16. O processo de Inventário e Mapeamento de Ativos de Informação será estruturado e revisto periodicamente, de modo a manter uma Base de Dados de Ativos de Informação atualizada e prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

§ 1º A Base de Dados de que trata o caput deve operar como infraestrutura material e técnica em condições de dar suporte às ações de cooperação entre entes federativos que têm sob as suas gerencias ativos de informação.

§ 2º A revisão do processo de Inventário e Mapeamento de Ativos de Informação ocorrerá, no máximo, a cada 6 (seis) meses.

Art. 17. Os Agentes Públicos devem reportar os incidentes que afetam a segurança dos ativos ou o descumprimento das Diretrizes de Segurança da Informação, por meio dos canais disponibilizados pelo Ministério da Saúde.

Art. 18. Os incidentes identificados como extravio, furto ou roubo de equipamentos devem ser tratados pela área de segurança patrimonial.

Parágrafo único. É responsabilidade do proprietário do ativo interagir com área de segurança patrimonial, a fim de garantir a tomada de todas as providências necessárias.

Art. 19. As situações não tratadas expressamente neste Anexo serão submetidas ao Subcomitê de Segurança da Informação e Comunicações para análise.

ANEXO A

TABELA - VALOR DO ATIVO DE INFORMAÇÃO

Valor (Relevância) - Importância do Ativo

aGRAU	b - Se o Ativo for comprometido:	cVALOR
Muito alto	Afeta serviços e produtos que garantem a saúde da população, ocasionando a perda de vidas, epidemias e outros	5
Alto	Afeta serviços e produtos que garantem a saúde da população, ocasionando o agravamento de quadros clínicos.	4
Médio	Afeta a disponibilidade dos serviços e produtos que garantem a saúde da população, podendo comprometer seu atendimento, mas não sua saúde.	3
Baixo	Afeta a disponibilidade dos serviços e produtos, mas não compromete a saúde da população.	2
Muito baixo	A interrupção não afeta a disponibilidade normal dos serviços e produtos.	1

ANEXO VI

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - GRSIC

CAPITULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Este Anexo estabelece as diretrizes e orientações para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC, no âmbito do Ministério da Saúde.

Parágrafo único. As ações deste Anexo deverão observar:

I - a Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 25 de fevereiro de 2013 - Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

II - a ABNT NBR ISO 31000:2009 - Gestão de Riscos: Princípios e Diretrizes;

III - a ABNT NBR ISO GUIA 73:2009 - Gestão de Riscos: Vocabulário; e

IV - a ABNT NBR ISO 27005:2011 - Tecnologia da Informação: Técnicas de segurança - Gestão de riscos de segurança da informação.

Art. 2º Para fins deste Anexo, consideram-se as seguintes definições:

I - aceitação do risco: decisão informada para aceitar as consequências e a probabilidade de um particular risco;

II - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

III - análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;

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

V - ativo de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

VII - componentes: sistemas ou softwares que compõem o ativo e o ambiente em que o ativo está inserido, podendo ser sistemas operacionais, aplicativos, serviços ou estrutura física.

VIII - comunicação do risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

IX - criticidade dos ativos: relação entre a vulnerabilidade frente às ameaças existentes, conforme os riscos de ocorrência de determinados tipos de evento, considerados o impacto resultante e sua dependência a outros processos e ativos;

X - controle: recomendação de segurança feita para que se elimine o risco contido em uma vulnerabilidade;

XI - estimativa de riscos: processo utilizado para atribuir valores à probabilidade e consequências de um risco;

XII - evitar risco: uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

XIII - gestão de riscos de segurança da informação e comunicações - GRSIC: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-las com os custos operacionais e financeiros envolvidos;

XIV - gestor do risco: pessoa ou entidade com a responsabilidade ou autoridade para gerenciar riscos de segurança da informação;

XV - identificação de riscos: processo para localizar, listar e caracterizar elementos do risco;

XVI - reduzir risco: forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

XVII - reter risco: forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

XVIII - riscos de segurança da informação e comunicações: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XIX - risco residual ou risco retido: risco remanescente após tratamento do risco;

XX - transferir risco: forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

XXI - tratamento dos riscos: processo de implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

XXII - 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; e

XXIII - análise/avaliação de riscos: processo completo de análise e avaliação de riscos.

Art. 3º A implementação da GRSIC está alinhada ao modelo denominado PDCA (Plan-Do-Check-Act), conforme definido na Norma Complementar nº 02/DSIC/GSIPR, publicada no Diário Oficial da União nº 199, Seção 1, de 14 de outubro de 2008, de modo a fomentar a sua melhoria contínua.

CAPITULO II

DO PROCESSO DE GRSIC

Art. 5º O processo de GRSIC deve considerar:

I - todos os ativos de informação classificados como vitais e críticos para a realização das atividades fins do Ministério da Saúde; e

II - os objetivos estratégicos, os processos de negócio, os requisitos legais, a estrutura organizacional e a Política de Segurança da Informação e Comunicações do Ministério da Saúde, e

III - a metodologia de GRSIC, que deverá atender aos objetivos, diretrizes gerais e o escopo definido contemplando, no mínimo, os critérios de avaliação e de aceitação do risco.

Art. 6º Cabe ao Gestor de Segurança da Informação e Comunicações do Ministério da Saúde, no âmbito de suas atribuições, coordenar o processo de GRSIC.

Art. 7º O processo de GRSIC será estruturado e realizado em ciclos anuais, compreendendo as seguintes etapas:

I - definições preliminares;

II - análise e avaliação dos riscos;

III - plano de tratamento dos riscos;

IV - aceitação dos riscos;

V - implementação do Plano de Tratamento dos Riscos;

VI - monitoramento e análise crítica;

VII - melhoria do processo de GRSIC; e

VIII - comunicação.

Art. 8º Na etapa definições preliminares serão realizadas as seguintes atividades:

I - realização de análise do órgão a fim de identificar os critérios e o enfoque mais apropriado, apoiando-se na definição do escopo e na adoção de uma metodologia; e

II - definição de escopo delimita o âmbito de atuação da GRSIC, podendo abranger o órgão, uma unidade, um processo, um sistema, um recurso ou um ativo de informação.

Art. 9º Na etapa de análise e avaliação dos riscos serão realizadas as seguintes atividades:

I - identificação dos riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação para, em seguida, serem estimados os níveis de riscos de modo que eles sejam avaliados e priorizados;

II - identificação dos ativos e seus respectivos responsáveis dentro do escopo estabelecido e conforme a Política de Segurança da Informação e Comunicações e a legislação pertinente;

III - identificação dos riscos associados ao escopo definido, considerando:

a) ameaças envolvidas;

b) vulnerabilidades existentes nos ativos de informação;

c) ações de Segurança da Informação e Comunicações (SIC) já adotadas;

d) fontes de risco;

e) áreas de impactos;

f) eventos (incluindo mudanças nas circunstâncias);

g) causas; e

h) consequências potenciais;

IV - realização de estimativa dos riscos levantados, considerando os valores ou níveis para a probabilidade e para a consequência do risco associados à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados;

V - avaliação dos riscos, determinando se são aceitáveis ou se requerem tratamento, comparando a estimativa de riscos com os critérios estabelecidos; e

VI - relacionamento dos riscos que requeiram tratamento, priorizando-os de acordo com os critérios estabelecidos pelo órgão ou entidade.

Art. 10. Na etapa plano de tratamento dos riscos serão realizadas as seguintes atividades:

I - determinação das formas de tratamento dos riscos, considerando as opções de reduzir, evitar, transferir, compartilhar ou aceitar o risco observando:

a) a avaliação do tratamento de riscos já realizado;

b) a eficácia das ações de Segurança da Informação e Comunicações - SIC já existentes;

c) a avaliação da eficácia desse tratamento;

d) as restrições organizacionais, técnicas e estruturais;

e) os requisitos legais; e

f) a análise de custo-benefício; e

II - avaliação e decisão quanto aos níveis de risco residual, se não forem toleráveis, deve-se definir a implementação de um novo tratamento para os riscos.

Parágrafo único. O plano para o tratamento dos riscos será formulado, relacionando, no mínimo:

I - razões para a seleção das opções de tratamento, incluindo os benefícios que se espera obter;

II - responsáveis pela aprovação do plano e os responsáveis pela implementação do plano;

III - ações de SIC propostas;

IV - prioridades e prazos de execução necessários à sua implantação;

V - os recursos requeridos, incluindo contingências;

VI - medidas de desempenho e restrições;

VII - requisitos para a apresentação de informações e de monitoramento; e

VIII - cronograma e programação.

Art. 11. Na etapa de aceitação dos riscos será realizada análise dos resultados do processo de análise e avaliação dos riscos, considerando o plano de tratamento, aceitando-os ou submetendo-os à nova avaliação.

Art. 12. Na etapa de implementação do plano de tratamento dos riscos serão executadas as ações e medidas de controles de SIC incluídas no Plano de Tratamento dos Riscos.

Art. 13. A etapa de monitoramento e análise crítica tem por objetivo detectar possíveis falhas nos resultados, por meio da avaliação:

I - dos riscos;

II - das ações de SIC; e

III - da eficácia do processo de GRSIC.

§ 1º O monitoramento e análise crítica dos riscos verificará regularmente, no mínimo, as mudanças:

I - nos critérios de avaliação e aceitação dos riscos;

II - no ambiente;

III - nos ativos de informação;

IV - nas ações de SIC; e

V - nos fatores do risco, tais como ameaça, vulnerabilidade, probabilidade e impacto.

§ 2º O monitoramento e análise crítica da eficácia do processo de GRSIC será realizada por meio da análise do seu alinhamento às diretrizes gerais estabelecidas e às necessidades do Ministério da Saúde;

§ 3º As responsabilidades relativas ao monitoramento e à análise crítica devem ser claramente definidas.

§ 4º Os resultados serão registrados e divulgado internamente para avaliação e, quando couber, externamente para conhecimento, sendo utilizados como entrada para a análise crítica da estrutura de Gestão de Riscos de Segurança da Informação e Comunicações.

Art. 14. A etapa de melhoria do processo de GRSIC tem por objetivo:

I - informar ao Gestor de Segurança da Informação e Comunicações a necessidade de implementação de melhorias identificadas na etapa de monitoramento e análise crítica; e

II - executar as ações corretivas e preventivas aprovadas e assegurar que as melhorias atinjam os objetivos pretendidos.

Art. 15. A etapa de comunicação será permanente, mediante a consulta às partes interessadas durante todas as fases do processo de GRSIC, objetivando:

I - manter as instâncias superiores informadas a respeito de todas as fases da gestão de risco, compartilhando as informações entre o tomador da decisão e as demais partes envolvidas e interessadas;

II - assegurar que os responsáveis pela implementação do processo de GRSIC e as partes interessadas compreendam os fundamentos sobre os quais as decisões são tomadas e as razões pelas quais ações específicas são requeridas; e

III - abordar questões relacionadas com o risco, suas causas e consequências e medidas tomadas para tratá-lo.

Parágrafo único. Os planos de comunicação e consulta serão desenvolvidos em estágio inicial do processo de GRSIC.

CAPITULO II

DAS DISPOSIÇÕES FINAIS

Art. 16. Todos os setores do Ministério da Saúde devem adotar a Gestão de Riscos de Segurança da Informação e Comunicações nos seus processos de trabalho, considerando a Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações estabelecida e ajustada para as atividades que desempenha.

Parágrafo único. A GRSIC está limitada às ações e medidas de proteção dos ativos que sustentam os produtos e serviços do Ministério da Saúde.

Art. 17. A GRSIC deverá produzir subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações - SGSI e a Gestão de Continuidade de Negócios - GCN.

Art. 18. A GRSIC será executada ao menos uma vez ao ano e sempre que houver mudanças significativas nos ativos de informação de cada área de negócio.

ANEXO A

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

ANEXO VI

USO DE DISPOSITIVOS MÓVEIS NO ÂMBITO DO MINISTÉRIO DA SAÚDE

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Este Anexo estabelece diretrizes e orientações básicas para uso e manuseio dos dispositivos móveis no âmbito do Ministério da Saúde.

Parágrafo único. As ações deste Anexo deverão observar:

I - a Norma complementar 12/IN01/DSIC/GSIPR de 30 de janeiro de 2012 - Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal (APF); e

II - a Portaria GM/MS nº 271, de 27 de janeiro de 2017 - Política de Segurança da Informação e Comunicações do Ministério da Saúde (POSIC/MS).

Art. 2º Para fins deste Anexo, consideram-se as seguintes definições:

I - dispositivos móveis: equipamentos portáteis com capacidade computacional de processamento, tais como notebooks, smartphones, tablets, entre outros;

II - dispositivos móveis corporativos: dispositivos móveis de propriedade do Ministério da Saúde;

III - dispositivos móveis particulares: dispositivos móveis de propriedade do agente público ou de empresa prestadora de serviço; e

IV - usuário visitante: agente público ou não que utiliza dispositivos móveis de sua propriedade para acessar a Internet do Ministério da Saúde.

CAPITULO II

DAS DIRETRIZES GERAIS

Art. 3º O uso de dispositivos móveis por agentes públicos nas dependências do Ministério da Saúde somente será realizado para os interesses de negócio da instituição.

Art. 4º A exceção dos casos previstos em contratos firmados com o Ministério da Saúde, ao agente público ou visitante não é permitido o uso de dispositivo móvel particular para acessar à rede do Ministério da Saúde.

Parágrafo único. Os dispositivos móveis particulares que necessitarem de acesso à rede do Ministério da Saúde devem se submeter aos padrões corporativos de software e aos controles de segurança estabelecidos pelo DATASUS.

Art. 5º É vedada a instalação de aplicativos ou recursos que não homologados pelo DATASUS em dispositivos móveis corporativos do Ministério da Saúde.

CAPITULO III

DOS PROCEDIMENTOS

Art. 6º O uso de dispositivos móveis corporativos no âmbito do Ministério da Saúde deve observar os seguintes procedimentos:

I - os dispositivos móveis fornecidos pelo Ministério da Saúde devem:

a) ter sua utilização autorizada por agente responsável; e

b) ser cadastrados conforme procedimento formal, de modo a garantir a identificação única do dispositivo e a identificação do agente público responsável pelo uso;

c) ser de utilização única e exclusiva do agente público que assumir a responsabilidade pelo seu uso;

II - implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis; e

III - orientação dos agentes públicos, por área responsável, quanto aos procedimentos de segurança da informação acerca dos dispositivos que lhes forem disponibilizados.

§ 1º É obrigatória a assinatura do termo de responsabilidade de uso de equipamento do Ministério da Saúde de que trata o Anexo A, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido.

§ 2º É recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados e informações classificadas armazenados nos dispositivos móveis.

Art. 7º O uso de dispositivos móveis particulares para visitantes deve observar os seguintes procedimentos:

I - os dispositivos móveis que não são de propriedade do Ministério da Saúde não poderão fazer uso da rede corporativa, permitido somente o acesso à internet, por meio de rede específica para visitante;

II - procedimentos para controle e concessão de acesso com a autenticação, autorização e registro de acesso do usuário, serão aplicados aos visitantes que necessitarem acessar a internet com seus dispositivos móveis particulares durante a permanência nas dependências do Ministério da Saúde;

III - a concessão de uso deve estar vinculada à concordância do usuário às normas internas de uso deste serviço, seguindo os critérios estabelecidos pelo Ministério da Saúde; e

IV - a permissão de uso poderá ser revogada, sem prévio aviso, caso seja identificada alguma não conformidade com as regras de segurança da informação e comunicações estabelecidas pelo Ministério da Saúde.

Art. 8º O uso de dispositivos móveis particulares por agente público deve observar os seguintes procedimentos:

I - a utilização do dispositivo móvel particular como corporativo será permitido desde que previsto ou sob o amparo de contrato firmado com o Ministério da Saúde e autorizado por chefia imediata;

II - o dispositivo móvel particular, após ser submetido aos padrões corporativos da rede, estará em conformidade com os padrões corporativos do Ministério da Saúde; e

III - o agente público que autorizado a utilizar o dispositivo móvel particular e que esteja em conformidade com os padrões corporativos, após conferencia realizada por equipe técnica responsável, deverá assinar o Termo de Responsabilidade constante no Anexo B.

Parágrafo único. Os procedimentos para autorização de uso de dispositivo móvel particular, para interesses da instituição, são de responsabilidade do DATASUS.

CAPITULO IV

DISPOSIÇÕES FINAIS

Art. 9º O Subcomitê Gestor de Segurança da Informação e Comunicações - SGSIC, com auxílio do Comitê de Informação e Informática em Saúde - CIINFO, terá a responsabilidade revisar periodicamente as normas deste Anexo.

ANEXO A

TERMO DE RESPONSABILIDADE DE USO DE EQUIPAMENTOS CORPORATIVOS DO MINISTÉRIO DA SAÚDE

Pelo presente instrumento, eu _____, CPF_____, identidade _____, órgão expedidor _____, lotado _____, declaro, sob pena das sanções cabíveis nos termos da legislação vigente, ter recebido o(s) equipamento(s) abaixo discriminado(s) para uso e desempenho das minhas funções profissionais, sendo responsável pelo seu uso e guarda.

Declaro ainda estar ciente que, em caso de perda ou dano no equipamento, deverei ressarcir o Ministério da Saúde, salvo prova inequívoca de ausência de dolo ou culpa.

Assumo ainda a responsabilidade por:

1) zelar e tratar o(s) ativo(s) de informação como patrimônio do Ministério da Saúde;

2) utilizar as informações sob minha custódia, exclusivamente, no interesse do serviço do Ministério da Saúde;

3) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Política de Segurança da Informação e Comunicações do Ministério da Saúde;

4) utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Ministério da Saúde; e

5) responder, perante o Ministério da Saúde, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Item	Equipamento	Marca/Modelo	Patrimônio	Nº de Série	Periféricos

Local, ___de _____de _____.

_____

Nome do agente responsável

Setor organizacional

_____

Nome do agente público

Setor organizacional

ANEXO B

TERMO DE RESPONSABILIDADE DE USO DE EQUIPAMENTOS PARTICULARES

Pelo presente instrumento, eu _____, CPF_____, identidade _____, órgão expedidor _____, declaro, sob pena das sanções cabíveis nos termos da legislação vigente, ter autorizado a equipe técnica do Ministério da Saúde a aplicar no(s) equipamento(s) de minha propriedade abaixo discriminado(s), os padrões corporativos, de modo a utiliza-lo(s) para uso e desempenho das minhas funções profissionais nas instalações do Ministério da Saúde.

Assumo, ainda, a responsabilidade por:

1) zelar e tratar o(s) ativo(s) de informação como patrimônio do Ministério da Saúde;

2) utilizar as informações sob minha custódia, exclusivamente, no interesse do serviço do Ministério da Saúde;

3) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Política de Segurança da Informação e Comunicações do Ministério da Saúde;

4) utilizar as credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Ministério da Saúde; e

5) responder, perante o Ministério da Saúde, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Item	Equipamento	Marca/Modelo	Nº de Série	Periféricos

Local, ___de _____de _____.

_____

Nome do responsável pelo equipamento

Empresa Prestadora de Serviço