METODOLOGIA
DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO MINISTÉRIO DA SAÚDE

SUMÁRIO

GLOSSÁRIO

Ameaça – Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

Ativos de Informação – 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;

Controle – ação, medida ou dispositivo utilizado para tratar o risco;

Estimativa de riscos – Processo utilizado para atribuir valores à probabilidade e consequências de um risco;

Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) – Conjunto de processos que permitem 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;

Impacto - Consequência de um incidente de segurança sobre os Ativos e negócios da Organização. Pode ser tangível (exemplo: perdas financeiras) ou intangível (exemplo: perda de credibilidade). Corresponde ao produto S (Severidade) x R (Relevância do Ativo).

Probabilidade - Grau de possibilidade de que uma ou mais vulnerabilidades (na falta de Controles) existentes num Ativo venham a ser exploradas por Ameaças, causando um incidente de segurança.

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;

Segurança da Informação - Preservação da confidencialidade, integridade e disponibilidade da informação.

Serviços – Considera-se serviço como sendo toda a infraestrutura de base tecnológica e os meios de acesso às informações de saúde.

Severidade - Medida do grau em que um Ativo será afetado, caso as ameaças explorem a(s) vulnerabilidade(s) nos aspectos Confidencialidade, Integridade e Disponibilidade.

Sistemas - Componentes ou processos de alto nível de elevada importância estratégica ou que possuem algum outro atributo merecedor de tratamento diferenciado dos demais processos do MS/DATASUS por parte do executivo.

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.

APRESENTAÇÃO

Este documento apresenta a metodologia proposta para a Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC do Ministério da Saúde, abrangendo todos os seus ativos de Informação.

É importante lembrar que antes de desenvolver um Plano de Gestão dos Riscos de Segurança da Informação e Comunicações (processo de identificar e tratar os riscos da organização de forma sistemática e contínua), as áreas devem estar em conformidade com a Política de Gestão de Risco de Segurança da Informação e Comunicações e também com o processo apresentado nesta metodologia.

Para efeito desta metodologia utilizaremos o termo gestão de risco no seu sentido mais estrito, referindo-se ao risco de segurança da informação e comunicações e não na sua acepção mais ampla do risco coorporativo.

1. INTRODUÇÃO

É função do Ministério da Saúde dispor de todas as condições para a promoção, proteção e recuperação da saúde da população, reduzindo as enfermidades, controlando as doenças endêmicas e parasitárias, melhorando a vigilância à saúde e dando qualidade de vida ao brasileiro.

Devido a estas atribuições, o Ministério da Saúde impõe-se o desafio de garantir o direito do cidadão ao atendimento à saúde e prover condições para que esse direito esteja ao alcance da população, independente da condição social.

Tendo como base que a informação é fundamental para a democratização da Saúde e o aprimoramento de sua gestão, a informatização das atividades do Sistema Único de Saúde (SUS), dentro das diretrizes tecnológicas adequadas, é essencial para a descentralização das atividades de saúde, viabilização e controle social sobre a utilização dos recursos disponíveis.

Para alcançar tais objetivos, foi atribuída ao Departamento de Informática do SUS - DATASUS, criado pelo Decreto 100 de 16.04.1991, a responsabilidade de coletar, processar, prover e disseminar informações sobre saúde, além de representar papel importante como centro tecnológico de suporte técnico e normativo sobre a Gestão de Segurança da Informação para a montagem dos sistemas de informática e informação da Saúde.

Por meio do processo de GRSIC, os riscos a que estão submetidas as informações do MS podem ser identificados, e as possíveis ameaças e vulnerabilidades tratadas de forma adequada por meio da implementação das medidas de proteção necessárias, organizadas de forma estratégica em planos de tratamento, de modo a minimizar os possíveis prejuízos ao MS.

2. ABRANGÊNCIA

Entretanto, cabe ressaltar que o DATASUS não é a única área do MS a tratar, armazenar e divulgar informações de Saúde, motivo pelo qual torna-se preponderante o estabelecimento da Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, que tenha alcance em todas as áreas do MS.

A Metodologia de GRSIC se aplica as áreas do Ministério da Saúde que tenham a responsabilidade de gerar, coletar, processar, armazenar, prover e disseminar informações sobre saúde.

É importante frisar que a GRSIC não se aplica somente a tecnologia e sim a qualquer outro tipo de ativo de informação: pessoas, processos e ambientes.

3. METODOLOGIAS

A metodologia proposta para a Gestão de Riscos utiliza como base as seguintes normas: ISO/IEC GUIDE 73, a ABNT NBR ISO/IEC 27005:2008 e as Normas Complementares - NC 02 e NC 04 do Gabinete de Segurança Institucional da Presidência da Republica.

3.1. ABNT NBR ISO/IEC GUIDE 73

Norma genérica que fornece um vocabulário básico para desenvolver entendimentos comuns sobre a Gestão de Riscos.

3.2. ABNT NBR ISO/IEC 27005:2008

Norma brasileira que fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização. Nela estão contempladas apenas diretrizes que devem ser utilizadas pelas organizações para definir uma abordagem do processo de gestão de riscos adequada ao seu negócio.

3.3. NC 02 GSI/PR

Norma Complementar do Gabinete de Segurança Institucional da Presidência da República que define a metodologia de Gestão de Segurança da Informação e Comunicações a ser utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Essa norma traz as melhores práticas no gerenciamento de riscos por meio do processo de melhoria contínua estabelecido pela norma ABNT NBR ISO/IEC 27001:2006, e denominado ciclo “PDCA” (Plan-Do-Check-Act). PLANEJAR → FAZER → VERIFICAR → AGIR.

3.4. NC 04 GSI/PR

Norma complementar do Gabinete de Segurança Institucional da Presidência da República que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos ou entidades da Administração Pública Federal, direta e indireta.

O processo de Gestão de Riscos de Segurança da Informação e Comunicações deve estar alinhado ao modelo PDCA de modo a fomentar a sua melhoria contínua.

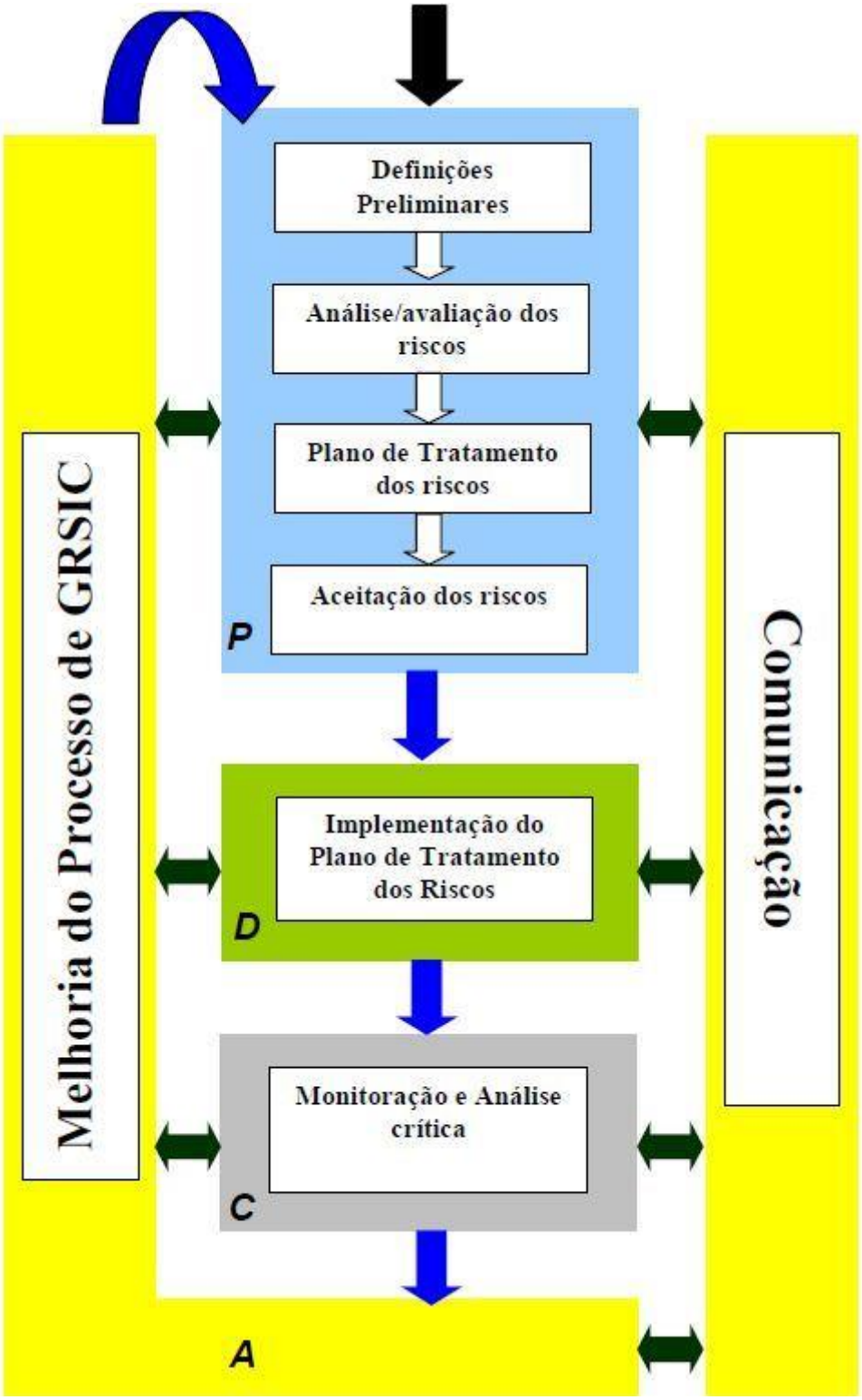


Figura 1 - PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES NC 04 GSI/PR

4. METODOLOGIA PROPOSTA

Foram considerados quatro critérios para a escolha da metodologia:

a) Simplicidade no modelo de gestão.

b) Coerência com as práticas de qualidade adotadas na Administração Pública Federal.

c) Compatibilidade com a prática de Gestão de Segurança da Informação em uso no MS.

d) Flexibilidade. Todas as etapas do ciclo de Gestão de Riscos podem ser aplicadas aos vários níveis da organização: estratégico, tático e operacional.

A Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Ministério da Saúde adota o ciclo composto pelas quatro etapas apresentadas na Política de Gestão de Riscos de Segurança da Informação e Comunicações, alinhado ao PDCA. Esse processo é composto pelas etapas: definições preliminares; inventariar; analisar; avaliar; tratar os riscos; monitoração, comunicação do risco e análise crítica, que objetiva a melhoria do processo de GRSIC.

4.0. Comunicar Áreas Envolvidas

Recebida uma solicitação para que se proceda a gestão de risco de um determinado escopo, a primeira atividade a ser executada é a comunicação das áreas e pessoas envolvidas, a data de início dos trabalhos, os prazos, custos, pessoas envolvidas e resultados esperados.

4.1. Definições Preliminares

Nesta fase ocorre a definição e detalhamento do escopo ou contexto de aplicação da GRSIC a fim de delimitar o âmbito de atuação. O escopo

pode ser o Ministério da Saúde como um todo, uma estrutura funcional, um processo, sistema, recurso ou determinado ativo. Também devem ser definidos os prazos (cronograma), custos, pessoas envolvidas e resultados esperados. Estas informações devem ser comunicadas às áreas e pessoas envolvidas já no início dos trabalhos.

De modo a otimizar o ciclo de Gestão de Riscos, toda Análise de Riscos do MS deve ser criada como projeto, ter escopo definido e possuir um grupo de responsável (eis). Por esse método, os processos de avaliação, tratamento e comunicação tornam-se mais simples, práticos e rápidos.

4.2. Inventariar

Esta etapa corresponde ao conjunto de ações necessárias para levantamento, detalhamento e estruturação dos componentes de negócio, das ameaças e dos ativos (processos, tecnologias, ambientes e pessoas) que podem impactar os objetivos, missão ou atividades finalísticas do MS.

Para que a execução do ciclo de gestão de riscos seja realizada de acordo com os objetivos estratégicos, é necessário que todos os ativos sob o escopo sejam inventariados. Essa atividade pode ser executada por meio de reuniões entre as equipes envolvidas. A partir disso, é necessário que os ativos e suas características (incluindo suas interdependências) sejam cadastrados em sistema específico de gestão de riscos. Essa lista de ativos deve ser revalidada ao final da atividade, garantindo que o escopo possui todos os ativos necessários para indicar os índices de riscos corretos.

Tipo do Ativo	Descrição
Tecnologia	Ativos de conectividade (Switch, roteador, Hub, etc.), servidores, estações de trabalho, computação móvel e outros equipamentos (telefones celulares, tablet, etc.). Também se inserem neste tipo, qualquer software que esteja dentro de servidores ou computadores, podendo ser Sistema Gerenciador de Banco de Dados, Servidores de WEB, sistemas operacionais e aplicativos específicos.
Pessoas	Podem ser usuários, gerentes, administradores de rede, analistas de sistemas, etc.

Ambientes	Ambientes críticos ou sensíveis ao negócio. Podem ser salas de servidores, Data centers, salas/escritórios ou ambientes de produção.
Processos	Práticas e Processos críticos ou sensíveis ao negócio. Podem ser processos de planos de contingência, processo de política de segurança, etc. Processos identificados pelo conjunto de atividades, insumos e resultados de uma área ou departamento.

Tabela 1 - Tipificação dos ativos

Após definir os ativos no escopo, deve-se identificar as ameaças, vulnerabilidades, probabilidades e criticidade dos ativos, de acordo com os objetivos de negócio ou particularidades das áreas, departamentos, sistemas ou processos.

4.3. Análise de Riscos

O método sugerido para a execução das análises de riscos é composto pela criação de questionários ou checklists que contenham as particularidades para cada um dos ativos do escopo. Os questionários devem ser capazes de identificar as ameaças e vulnerabilidades associadas a cada ativo de informação, a probabilidade de ocorrência das ameaças, a severidade dos possíveis danos associados, assim como a relevância do ativo de informação para o escopo em análise.

Durante a fase de Análise, se obtém a estimativa de Risco a que está submetido cada ativo, pelo produto dos seguintes atributos:

Probabilidade da vulnerabilidade ser explorada por uma ameaça;

Severidade das consequências da vulnerabilidade ser explorada

Relevância, que significa o grau de impacto do Ativo ser afetado por uma ameaça, o quão importante é o ativo para o escopo em análise. A relevância deve ser atribuída durante o levantamento dos ativos. Ela é obtida do cadastro de ativos e corresponde ao atributo “valor” do ativo.

As Tabelas 2, 3 e 4 a seguir apresentam as escalas de valores para os fatores: Probabilidade, Severidade e Relevância. Os valores variam de 1 a 5 em função do grau muito baixo a muito alto dos fatores.

Probabilidade

GRAU	A vulnerabilidade pode ser explorada por uma ameaça	VALOR
Muito alto	É quase certa (P > 95%)	5
Alto	É muito provável (65% < P < 95%)	4
Médio	É provável (35% < P < 65%)	3
Baixo	É pouco provável (5% < P < 35%)	2
Muito baixo	É improvável (P <5%)	1

Tabela 2 - explicativa da pontuação da Probabilidade.

Severidade

GRAU	Consequência para o Ativo caso a vulnerabilidade seja explorada pela ameaça	VALOR
Muito alto	Afeta extremamente o ativo	5
Alto	Afeta muito gravemente o ativo	4
Médio	Afeta gravemente o ativo	3
Baixo	afeta pouco o ativo	2
Muito baixo	Quase não afeta o ativo	1

Tabela 3 - explicativa da pontuação da Severidade.

Relevância - Quão importante é o Ativo

GRAU	Se o Ativo for comprometido:	VALOR
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

Tabela 4 – explicativa da pontuação da Relevância.

PSR = Probabilidade x Severidade x Relevância - os fatores da Probabilidade e Severidade são pontuados durante as análises técnicas e a Relevância pontuada no processo de levantamento dos ativos, considerando-se a importância do ativo para o negócio ou serviço.

Assim, o valor do risco de um ativo é obtido pelo somatório dos produtos dos três fatores (**P x S x R)** calculado cada uma das ameaças ao ativo em análise.

O histórico das análises deve ser preservado para que se possa verificar a evolução na aplicação dos controles dos ativos.

Após a análise de riscos nos ativos do escopo, é necessário que os resultados sejam consolidados de forma a auxiliar o entendimento sobre as ameaças às quais os objetivos estratégicos estão sujeitos, com maior ou menor probabilidade de ocorrência. Essa consolidação deve considerar as interdependências entre ativos, sistemas e processos, de acordo com o escopo ou contexto definido. Também é necessário que as possíveis pendências sejam avaliadas e registradas como entrada para o próximo ciclo de análise crítica e melhoria do processo de gestão integrada.

Ao consolidar os resultados, torna-se necessário que sejam gerados relatórios contendo histórico de execução, resultados obtidos, ameaças mais significativas, índices de riscos por ativo, priorização de controles e sugestões de correção.

A Análise contribui para as decisões estratégicas sobre os riscos e sobre a forma mais adequada e economicamente viável de tratamento.

A tabela 5 a seguir traz um exemplo de análise de risco de TIC.

Sistema	Ativo	Ameaças	Vulnerabilidade	Probabilidade	Severidade	Relevancia	Grau de Risco	Controle/Ação
SNT	Servidor WEB	Ataque de Hackers	Bugs	2	4	5	40	Manter sistema operacional atualizado
		Sobrecarga de Energia	Energia não estabilizada	2	5	5	50	aquisição de nobreak/estabilizador
	Estações de Trabalho	Queima de Fonte	Energia não estabilizada	2	4	1	8	
	Operadores	acesso indevido	vazamento de senha	3	5	5	75	controle biométrico / uso de certificado digital
SISREG	Servidor WEB	Ataque de Hackers	Bugs	3	4	5	60	Manter sistema operacional atualizado
		Sobrecarga de Energia	Energia não estabilizada	2	5	5	50	aquisição de nobreak/estabilizador
	Estações de Trabalho	Queima de Fonte	Energia não estabilizada	3	4	1	12	
	Operadores	acesso indevido	vazamento de senha	3	5	5	75	controle biométrico / uso de certificado digital

Tabela 5 – Análise de Risco de TIC

4.4. Avaliação dos Riscos

Definido como o processo de comparar o risco, previamente identificado e estimado na fase de Análise, com critérios de risco predefinidos para determinar a importância do risco.

O objetivo da Avaliação de Riscos é tomar decisões sobre qual risco necessita de tratamento ou aceitação, bem como sua prioridade, com base nos resultados obtidos na Análise de Riscos.

As decisões estratégicas devem considerar o contexto mais amplo do risco, incluindo o exame de quão tolerável são os riscos a serem assumidos. Para isso, com as informações sobre os processos de negócio da organização e os ativos que os suportam, deve-se:

a) Priorizar os riscos – os ativos que possuírem os maiores níveis de risco (PSR) serão priorizados em termos de recursos e proteções.

b) Ter maior conhecimento sobre os riscos e avaliar as melhores soluções de proteção, considerando seu custo-benefício.

4.5. Tratamento dos Riscos

As formas de tratamento dos riscos consistem em reduzir, evitar, transferir ou reter o risco, observando:

a) A eficácia das ações de Segurança da Informação e Comunicações já existentes;

b) As restrições organizacionais, técnicas e estruturais;

c) Os requisitos legais; e

d) A análise custo/ benefício.

Reduzir o risco – implantar controles de proteção que reduzam o risco do ativo.

Evitar o 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;

Transferir o risco – é a decisão de compartilhar os riscos com outras entidades. A implantação do tratamento pode ser feita por um seguro que cubra as consequências, ou pela mudança do ativo para outro local ou empresa que cubra eventuais prejuízos.

Reter o risco (aceitar) – não há implantação de controles, caso o nível do risco atenda aos critérios de aceitação do risco.

O tratamento do risco pode ser iniciado quando nas fases de análise e avaliação forem fornecidas informações suficientes para determinar as ações necessárias para reduzir os riscos a níveis aceitáveis. Esta fase envolve a identificação dos controles previamente avaliados, além da preparação e implantação das ações em planos de tratamento. Esses planos visam à redução dos riscos para os níveis aceitáveis e podem ter opções no tratamento de eventos internos e externos.

Na gestão de tratamento dos riscos avaliados é importante estabelecer critérios para priorizar o tratamento dos riscos, considerando a tabela PSR.

A tabela 6 a seguir representa os valores possíveis para o produto dos fatores Severidade x Relevância:

Severidade						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Relevância				

Tabela 6 - Possíveis valores do produto Severidade X Relevância

Estes valores possíveis são agora multiplicados pelo fator probabilidade, obtendo-se a tabela 7 a seguir, que demonstra a distribuição dos possíveis valores de Risco (**PSR**):

Probabilidade															
	5	5	10	15	20	25	30	40	45	50	60	75	80	100	125
	4	4	8	12	16	20	24	32	36	40	48	60	64	80	100
	3	3	6	9	12	15	18	24	27	30	36	45	48	60	75
	2	2	4	6	8	10	12	16	18	20	24	30	32	40	50
	1	1	2	3	4	5	6	8	9	10	12	15	16	20	25
SxR		1	2	3	4	5	6	8	9	10	12	15	16	20	25
		Severidade x Relevância													

Tabela 7 - Possíveis valores do produto Probabilidade X Severidade X Relevância

Da tabela anterior são identificadas e definidas as faixas para os níveis de risco que irão orientar a priorização da faze de tratamento dos riscos, priorizando o tratamento dos riscos mais altos, conforme a Tabela 8 a seguir.

NÍVEL RISCO	PSR	%
Muito Alto	DE 60 a 125	40 < NR <=100
Alto	de 32 a 50	24< NR <= 40
Médio	de 15 a 30	9,6< NR <=24
Baixo	de 06 a 12	4 < NR <=9,6
Muito Baixo	de 01 a 05	NR<= 4

Tabela 8 – Critério de Risco - Prioridade para Tratamento de Riscos

Considerando-se que o cálculo do índice PSR representa o risco associado à ausência de um controle, quanto maior o índice PSR, maior a ausência de controle e consequentemente o grau de risco.

CRITÉRIOS PARA ACEITAÇÃO DO RISCO

Conforme recomendação da Norma Complementar, NC 02/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações, do Gabinete de Segurança Institucional da Presidência da República, o Ministério da Saúde deve identificar os níveis de riscos aceitáveis e os critérios para sua aceitação, considerando as decisões da direção e o seu planejamento estratégico.

Como risco aceitável, o Ministério da Saúde considera os níveis que apresentarem PSR Baixo ou Muito Baixo. Portanto, deverão ser tratados os riscos Muito Alto, Alto e Médio, cabendo ao Gestor da área analisar os casos especiais, nos quais a aceitação do risco é justificável. Podem ser entendidos como casos especiais, dentre outros, as atividades temporárias ou de curto prazo; a implantação de controles cujo custo supera o valor da consequência causada pela ocorrência do evento.

4.5.1. Plano de Tratamento de Riscos

Juntamente com o relatório de riscos residuais ou aceitos, deve ser criado um plano de tratamento com as sugestões de controles para a minimização dos riscos provenientes dos controles identificados nas análises como não implantados ou aplicados. O plano de tratamento deve incluir estimativas de custos, impactos nas atividades cotidianas, procedimentos necessários e prazos. Essa categorização auxilia tanto o gestor quanto o técnico especialista na priorização das ações de implantação dos controles analisados.

4.5.2. Aprovação do Plano de Tratamento de Riscos

O plano de tratamento deve ser aprovado pela alta gestão ou gestor dos ativos que definirá ou ajustará as atividades de acordo com as restrições que porventura existam, como orçamento disponível ou priorização de atividades externas à gestão de riscos. Com isso, será atualizado o plano

com as devidas justificativas para a não implantação dos controles sugeridos, assim como atualizará também os relatórios de riscos residuais ou aceitos na mesma proporção.

4.5.3. Execução do Plano de Tratamento de Riscos

Executar o Plano de Tratamento significa a implantação dos controles selecionados para cada ativo, de acordo com suas particularidades, características e tipos de ativos – tecnológicos, ambientais, humanos ou processuais.

4.6. Monitoração

Esta fase tem como objetivo detectar possíveis falhas nos resultados, verificando a eficácia do processo de Gestão de Riscos de Segurança da Informação e Comunicações.

4.7. Análise Crítica

Devem ser analisados os artefatos do projeto (relatórios) em todas as fases do processo de GRSIC, de forma a mantê-los alinhados às diretrizes gerais estabelecidas.

Os riscos devem monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças:

a) Nos critérios de avaliação e aceitação dos riscos;

b) No ambiente;

c) Nos ativos de informação;

d) Nas ações de Segurança da Informação e Comunicações;

e) Nos fatores do risco (ameaça, vulnerabilidade, probabilidade e severidade).

4.8. Melhoria do Processo de GRSIC

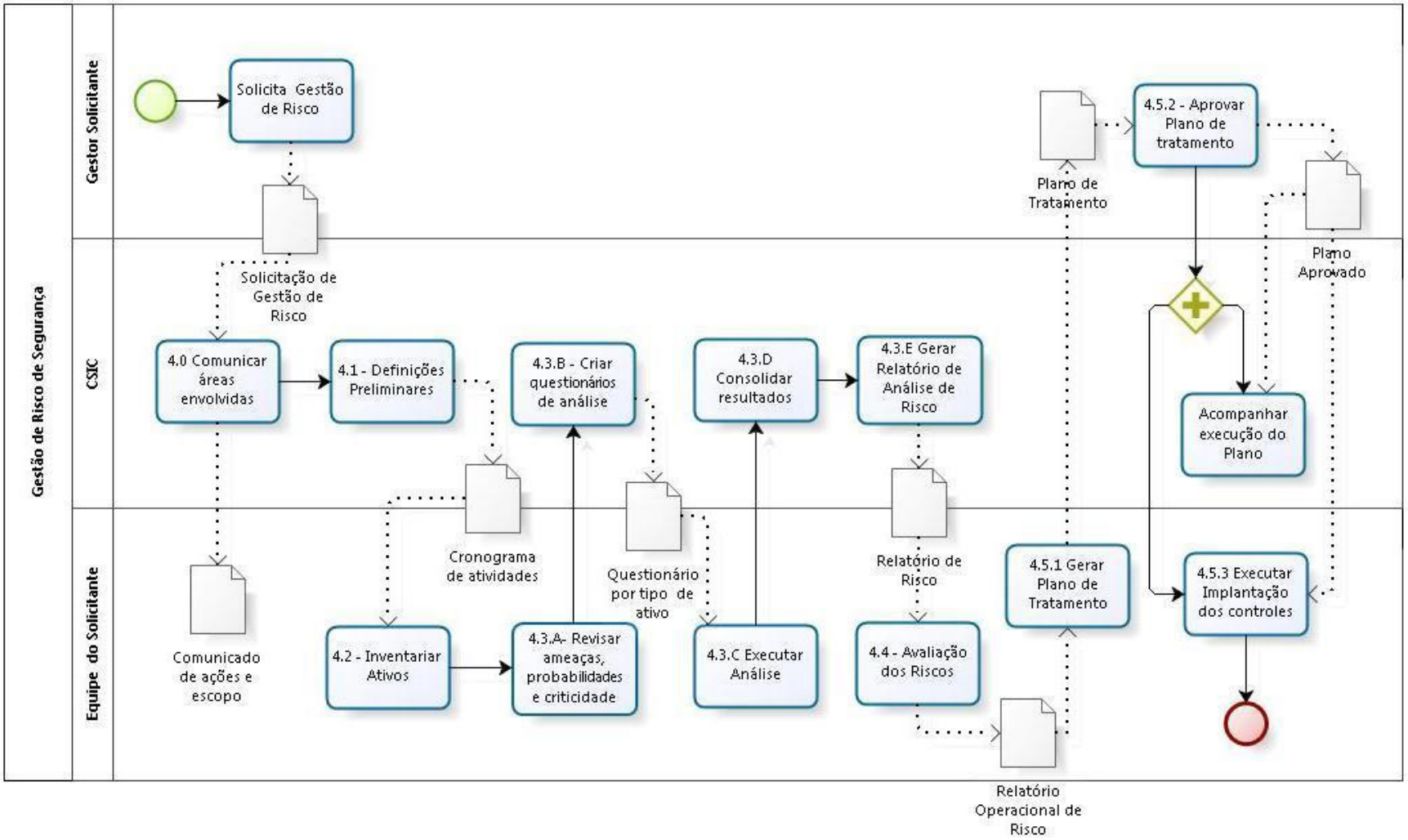
Após monitoração e análise crítica do Processo de GRSIC, as considerações deverão ser propostas à gestão de Segurança da Informação e Comunicações do MS para avaliação e consideração a fim de implantar as melhorias no Processo.

5. CONSIDERAÇÕES FINAIS

A Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações, apresentada neste documento, deve complementar os processos de Gestão de Segurança da Informação e Comunicações, previstos na IN 01 GSI, de 13 de junho de 2008.

O Ministério da Saúde já dispõe de uma ferramenta informatizada para a Gestão de Riscos de Segurança da Informação e Comunicações, que é operacionalizada pelo DATASUS e que está disponível para uso em todo o MS. Entretanto, esta metodologia não se restringe ao uso da ferramenta informatizada.

ANEXO: Processo de Gestão de Riscos



Atividade	**4.0. Comunicar áreas envolvidas**
Descrição	Comunicar as áreas e pessoas envolvidas no escopo sobre as atividades a serem executadas, incluindo período de execução, resultados esperados e custos (opcional).
Responsável	Comunicar áreas envolvidas: gestor de Risco ou representante do nível decisório do escopo.
Entrada	Solicitação de diagnóstico (análise e avaliação) de risco de um determinado escopo ou contexto
Saída	Comunicado oficial informando as áreas e pessoas envolvidas sobre as ações a serem executadas e o escopo a ser trabalhado.

Atividade	**4.1. Definições Preliminares: responsáveis prazos e impactos**
Descrição	Definir os responsáveis por atividades como inventário e comunicação entre áreas. Definir um cronograma para acompanhamento das ações e impactos que podem ocorrer nas atividades durante a execução do ciclo de gestão de riscos.
Responsável	Definir características do projeto: gestor de SIC ou representante do nível decisório do escopo.e nível tático das áreas envolvidas.
Entrada	Relatório de contexto e escopo, organogramas, resultados de reuniões entre as áreas abrangidas pelo escopo.
Saída	Cronograma de atividades com prazos e responsáveis por cada atividade subsequente.

Atividade	**4.2. Inventariar ativos**
Descrição	Efetuar a identificação dos ativos definidos no escopo do projeto e levantamento de suas características, incluindo dependências e ligações com outros ativos.
Responsável	Identificação e levantamento de características dos ativos: representante do nível operacional do escopo junto aos responsáveis pelos ativos. Listagem das características dos ativos: responsáveis pelos ativos (nível operacional). Cadastro dos ativos e suas características: equipe do nível operacional do escopo
Entrada	Declaração do contexto e escopo; objetivos estratégicos; descrição dos ativos e respectivas características. Essa atividade pode ser executada por meio de reuniões entre as equipes envolvidas, como a gestão da área e os responsáveis pelos ativos.
Saída	Relação dos ativos, suas características, dependências e responsáveis..

4.3. Análise de Risco

Atividade	**A. Revisar ameaças, probabilidades e criticidade dos ativos**
Descrição	Identificar as ameaças, avaliar probabilidades e definir relevância dos ativos de acordo com os objetivos de negócio ou particularidades das áreas, departamentos, sistemas ou processos.
Responsável	identificar ameaças: representante do nível operacional do escopo Avaliar probabilidades: responsáveis pelos ativos do escopo. Definir relevância dos ativos: responsáveis pelos ativos, áreas, departamentos, sistemas ou processos.
Entrada	Ativos, suas características, dependências e responsáveis. Cadastro de informações dos ativos.
Saída	Atualização do inventário no sistema de gestão de riscos.

Atividade	**B. Criar questionários de análise e enviar aos responsáveis**
Descrição	Criar questionários ou *checklists* que contenham as melhores práticas de mercado para cada um dos ativos do escopo e suas particularidades.
Responsável	Criação e envio dos questionários: representante do nível operacional do escopo
Entrada	Questionário criado para cadastramento em sistema de gestão de riscos.
Saída	Questionários desenvolvidos para cada tipo de ativos do escopo e envio dos questionários criados.

Atividade	**C. Executar as análises nos ativos selecionados**
Descrição	Executar as análises de riscos por meio da avaliação dos controles sugeridos nos questionários comparados às evidências encontradas nos ativos.
Responsável	Realizar as análises de riscos: representante do nível operacional do escopo Acompanhar as análises: responsáveis pelos ativos.
Entrada	Questionários respondidos com as características dos ativos do escopo, cronograma de execução, escopo de atuação, inventário dos ativos.
Saída	Listagem de ativos e índices de riscos para cada ativo, sistema ou processo.

Atividade	**D. Consolidar resultados e verificar pendências**
Descrição	Consolidar os resultados após a análise de riscos nos ativos do escopo considerando as ligações ou dependências entre ativos, sistemas e processos, de acordo com o escopo ou contexto definido.
Responsável	Consolidar os resultados: representante do nível operacional do escopo Verificar e registrar pendências: Gestor de Segurança da Informação e Comunicações.
Entrada	Listagem de ativos e índices de riscos para cada ativo, sistema ou processo.
Saída	Resultados consolidados de acordo com os objetivos definidos no escopo de atuação.

Atividade	**E. Gerar relatórios de análise de riscos**
Descrição	Gerar relatórios contendo histórico de execução, resultados obtidos, ameaças mais significativas, índices de riscos por ativo, priorização de controles e sugestões de correção.
Responsável	Gerar relatórios de análise de riscos: representante do nível operacional do escopo
Entrada	Resultados consolidados de acordo com os objetivos definidos no escopo de atuação.
Saída	Relatório de análise de riscos e relatório operacional de riscos.

Atividade	**4.4. Avaliar riscos**
Descrição	Avaliar os riscos de acordo com o método autorizado pelos níveis decisórios.
Responsável	Avaliar os riscos: representante do nível operacional do escopo em conjunto com as equipes

	táticas responsáveis pelos ativos do escopo. Gerar relatórios de riscos aceitos ou residuais: representante do nível operacional do escopo, após avaliação dos riscos.
Entrada	Relatórios de análise de riscos e Relatórios Operacionais de Riscos.
Saída	Relatório de Avaliação de riscos (aceitos ou residuais, dependendo do tipo da análise realizada – identificação ou validação dos controles implementados).

4.5. Tratamento dos Riscos

Atividade	**4.5.1. Gerar plano de tratamento de riscos**
Descrição	Criar um plano de tratamento com as sugestões de controles para a minimização dos riscos provenientes dos controles identificados como não implementados, incluindo estimativas de custos, impactos nas atividades cotidianas, procedimentos necessários e prazos.
Responsável	Gerar plano de tratamento de riscos: representante do nível operacional do escopo
Entrada	Relatório Operacional de Riscos e Relatório de riscos aceitos ou residuais.
Saída	Plano de tratamento de riscos.

Atividade	**4.5.2. Aprovar plano de tratamento de riscos**
Descrição	Submeter para aprovação o plano de tratamento para alta gestão e gestor dos ativos que definirá ou ajustará as atividades de acordo com restrições que porventura existam como orçamento disponível ou priorização de atividades externas à gestão de riscos.
Responsável	Aprovar plano de tratamento e riscos residuais ou aceitos: Alta Gestão e nível tático considerando o escopo ou contexto de execução.
Entrada	Plano de tratamento de riscos e riscos residuais propostos pelo nível tático.
Saída	Plano de tratamento ajustado e aprovado. Relatório de riscos aceitos ou residuais.

Atividade	**4.5.3. Executar implantação dos controles selecionados**
Descrição	Executar a implantação dos controles selecionados para cada ativo de acordo com suas particularidades, características e tipos de ativos – tecnológicos, ambientais, humanos ou processuais.
Responsável	Executar a implantação dos controles selecionados: área ou responsáveis pelos ativos sob escopo (tecnologia, ambiente, processos ou pessoas).
Entrada	Plano de tratamento de riscos.
Saída	Controles de redução dos riscos implantados e indicadores gerados durante a implementação.