Ministério da Saúde

FIOCRUZ
Fundação Oswaldo Cruz

Número 001/2016-VPGDI	
Folha 1	De 7
Entrada em vigor	

Portaria da Presidência

O Vice-Presidente de Gestão e Desenvolvimento Institucional, no uso de suas atribuições

RESOLVE:

1.0 **PROPÓSITO**

Instituir o Modelo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC na Fiocruz.

2.0 OBJETIVO

Difundir o Modelo de Gestão de Riscos de Segurança da Informação e Comunicações no âmbito da Fiocruz, inclusive em seus institutos, visando estabelecer um processo sistemático e contínuo do gerenciamento dos riscos dos ativos de informação da instituição.

3.0 CONCEITOS E DEFINIÇÕES

Ativo de informação: qualquer pessoa, tecnologia, processo ou ambiente que processe, armazene, transporte ou descarte informação institucional;

Incidente de segurança: qualquer evento indesejado ou inesperado, que comprometa as operações ou ameace a segurança da informação;

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.

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.

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Cancela	Altera	Distribuição	Data
		Geral	**01/6/2016**

4.0 REFERÊNCIAS LEGAIS E NORMATIVAS

- NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação;
- NBR ISO/IEC 31000:2009 – Gestão de riscos - Princípios e diretrizes;
- Instrução Normativa nº 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009, que disciplina a Gestão de Riscos de Segurança da Informação e Comunicações – Gestão de Riscos de Segurança da Informação e Comunicações;

5.0 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - GRSIC

A GRSIC estabelece um conjunto de atividades que permite identificar os riscos a que estão submetidos uma organização. Através de um processo sistêmico é possível traçar a evolução do risco, tornando-se possível realizar ações de tratamento de forma efetiva, com o objetivo de reduzir os riscos a níveis aceitáveis. O modelo aqui apresentado está alinhado ao ciclo PDCA (*Plan-Do-Check-Act*), de modo a garantir a melhoria continua da gestão de riscos.

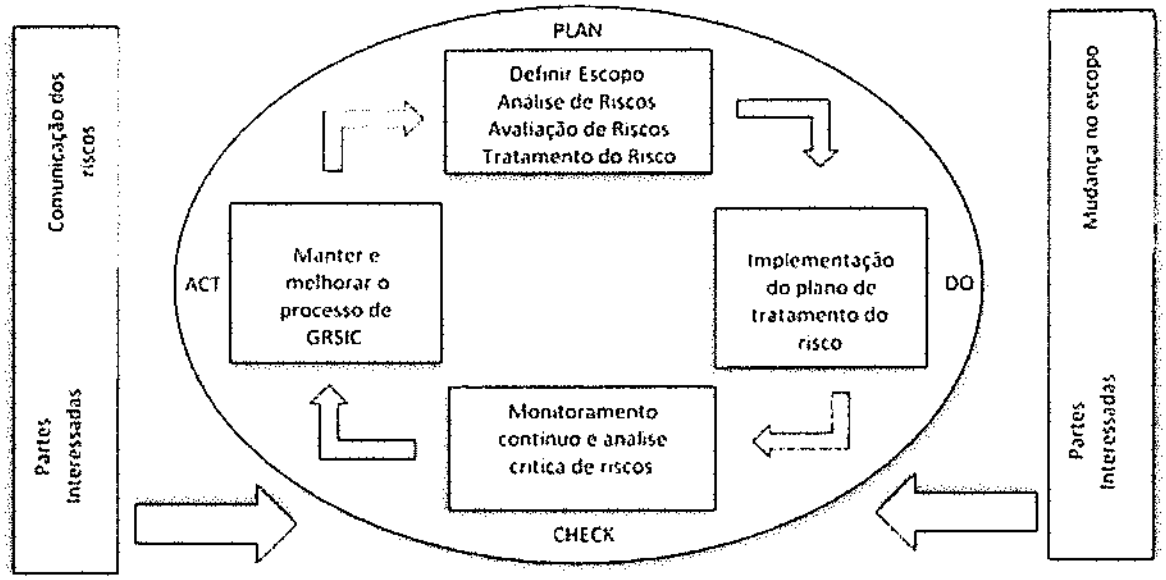

Figura 1: processo GRSIC alinhado ao ciclo PDCA

5.1 Planejamento da Gestão de Riscos

5.1.1. Definição do Escopo: O escopo da análise de riscos pode abranger a unidade como um todo, um sistema, um serviço de TI, um processo, um fornecedor ou um ativo de informação;

5.1.2. Análise dos Riscos: Na fase de análise dos riscos, devem ser identificados, minimamente, dentro do escopo definido:

a) Os ativos de informação e seus responsáveis;
b) As ameaças associadas ao escopo;
c) As vulnerabilidades existentes nos ativos de informação;
d) Estimar a probabilidade de a ameaça explorar a vulnerabilidade do ativo de informação;
e) Estimar o impacto a organização caso a ameaça explore a vulnerabilidade do ativo de informação;
f) As ações de SIC já adotadas.

Desta forma, é possível identificar o grau de risco a partir do produto da probabilidade pelo impacto, sendo representado através da seguinte expressão:

Grau de Risco = Grau de Probabilidade x Grau de Impacto

A probabilidade pode ser entendida como a chance de uma ameaça se concretizar. Para definir o grau da probabilidade, pode-se utilizar como referência a tabela abaixo:

Valor	Probabilidade	Descrição
1	Muito baixa	Muito improvável de acontecer (1 a 10%)
2	Baixa	Improvável de ocorrer (11 a 30%)
3	Média	Ocorre ocasionalmente (31 a 70%)
4	Alta	Provável de ocorrer (71 a 90%)
5	Muito alta	Ocorre frequentemente (91 a 100%)

Tabela 1: Definição do grau de probabilidade

O impacto deve considerar os potenciais prejuízos causados, caso o incidente se concretize. Por conta das informações que suportam, os ativos de informação têm relevâncias diferentes para o negócio. Quanto maior a relevância do ativo, maior será a severidade de um incidente. Para definir o grau de impacto, pode-se utilizar como referência a seguinte tabela:

Valor	Impacto	Descrição
1	Desprezível	Os danos são insignificantes para a organização.
2	Baixo	A organização consegue reparar os danos com seus próprios recursos.
3	Crítico	A recuperação dos danos extrapola os recursos da organização.
4	Grave	Danos que venham manchar a imagem do órgão ou gerar algum incidente grave.
5	Gravíssimo	Destruição irreparável da imagem do órgão e oferece risco de morte dos seus agentes públicos.

Tabela 2: Definição do grau de impacto

Após estimar a probabilidade e o impacto, é possível identificar o Grau do Risco, utilizando como referência a Matriz de Risco abaixo:

		Probabilidade				
		M. Baixa	Baixa	Média	Alta	M. Alta
Impacto	Desprezível	1	2	3	4	5
	Baixo	2	4	6	8	10
	Crítico	3	6	9	12	15
	Grave	4	8	12	16	20
	Gravíssimo	5	10	15	20	25

(Tabela 3) Matriz de Risco

5.1.3. Avaliação dos Riscos: Nesta fase, é comparado o grau de risco obtido através da Matriz de Risco com os critérios de risco. Esta comparação tem como objetivo determinar a importância do risco e servirá de subsídio para a fase de tratamento. A tabela a seguir estabelece os critérios de risco:

Valor	Grau de Risco	Critérios
16 - 25	Muito Alto	Os riscos são inaceitáveis e os responsáveis devem ser orientados para minimizar imediatamente.
10 - 15	Alto	Os riscos são inaceitáveis e os responsáveis devem minimamente controlá-los.
6 - 9	Médio	Os riscos podem ser aceitos após revisão e confirmação dos responsáveis. Entretanto, a aceitação dos riscos deve ser feita por meios formais.
4 - 5	Baixo	Os riscos podem ser aceitáveis, entretanto deve ser feita a revisão e confirmação dos responsáveis.
1 - 3	Muito Baixo	Os riscos são aceitáveis e devem ser informados aos responsáveis.

(Tabela 4) Critérios de Riscos

5.1.4. Tratamento de Risco: Esta fase é responsável por implementar ações de segurança orientadas pelo resultado da avaliação dos riscos. Existem quatro formas para tratar o risco:

- Evitar: Nesta forma de tratamento, 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.
- Reter: Forma de tratamento de risco na qual se decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.
- Reduzir: Também conhecida como mitigar risco, esta forma de tratamento implementa ações para reduzir a probabilidade, as consequências negativas, ou ambas.
- Transferir: Forma de tratamento de risco na qual se decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco.

É importante realizar uma análise do custo-benefício das medidas/controles de segurança em relação a sua aplicabilidade e os benefícios que poderão ser agregados ao negócio. Muitas das vezes o custo financeiro da implementação de uma ação pode ser maior do que o custo do ativo de informação que se quer proteger.

5.2 Implementação do plano de tratamento

Nesta etapa do ciclo PDCA (executar) serão determinadas as formas de tratamento dos riscos, as ações que serão adotadas, os responsáveis por cada ação, o prazo para a implementação das ações, etc. Também é importante observar:

a) A eficácia das ações de SIC já existentes;
b) As restrições organizacionais, técnicas e estruturais;
c) Os requisitos legais; e
d) Análise custo-benefício.

Importante: O plano de tratamento deve ter aprovação formal da Alta Administração.

5.3 Monitoramento contínuo e análise crítica dos riscos

Na terceira fase do Ciclo PDCA (Checar) é monitorado e analisado criticamente a eficácia do processo de Gestão de Riscos de forma a garantir o alinhamento do Modelo de Gestão de Riscos às necessidades da Fiocruz. Essa análise ocorre simultaneamente às demais fases, devendo ser observadas oportunidades de melhorias ou falhas no próprio processo.

Em relação ao risco, devem ser monitorados e analisados criticamente, de forma regular, as seguintes mudanças:

- Critérios de avaliação e aceitação dos riscos;
- Ambientes;
- Ativos de informação;
- Ações de SIC;
- Fatores de risco (ameaça, vulnerabilidade, probabilidade e impacto).

Outro fator que deve ser observado é a percepção do risco, pois uma determinada percepção pode mudar com o decorrer do tempo, como por exemplo:

- Um determinado escopo sofreu alteração dos seus ativos;
- A probabilidade de uma ameaça explorar uma vulnerabilidade era baixa e agora é alta;

- Um risco que era aceito, agora será tratado; e
- Surgimento de novos riscos.

A fase de monitoramento contínuo também é responsável por garantir:

- Se o tratamento do risco está sendo realizado conforme planejado;
- Se foram realizadas alterações no contexto/escopo;
- Se as ações implementadas estão sendo eficazes na correção das vulnerabilidades; e
- A gestão de riscos de segurança está sendo realizado de forma adequada.

5.4. Manter e melhorar o modelo de gestão de riscos

A etapa do Ciclo PDCA *Act* (agir) tem como objetivo garantir a melhoria continua de todo o processo de gestão de riscos, assim como:

- Propor a alta administração a necessidade de implementar as melhorias identificadas durante a fase de monitoramento e análise crítica;
- Executar as ações corretivas ou preventivas aprovadas; e
- Assegurar que as melhorias atinjam os objetivos pretendidos.

5.5 Comunicação do risco

A comunicação do risco é uma etapa que deve ocorrer paralelamente a todo o processo de gestão de riscos. Deve haver uma troca interativa, formalmente documentada, intencional e contínua, de conhecimentos, informações e percepções sobre os riscos que devem ser gerenciados. Através desta etapa devem ser transmitidas as informações sobre o desenvolvimento das atividades, modificações no contexto/escopo e os resultados alcançados as partes interessadas.

6.0 VIGÊNCIA

A presente Portaria entra em vigor na data de sua publicação.

Pedro Ribeiro Barbosa
Vice-Presidente de Gestão e Desenvolvimento Institucional
Fundação Oswaldo Cruz