Processo de Gestão de Riscos de Segurança da Informação

CONTROLE DE REVISÂO DO DOCUMENTO

Versão	Descrição	Data	Autor
1.0	Versão inicial do documento	13/09/2017	Anilton Maia/Leonardo Nakahara/Renata Braga
1.1	Release	21/09/2017	Anilton Maia/Leonardo Nakahara/Renata Braga

Sumário

Objetivo

Este documento tem por objetivo estabelecer o processo de Gestão de Riscos de Segurança da Informação (GRSI) no âmbito do Hospital Universitário da Universidade Federal do Maranhão (HU-UFMA).

A gestão de risco é o processo de planejar, organizar, dirigir e controlar os recursos humanos e materiais de uma organização, no sentido de minimizar ou aproveitar os riscos e incertezas sobre essa organização.

Espera-se, com esse processo, tornar a gestão de riscos do HU-UFMA eficaz, buscando aumentar a probabilidade de cumprimento da missão institucional; melhorar a governança; estabelecer uma base confiável para a tomada de decisão e o planejamento; e melhorar a eficácia e eficiência operacional.

Aplicabilidade

O processo de Gestão de Riscos tem aplicabilidade em toda as áreas organizacionais do HU-UFMA.

Referências Normativas

A elaboração do processo descrito por este documento utilizou como referência as seguintes normas:

- ABNT NBR ISO/IEC 27005:2008;
- ISO/IEC 31000:2009.

Termos e Definições

- **Ameaça:** causa potencial de um incidente indesejado que pode resultar em dano para a organização;
- **Ativo**: qualquer recurso que tenha valor para a organização e cujo risco precisa ser controlado;
- **Vulnerabilidade:** fragilidade de um ativou ou grupo de ativos que pode ser explorada por uma ou mais ameaças;
- **BPMN**: Acrônimo de *Business Process Modeling Notation*. Notação gráfica que descreve a lógica dos passos de um processo de negócio. É um padrão internacional de modelagem que permite modelar o processo de uma maneira unificada e padronizada;
- **Probabilidade do risco:** possibilidade de concretização de uma ameaça;
- **Nível de risco**: magnitude do risco, expressa em termos da combinação das consequências e de suas probabilidades.
- **Evento de Segurança da Informação**: ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança

da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

- **Risco de segurança da informação:** possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos. É medido em função da combinação da probabilidade de um evento e de sua consequência;
- **Risco Residual:** Risco remanescente após o tratamento de risco ter sido implementado. O risco residual pode conter riscos não identificados;
- **Contexto Externo:** é o ambiente externo no qual a organização se situa e busca atingir seus objetivos (ambiente cultural, financeiro, regulatório, econômico, entre outros);
- **Contexto Interno:** é o ambiente interno no qual a organização busca atingir seus objetivos (governança, estrutura organizacional, políticas, normas, objetivos, diretrizes, cultura organizacional, entre outros);
- **TIC:** Tecnologia da Informação e Comunicações;
- **Impacto (ou consequência):** uma das consequências da ocorrência de um evento. Ocasiona mudança adversa no nível obtido dos objetivos.

Papéis e Responsabilidades

Na Tabela 1 estão descritos os papéis e responsabilidades relacionadas ao Processo de Gestão de Riscos de Segurança da Informação do HU-UFMA.

Papel	Responsabilidades
Superintendência	• Analisar as deliberações relacionados à Gestão de Riscos e decidir sobre possíveis providências; • Aprovar o Processo de Gestão de Riscos de Segurança da Informação;
Subcomitê Gestor de Segurança da Informação e Comunicação	• Deliberar sobre as principais diretrizes e temas relacionados à Gestão de Riscos de Segurança da Informação; • Submeter o Processo de Gestão de Riscos da Segurança da Informação e suas revisões para aprovação pela Superintendência; • Aprovar os critério de riscos (apetite a risco, graus de impacto, graus de probabilidade e classificação de riscos);
Unidade de Infraestrutura e Segurança da Informação	• Elaborar o Processo de Gestão de Riscos de Segurança da Informação;

	• Gerir e executar o Processo de Gestão de Riscos de Segurança da Informação. • Elaborar Planos de Tratamento de Riscos; • Acompanhar a execução dos planos de ação; • Realizar o monitoramento e a análise crítica do Processo de Gestão de Riscos de Segurança da Informação, propondo ajustes e medidas preventivas e proativas; • Disseminar cultura voltada para identificação e tratamento de riscos; • Fornecer consultoria interna em gestão de riscos; • Comunicar os riscos às partes interessadas;

Tabela 1- Papéis e Responsabilidades

Critérios para avaliação de risco

Os critérios de riscos são parâmetros estabelecidos para avaliar a magnitude dos riscos, a fim de seja possível quantificar o impacto negativo na busca da obtenção de resultados esperados pelo HU-UFMA em sua missão institucional.

Para efeito deste processo, definiu-se como metodologia para a análise de risco a forma proposta pela norma ABNT NBR ISO 31000:2009, a qual define o nível do risco em termos da combinação dos impactos e de suas probabilidades.

Serão utilizadas escalas quantitativas para estimar a probabilidade e o impacto. Tais escalas encontram-se representadas nas Tabela 2 e Tabela 3.

Peso	Critérios	Probabilidade
5	Muito Alta	50% < Probabilidade <= 100%
4	Alta	20% < Probabilidade <= 50%
3	Média	8% < Probabilidade <= 20%
2	Baixa	2% < Probabilidade <= 8%
1	Muito Baixa	0% < Probabilidade <= 2%

Tabela 2- Critérios de Probabilidade

Peso	Impacto	Descrição
5	Catastrófico	Impacto máximo nos objetivos do processo avaliado, sem possibilidade de recuperação.
4	Muito Relevante	Impacto significante nos objetivos do processo avaliado, com possibilidade remota de recuperação.
3	Relevante	Impacto mediano nos objetivos do processo avaliado, com possibilidade de recuperação.
2	Pouco Relevante	Impacto mínimo aos objetivos do processo avaliado. São facilmente remediáveis.
1	Insignificante	Impacto insignificante nos objetivos do processo avaliado. Dispensa qualquer medida de reparação.

Tabela 3- Critérios de Impacto

O nível do risco é calculado pelo produto entre a probabilidade e o impacto. A Tabela 4 apresenta a matriz de risco, ferramenta utilizada para a classificação dos níveis de risco.

Extremo Elevado Médio Baixo		PROBABILIDADE				
		Muito baixa (1)	Baixa (2)	Média (3)	Alta (4)	Muito Alta (5)
IMPACTO	Catastrófico (5)	5	10	15	20	25
	Muito relevante (4)	4	8	12	16	30
	Relevante (3)	3	6	9	12	15
	Pouco Relevante (2)	2	4	6	8	10
	Insignificante (1)	1	2	3	4	5

Tabela 4 - Matriz de Risco

Processo de Gestão de Riscos

O modelo adotado pelo SGPTI para o gerenciamento de riscos pautou-se na norma ISO 31000:2006. A Figura 1 apresenta a visão geral do processo.

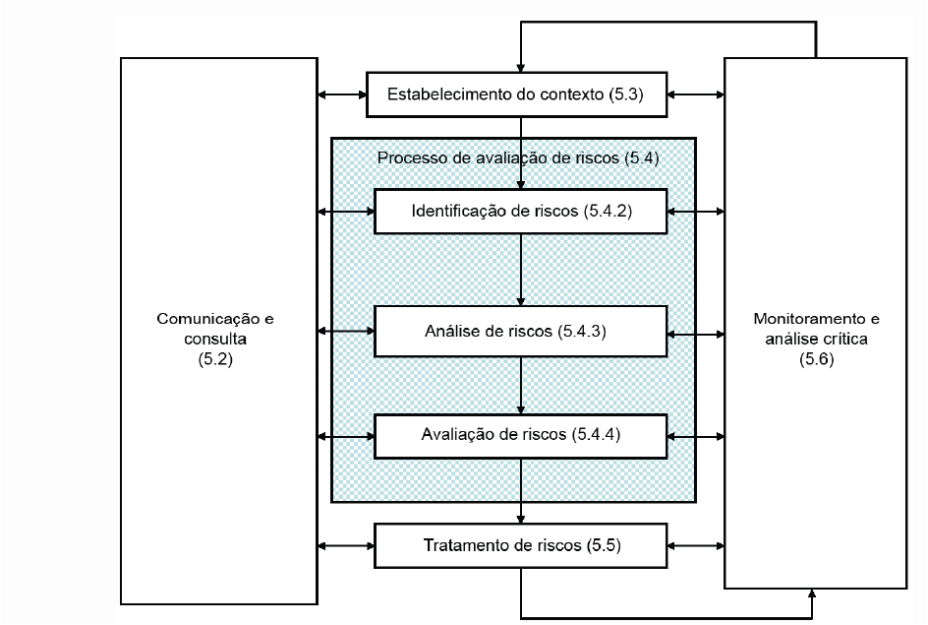


Figura 1 - Processo de Gestão de Risco ABNT NBR ISO 31000:2009

O processo engloba os seguintes elementos:

- Estabelecimento do contexto;
- Avaliação de riscos (identificação, análise e avaliação de riscos);
- Tratamento de riscos;
- Comunicação e consulta;
- Monitoramento e análise crítica.

O fluxo processo de Gestão de Risco do HU-UFMA encontra-se desenhado em BPMN no Anexo I.

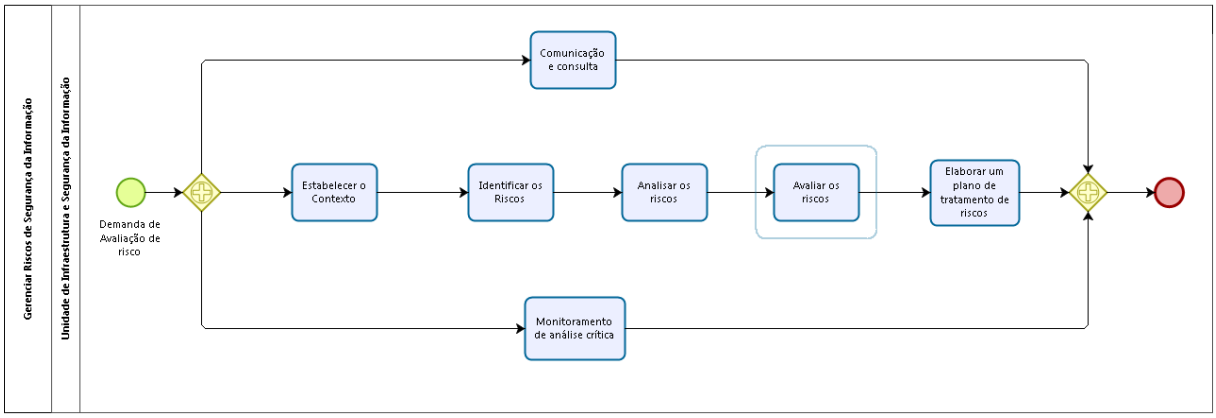
As tarefas previstas pelo Processo de Gestão de Riscos de Segurança da Informação do HU-UFMA estão especificadas no Anexo II.

É importante destacar que embora todas as tarefas do processo sejam de responsabilidade da Unidade de Infraestrutura e Segurança da Informação, a participação de outras unidades da área de TIC (Desenvolvimento, Governança, Relacionamento com o Usuário e AGHU) e do Subcomitê Gestor de Segurança da Informação e Comunicações são indispensáveis para o sucesso na gestão dos riscos.

As unidades de TIC participarão das atividades sempre os riscos envolverem as suas respectivas áreas de atuação. E o Subcomitê Gestor de Segurança da Informação e

Comunicações será instado a validar e aprovar os artefatos produzido ao longo do processo quando for necessário o estabelecimento de diretrizes com aplicabilidade em todo Hospital.

ANEXO I - Fluxo do Processo de Gestão de Riscos



ANEXO II - Tarefas do Processo de Gestão de Riscos

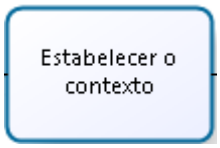
	**Estabelecer o contexto**
Objetivo: Estabelecer o contexto externo e interno para apoiar o Processo de Gestão de Riscos de Segurança da Informação.	
Entradas: Todas as informações relevantes sobre a organização para a definição do contexto da gestão de riscos.	
Descrição da atividade: • Definir os critérios básicos para a gestão de riscos, tais como critério de avaliação de riscos, critério de impacto e critérios de aceitação do risco; • Estipular os objetivos a serem alcançados. Por exemplo: conformidade legal, preparação de um plano de resposta a incidentes, etc.; • Definir o escopo - descrição dos limites do projeto, sua abrangência, seus resultados e entregas.	
Responsável: Unidade de Infraestrutura e Segurança da Informação	
Saída: Especificação dos critérios básicos, o escopo e os limites do processo de gestão de riscos.	

Tabela 5 - Tarefa Estabelecer o contexto

	**Identificar os Riscos**

Objetivo:

Encontrar, reconhecer e iniciar o registro dos riscos como o objetivo de identificar o que poderia acontecer ou quais situações poderiam afetar o alcance dos objetivos do HU-UFMA.

Entradas:

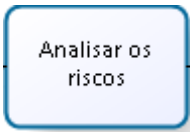
- Contexto dos riscos (critérios básicos, o escopo e os limites, e a organização do processo de gestão de riscos);
- Lista dos ativos relacionados aos riscos;
- Informações do histórico e de incidentes passados;
- Documentação dos controles, planos de implementação do tratamento do risco;

Descrição da atividade:

- Identificação de ativos - realizar o levantamento dos ativos que estão dentro do escopo estabelecido. Além disso, é necessário listar os serviços/sistemas relacionados aos ativos identificados;
- Identificação de ameaças - realizar o levantamento das ameaças que tem potencial de comprometer ativos, identificando as suas fontes;
- Identificação de controles existentes - realizar o levantamento dos mecanismos administrativos, físicos ou operacionais capazes de tratar a ocorrência de um incidente de segurança existentes no HU-UFMA;
- Identificação de vulnerabilidades - realizar o levantamento das vulnerabilidades que podem ser exploradas por ameaças para comprometer os ativos ou a organização. Essas vulnerabilidades podem ser das seguintes áreas: organização; processos e procedimento; rotinas de gestão; recursos humanos; ambiente físico; configuração do sistema de informação; hardware, software ou equipamento de comunicação; dependência de entidades externas;
- Identificação das consequências - realizar o levantamento do prejuízo ou das consequências para o HU-UFMA que podem decorrer de um cenário de incidente.

Um cenário de incidente é a descrição de uma ameaça explorando as vulnerabilidades.
Responsável: Unidade de Infraestrutura e Segurança da Informação
Saída: • Lista de ativos cujos riscos precisam ser controlados; • Lista de processos de negócios relacionados aos ativos; • Lista de ameaças com a identificação do tipo e da fonte das ameaças; • Lista de todos os controles existentes; • Lista de vulnerabilidades associadas aos ativos, ameaças e controles; • Lista de cenários de incidentes com suas consequências;

Tabela 6 - Tarefa Identificar os riscos

	**Analisar os riscos**

Objetivo:

Diz respeito ao entendimento do risco, com a definição das consequências e probabilidades para eventos identificados de risco. Com essa análise, busca-se o levantamento de informações que contribuam com a tomada de decisões estratégicas sobre os riscos e a forma mais adequada e rentável de tratamento.

Entradas:

- Lista de cenários de incidentes com suas consequências, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências para os ativos e processos do negócio;

Descrição da atividade:

- Avaliação das consequências - avaliar os impactos sobre os negócios do HU-UFMA levando-se em conta as consequências de uma violação de segurança da informação. As consequências poderão ser expressas em função de critérios financeiros, técnicos, humanos, do impacto nos negócios, dentre outros;
- Avaliação da probabilidade dos incidentes - avaliar a probabilidade de ocorrência de incidentes em cada cenário e seus impactos;
- Determinação do nível de risco - realizar a mensuração do nível de risco para todos os incidentes considerados com o uso dos resultados obtidos pela avaliação das consequências e avaliação de probabilidade;

Responsável:

Unidade de Infraestrutura e Segurança da Informação

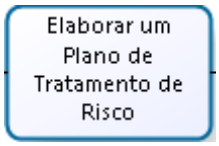
Saída:

- Lista de consequências avaliadas referente a um cenário de incidente;
- Probabilidade dos cenários de incidentes;
- Lista de riscos com níveis de valores designados;

Tabela 7 - Tarefa Analisar os riscos

	**Avaliar os riscos**
Objetivo: Compreender a natureza do risco a fim de auxiliar a tomada de decisão sobre ações futuras.	
Entradas: Lista de riscos com níveis de valores designados e critérios para a avaliação de riscos.	
Descrição da atividade: Consiste em comparar os níveis de riscos estimados com critérios de riscos definidos pelo HU-UFMA, a fim de determinar a ação mais adequada a ser tomada em relação ao risco, identificando quais riscos necessitam ser tratados e quais terão prioridade no tratamento.	
Responsável: Unidade de Infraestrutura e Segurança da Informação	
Saída: Lista de riscos priorizados, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.	

Tabela 8 - Tarefa Avaliar os riscos

	**Elaborar um Plano de Tratamento de Risco**

Objetivo:

Criação de um plano para tratamento dos riscos identificados, o que envolve a seleção de uma ou mais ações para modificar os riscos e a implementação dessas ações.

Entradas:

Lista de riscos priorizadas, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar a esses riscos.

Descrição da atividade:

Selecionar as opções de tratamento para os riscos selecionados considerando o resultado da análise/avaliação de riscos, custo esperado para implementação e benefícios previstos. Deve-se identificar a ordem de prioridade, bem como os prazos de execução. As respostas a riscos podem envolver uma ou mais das seguintes opções de tratamento:

- Evitar o risco - ação para evitar totalmente o risco.
- Transferir o risco - compartilhar ou transferir uma parte do risco a terceiros.
- Mitigar o risco - reduzir o impacto ou a probabilidade de ocorrência do risco.
- Aceitar o risco - aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício.

Responsável:

Unidade de Infraestrutura e Segurança da Informação

Saída:

Plano de tratamento de riscos;

Tabela 9 - Tarefa Elaborar um Plano de Tratamento de Risco

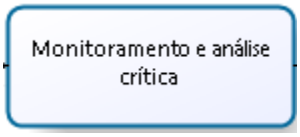
	**Monitoramento e Análise Crítica**
Objetivo: Trata da revisão e análise periódica da gestão de riscos, com vista ao aprimoramento contínuo desse processo pelo HU-UFMA.	
Entradas: Todas as informações sobre os riscos geradas ao longo da execução das atividades do Processo de Gestão de Riscos de Segurança da Informação.	
Descrição da atividade: • Monitoramento e análise crítica dos fatores de risco - assegurar o controle do risco, monitorando riscos residuais e identificando novas ameaças e vulnerabilidades, assegurando a execução dos planos de tratamento dos riscos e avaliando sua eficiência e eficácia na redução dos riscos; • Monitoramento, análise crítica e melhoria do processo de gestão de risco - garantir que o processo de gestão de riscos esteja realmente atendendo aos requisitos estratégicos do negócio;	
Responsável: Unidade de Infraestrutura e Segurança da Informação	
Saída: Alinhamento contínuo da gestão de riscos	

Tabela 10 - Tarefa Monitoramento e Análise Crítica

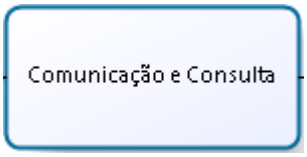
	**Comunicação e Consulta**
Objetivo: Compartilhamento contínuo das informações referente aos riscos entre as partes interessadas.	
Entradas: Todas as informações sobre os riscos geradas ao longo da execução das atividades do Processo de Gestão de Riscos de Segurança da Informação.	
Descrição da atividade: Realizar a comunicação das informações produzidas ao longo da execução do processo de gestão de riscos, bem com disponibilizar essas informações para consulta, a fim de assegurar a compreensão necessária à tomada de decisão envolvendo riscos.	
Responsável: Unidade de Infraestrutura e Segurança da Informação	
Saída: Entendimento contínuo do Processo de Gestão de Riscos de Segurança da Informação e dos resultados obtidos	

Tabela 11 - Tarefa Comunicação e Consulta