



Ministério da Educação
Universidade Federal de Alfenas
Rua Gabriel Monteiro da Silva, 700 - Bairro centro, Alfenas/MG - CEP 37130-001
Telefone: (35) 3701-9000 - <http://www.unifal-mg.edu.br>

COMITÊ DE GOVERNANÇA DIGITAL
Resolução Nº 06/2020, DE 10 DE JULHO DE 2020

Estabelece Processo de Gestão de Riscos de Segurança da Informação no âmbito da UNIFAL-MG.

O Comitê de Governança Digital (CGD) da Universidade Federal de Alfenas – UNIFAL-MG, no uso de suas atribuições regimentais e considerando:

A Instrução Normativa 01 do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR), de 27 de maio de 2020;

A Norma Complementar 04/DSIC/GSI/PR de 15 de fevereiro de 2013;

A Norma Complementar 14/DSIC/GSI/PR de 13 de março de 2018;

A adoção pela UNIFAL-MG da Plataforma Gsuite for Education (Processo 23087.004781/2020-56);

As demais necessidades de gestão de riscos de segurança da informação no âmbito da UNIFAL-MG;

RESOLVE estabelecer as normas para o uso adequado dos serviços de armazenamento e compartilhamento de arquivos no âmbito da UNIFAL-MG, nos seguintes termos:

Art. 1º Este documento tem por objetivo estabelecer o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) no âmbito da Universidade Federal de Alfenas (UNIFAL-MG).

Art. 2º 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 da Unifal-MG 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.

Art. 3º O processo de Gestão de Riscos tem aplicabilidade nos serviços de Tecnologia de Informação e Comunicação oferecidos pelo Núcleo de Tecnologia da Informação (NTI) da Unifal-MG.

Art. 4º Para efeitos desta normativa, entende-se por:

I. Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para a organização;

II. Ativo: qualquer recurso que tenha valor para a organização e cujo risco precisa ser controlado;

III. Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

IV. 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;

V. Probabilidade do risco: possibilidade de concretização de uma ameaça;

VI. Nível de risco: magnitude do risco, expressa em termos da combinação das consequências e de suas probabilidades.

VII. 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.

VIII. 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;

IX. Risco Residual: Risco remanescente após o tratamento de risco ter sido implementado. O risco residual pode conter riscos não identificados;

X. Contexto Externo: é o ambiente externo no qual a organização se situa e busca atingir seus objetivos (ambiente cultural, financeiro, regulatório, econômico, entre outros);

XI. 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);

XII. TIC: Tecnologia da Informação e Comunicações;

XIII. Impacto (ou consequência): uma das consequências da ocorrência de um evento. Ocasionalmente mudança adversa no nível obtido dos objetivos.

Art. 5º São Responsabilidades do Comitê de Governança Digital:

I. Analisar as deliberações relacionados à Gestão de Riscos e decidir sobre possíveis providências;

II. Aprovar o Processo de Gestão de Riscos de Segurança da Informação;

Art. 6º São Responsabilidades da Gerência de Segurança da Informação (GSI) do Núcleo de Tecnologia da Informação da UNIFAL-MG

I. Deliberar sobre as principais diretrizes e temas relacionados à Gestão de Riscos de Segurança da Informação;

II. Submeter o Processo de Gestão de Riscos da Segurança da Informação e suas revisões para aprovação pelo CGD;

III. Aprovar os critérios de riscos (apetite a risco, graus de impacto, graus de probabilidade e classificação de riscos);

IV. Elaborar o Processo de Gestão de Riscos de Segurança da Informação;

V. Gerir e executar o Processo de Gestão de Riscos de Segurança da Informação.

VI. Elaborar Planos de Tratamento de Riscos;

VII. Acompanhar a execução dos planos de ação;

VIII. Realizar o monitoramento e a análise crítica do Processo de Gestão de Riscos de Segurança da Informação, propondo ajustes e medidas preventivas e proativas;

IX. Disseminar cultura voltada para identificação e tratamento de riscos;

X. Fornecer consultoria interna em gestão de riscos;

XI. Comunicar os riscos às partes interessadas;

Art. 7º 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 NTI/Unifal-MG em sua missão institucional. Serão utilizadas escalas quantitativas para estimar a probabilidade e o impacto. Tais escalas encontram-se representadas nas Tabelas 1 e 2 deste documento.

Tabela 1-Critérios de Probabilidade

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 Impacto

Peso	Impacto	Descrição
5	Catastrófico	Impacto máximo nos objetivos do processo avaliado, sem possibilidade de recuperação.
4	Muito Relevante	Impacto significativo 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.

Art. 8º O nível do risco é calculado pelo produto entre a probabilidade e o impacto. A Tabela 3 apresenta a matriz de risco, ferramenta utilizada para a classificação dos níveis de risco.

Tabela 3-Matriz de Risco

Extremo		Probabilidade				
Elevado						
Médio		Muito Baixa	Baixa	Média	Alta	Muito Alta
Baixo						
Impacto	Catastrófico	5	10	15	20	25
	Muito Relevante	4	8	12	16	20
	Relevante	3	6	9	12	15
	Pouco Relevante	2	4	6	8	10
	Insignificante	1	2	3	4	5

Art. 9º O processo de gestão de riscos no âmbito desta resolução engloba os seguintes elementos:

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

Art. 10 A representação visual do modelo de gestão de riscos adotado no contexto desta resolução encontra-se no Anexo I.

Art. 11 O fluxo processo de Gestão de Risco do UNIFAL-MG encontra-se desenhado em BPMN no Anexo II.

Art. 12 As tarefas previstas pelo Processo de Gestão de Riscos de Segurança da Informação do UNIFAL-MG estão especificadas no Anexo III.

Art. 13 A responsabilidade da Gerência de Segurança da Informação sobre as tarefas do processo de gestão de riscos não exime a participação de outras unidades do NTI ou outros órgãos da UNIFAL-MG.

Art. 14 O NTI dará ampla divulgação desta Resolução aos usuários da Universidade.

Art. 15 Os casos omissos nessa norma serão resolvidos pela GSI/NTI e, em grau de recurso, pelo Comitê de Governança Digital - CGD.

Art. 16 Esta Resolução entra em vigor na data de sua publicação.

Sandro Amadeu Cerveira

Presidente do Comitê de Governança Digital



Documento assinado eletronicamente por **Sandro Amadeu Cerveira, Presidente**, em 13/07/2020, às 14:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.unifal-mg.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0337664** e o código CRC **5C83F25C**.

ANEXO I - Processo de Gestão de Riscos

O modelo de gestão de riscos adotado no contexto desta resolução para o gerenciamento de riscos pautou-se na visão geral do processo conforme apresentada na Figura 1.

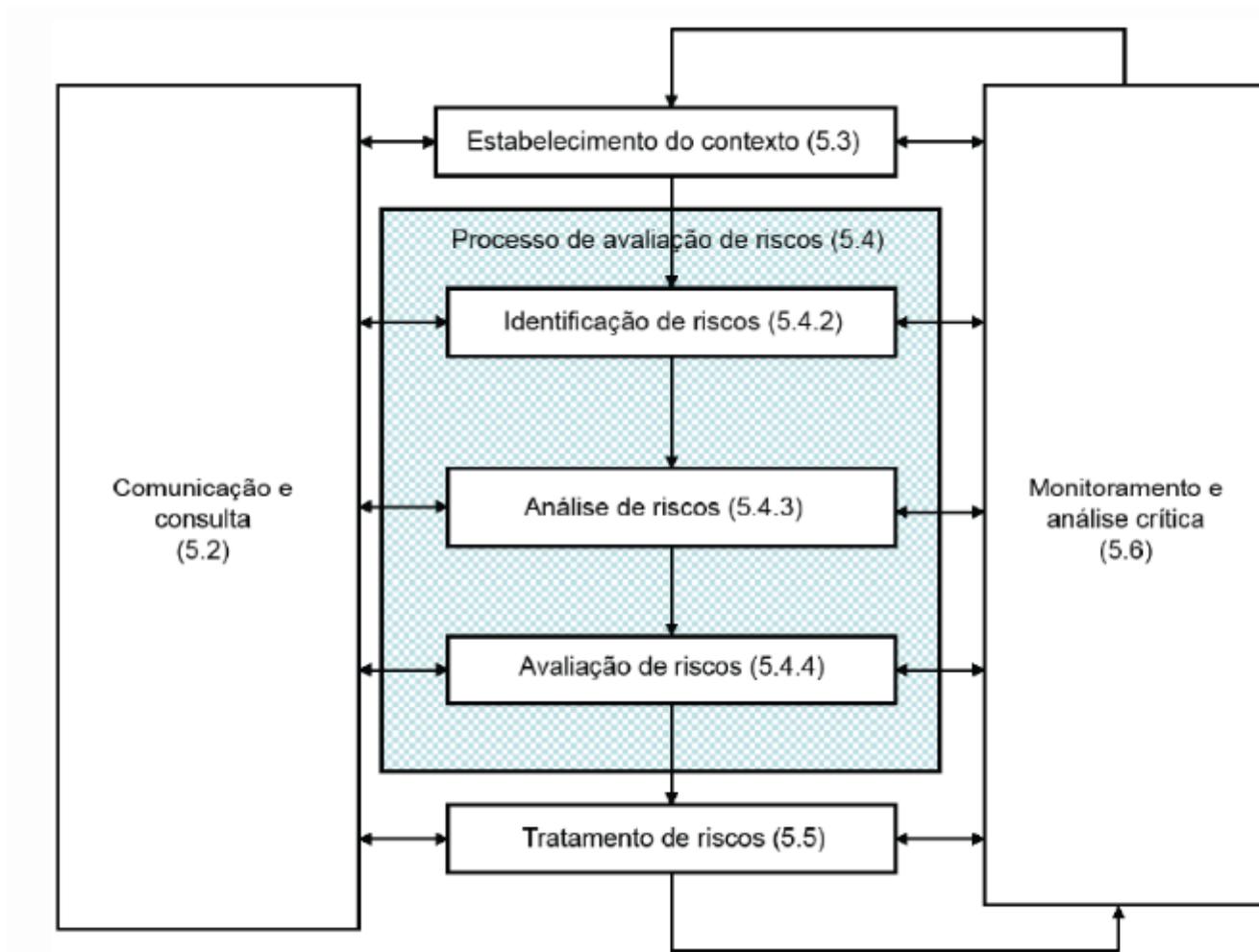
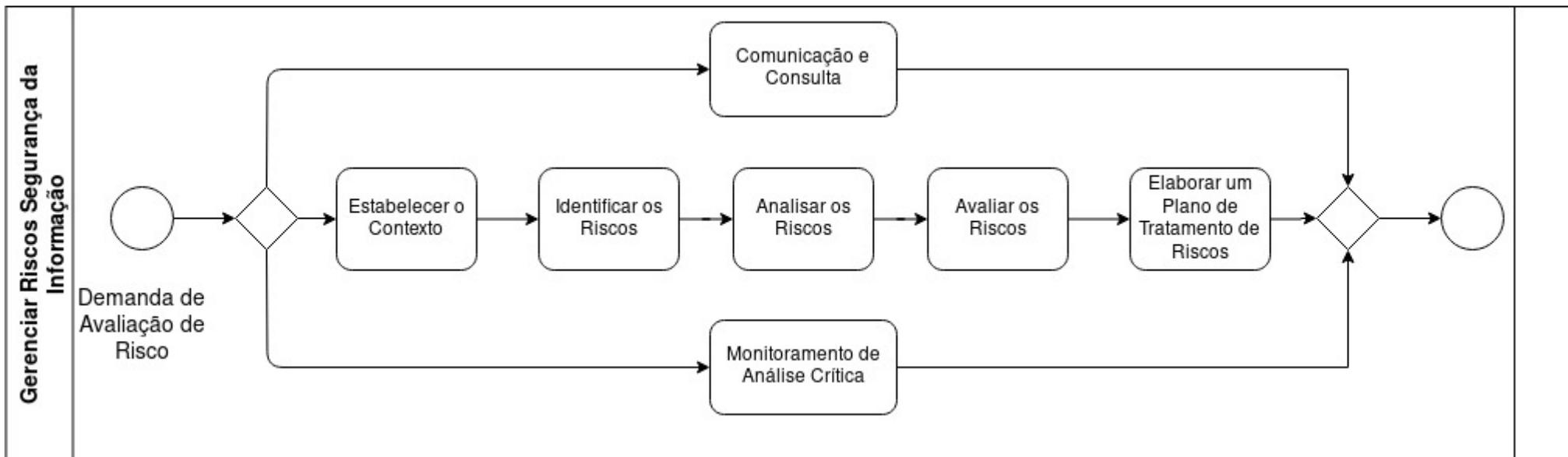


Figura 1-Processo de Gestão de Risco

ANEXO II -Fluxo do Processo de Gestão de Riscos



ANEXO III -Tarefas do Processo de Gestão de Riscos

Estabelecer 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 dos limites do projeto, sua abrangência, seus resultados e entregas.

Responsável:

Gerência de Segurança da Informação

Saída:

Especificação dos critérios básicos, o escopo e os limites do processo de gestão de riscos.

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 da Unifal-MG.

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 na Unifal-MG;
- 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 a Unifal-MG que podem decorrer de um cenário de incidente. Um cenário de incidente é a descrição de uma ameaça explorando as vulnerabilidades.

Responsável:

Gerência de 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;

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 da Unifal-MG 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:

Gerência de 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;

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 pela Unifal-MG, 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:

Gerência de 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.

Elaborar o Plano de Tratamento de Riscos**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:

Gerência de Segurança da Informação

Saída:

Plano de tratamento de riscos;

Monitoramento e Análise Crítica

Objetivo:

Trata da revisão e análise periódica da gestão de riscos, com vista ao aprimoramento contínuo desse processo pela Unifal-MG.

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:

Gerência de Segurança da Informação

Saída:

Alinhamento contínuo da gestão de riscos

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:

Gerência de Segurança da Informação

Saída:

Entendimento contínuo do Processo de Gestão de Riscos de Segurança da Informação e dos resultados obtidos