Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		1/27

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
Secretaria Executiva
Comitê de Segurança da Informação e Comunicações

GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES - GRSIC

ORIGEM

Comitê de Segurança da Informação e Comunicações - CSIC.

REFERÊNCIA NORMATIVA

Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.
Norma Complementar nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008.
Norma Complementar nº 04/IN01/DSIC/GSIPR, de 15 de fevereiro de 2013.
Portaria MCTIC nº 4.711, de 18 de agosto de 2017 – Posic/MCTIC.
ABNT NBR ISO/IEC 27001:2013.
ABNT NBR ISO/IEC 27002:2013.
ABNT NBR ISO IEC 27005:2011.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica aos órgãos de assistência direta e imediata ao Ministro de Estado, aos órgãos específicos singulares e às unidades descentralizadas deste Ministério.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

Gilberto Kassab
Ministro

1 FINALIDADE

Estabelecer as diretrizes para o processo de Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) no Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC).

2 DISPOSIÇÕES GERAIS

2.1 A Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC), objeto desta norma complementar, está limitada ao escopo das ações de Segurança da Informação e Comunicações e compreende apenas as medidas de proteção dos ativos de informação, conforme definição desta norma.

2.2 O processo de GRSIC deve ser contínuo, com a execução de suas atividades cíclicas e periódicas, em conformidade com o escopo definido para cada ciclo.

2.3 O processo de GRSIC é composto por 6 (seis) subprocessos:

a) estabelecer contexto;

b) identificar riscos;

c) analisar riscos;

d) tratar riscos;

e) monitorar processo; e

f) comunicar partes interessadas.

2.3.1 Os subprocessos das alíneas "a", "b", "c" e "d" do item 2.3 devem ocorrer durante os ciclos de análise e tratamento dos riscos da unidade.

2.3.2 Os subprocessos das alíneas "e" e "f" do item 2.3 devem ocorrer durante os ciclos de análise e tratamento dos riscos e em seus interstícios, de modo que o processo possa estar em constante aprimoramento.

2.3.3 Abaixo, figura com a representação gráfica do processo de Gestão de Riscos em Segurança da Informação e Comunicações.

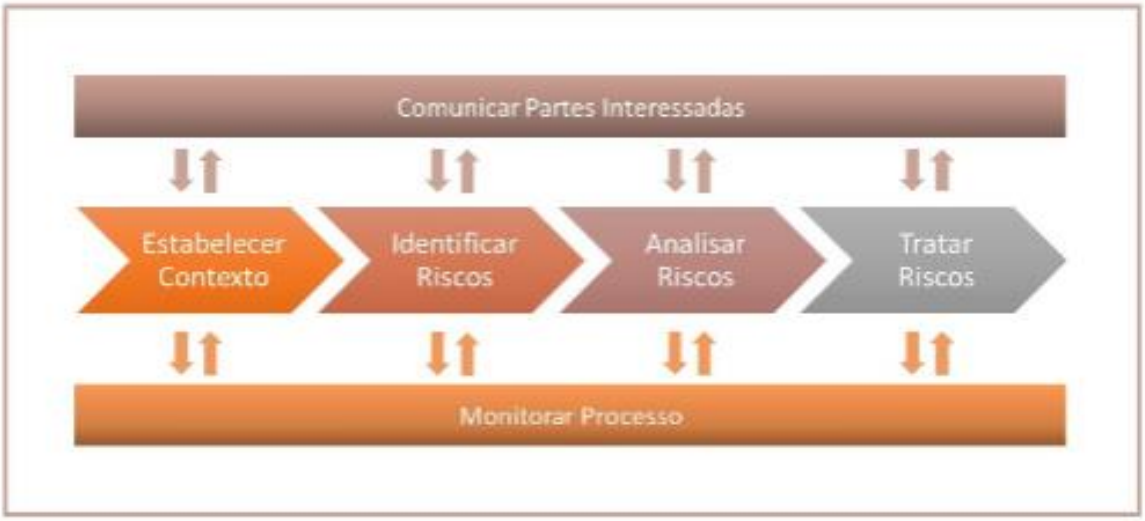


Figura I - Processo Gestão de Riscos em Segurança da Informação e Comunicações

2.4 O **Anexo I** desta norma detalha o processo de gestão de riscos em segurança da informação, indicando a descrição, objetivo, entradas e saídas de cada atividade.

2.5 Pode-se utilizar softwares específicos para o gerenciamento do processo bem como para a execução dos ciclos de análise.

2.5.1 Caso uma ferramenta de apoio à gestão de riscos de segurança da informação seja adotada, o Ministério deve disponibilizá-lo para todas as unidades executoras do processo de gestão de riscos, de modo que as informações e os resultados do processo estejam centralizadas e à disposição do Gestor de Segurança da Informação e Comunicações e do Comitê de Segurança da Informação e Comunicações.

3 RESPONSABILIDADES

3.1 O Gestor de Segurança da Informação e Comunicações é responsável pela coordenação do processo de gestão de riscos em segurança da informação, em atendimento à Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013.

3.2 O Gestor de Segurança da Informação e Comunicações poderá designar autoridades das unidades administrativas do MCTIC como Gestor de Riscos em Segurança da Informação e Comunicações, devendo conferir, no mínimo, as seguintes atribuições:

3.2.1 Análise, avaliação e tratamento dos riscos; e

3.2.2 Elaboração sistemática de relatórios de monitoramento da gestão de risco para o Gestor de Segurança da Informação e Comunicações, no qual deverá constar, dentre outras informações, a análise quanto à aceitação dos resultados obtidos e a consequente proposição de ajustes e de medidas preventivas e proativas à Alta Administração.

3.3 Os Gestores de Riscos em Segurança da Informação e Comunicações devem ser indicados entre os ocupantes de cargo de provimento em comissão do Grupo-Direção e Assessoramento Superiores (DAS), de nível 4 ou equivalente, ou de cargo de hierarquia superior.

3.4 O Gestor de Segurança da Informação e Comunicações ou os Gestores de Riscos de Segurança da Informação e Comunicações, quando devidamente autorizados, deverão indicar servidores, pertencentes às suas equipes, para formarem as Equipes de Gestão de Riscos em Segurança da Informação e Comunicações (ERSIC), que apoiarão na execução das atividades gerenciamento de riscos de segurança da informação previstas neste instrumento.

3.4.1 Os servidores que compõem as Equipes de Gestão de Riscos em Segurança da Informação e Comunicações (ERSIC) devem ser capacitados periodicamente em gestão de riscos.

4 VIGÊNCIA

Esta Norma entra em vigor na data de sua publicação.

Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		5/27

ANEXO I

DO PROCESSO DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÃO E COMUNICAÇÕES

1 OBJETIVO

Estabelecer o processo de Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) no Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), o qual proporcionará a identificação, a análise, a comunicação e o tratamento sistemático dos riscos encontrados.

2 TERMOS E DEFINIÇÕES

Para os efeitos desta norma, são estabelecidos os seguintes conceitos e definições:

2.1 **Ameaças** - conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

2.2 **Analisar Riscos** - processo para atribuir valores à probabilidade e consequências de um risco e para comparar o risco estimado com critérios de risco predefinidos para atribuir um valor ao risco;

2.3 **Ativo de informação** - os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como as instalações físicas onde se encontram esses meios e as pessoas que a eles têm acesso.

2.4 **Ciclo de análise e tratamento de riscos** - é a execução periódica dos processos de análise e tratamento dos riscos em segurança da informação. Os ciclos são compostos pelos processos "Estabelecer Contexto", "Identificar Riscos", "Analisar Riscos" e "Tratar Riscos".

2.5 **Comitê de Segurança da Informação e Comunicação (CSIC)** - grupo com a responsabilidade de avaliar, monitorar e direcionar as ações de segurança da informação.

2.6 **Comunicar Partes Interessadas** - processo para troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

2.7 **Confidencialidade** - propriedade de que a informação não esteja disponível ou revelada a pessoas, processos e outras entidades não autorizados.

2.8 **Controle de segurança** - qualquer ação, dispositivo, procedimento, técnica ou outra medida que reduza a probabilidade de ocorrência ou o grau de impacto decorrentes de um incidente de segurança.

2.9 **Disponibilidade** - propriedade da informação estar acessível e utilizável sob demanda por pessoas, sistemas e serviços autorizados.

Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		6/27

2.10 **Equipe de Gestão de Segurança da Informação e Comunicações (EGSIC)** - auxilia o Gestor de Riscos em Segurança da Informação e Comunicações no processo de gerenciamento de Riscos de Segurança da Informação nas unidades administrativas do MCTIC.

2.11 **Estabelecer Contexto** - processo para estabelecimento dos critérios que serão utilizados para o ciclo de análise e tratamento de riscos. Neste processo define o escopo, as restrições, os papéis e responsabilidades.

2.12 **Evitar risco** - uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver em uma situação de risco ou agir de forma a se retirar de uma situação de risco.

2.13 **Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)** - atividades coordenadas para direcionar e controlar a organização no que diz respeito a riscos de segurança da informação. O processo de gestão de riscos envolve a identificação, análise/avaliação, aceitação, tratamento, monitoramento e comunicação dos riscos.

2.14 **Gestor de Riscos em Segurança da Informação e Comunicações** - responsável pela unidade administrativa com atribuição de orientar, planejar, executar, monitorar e comunicar as ações de gerenciamento de riscos. Deve ser ocupante de cargo de provimento em comissão do Grupo-Direção e Assessoramento Superiores (DAS), de nível 4 ou equivalente, ou de cargo de hierarquia superior.

2.15 **Gestor de Segurança da Informação e Comunicações (GSIC)** - responsável pelas ações de segurança da informação e comunicações no âmbito do MCTIC

2.16 **Identificar Riscos** - processo para localizar, listar e caracterizar elementos do risco.

2.17 **Incidentes de segurança** - evento único ou uma série de eventos indesejados ou inesperados, que comprometa ou ameace a confidencialidade, integridade, disponibilidade ou qualquer outro requisito referente à segurança das informações. O não cumprimento da política e normas de segurança da organização também é considerado um incidente.

2.18 **Integridade** - propriedade de salvaguarda da exatidão e completeza da informação. A certeza de que uma informação não foi modificada de forma não autorizada.

2.19 **Lições aprendidas** - artefato que contém as lições aprendidas durante o processo de gestão de riscos em segurança da informação e comunicações

2.20 **Mapa de Riscos** - artefato produzido na etapa de análise de riscos o qual conterá a análise dos riscos identificados, indicando qual o valor do risco e seu respectivo nível. Este artefato pode ser uma atualização do Artefato Relação de Riscos.

2.21 **Monitorar Processo** - processo transversal de acompanhamento das atividades e dos resultados gerado em cada ciclo do processo, bem como o acompanhamento do processo em si.

2.22 **Plano de Comunicação** - artefato utilizado para a realização das comunicações durante os ciclos de análise do processo de gestão de riscos em segurança da informação. Deve conter quem deverá ser comunicado, o que deverá ser comunicado, quando deverá ser comunicado e como deverá ser comunicado.

Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		7/27

2.23 **Plano de Contexto** - artefato produzido na etapa de planejamento do processo, o qual conterá a delimitação do escopo da gestão de riscos em segurança da informação, as restrições, as ações a serem tomadas, as tomadas de decisão, os papéis e as responsabilidades.

2.24 **Plano de Tratamento de Riscos** - artefato produzido na etapa de tratamento de riscos que apresenta as ações que serão tomadas para cada risco identificado, bem como apresenta os riscos residuais que deverão ser aceitos formalmente pelo gestor responsável.

2.25 **Proposta de melhorias** - artefato que apresenta as propostas de melhorias a serem realizadas no processo de gestão de riscos em segurança da informação ou, pontualmente, nos ciclos de análise e avaliação de riscos.

2.26 **Reduzir risco** - uma 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.

2.27 **Relação de Riscos** - artefato produzido na etapa de identificação de riscos o qual conterá o inventário dos ativos, bem como as características de cada ativo, controles implementados, ameaças as quais estão sujeitos e as vulnerabilidades.

2.28 **Aceitar risco** - uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.

2.29 **Risco de segurança da informação** - combinação entre a probabilidade de ocorrência de um incidente de segurança e as suas consequências;

2.30 **Risco Residual** - risco encontrado após a definição e devido tratamento do risco inicial. Este risco deve ser formalmente aceito pelo gestor responsável e continuamente monitorado.

2.31 **Segurança da informação** - preservação dos requisitos de segurança das informações do MCTIC ou sob sua responsabilidade;

2.32 **Sistema de Gestão de Segurança da Informação (SGSI)** - conjunto de políticas, normas, processos, procedimentos e controles para gerir a segurança da informação, a partir de uma abordagem de risco ao negócio.

2.33 **Termo de Aceite de Riscos** - artefato de aceite formal dos riscos residuais.

2.34 **Termo de Conclusão do Plano de Tratamento de Riscos** - artefato de aceite formal de conclusão do tratamento dos riscos identificados no Plano de Tratamento de Riscos.

2.35 **Transferir risco** - uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco.

2.36 **Tratar Riscos** - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, aceitar ou transferir um risco.

2.37 **Unidade administrativa** - são as unidades que compõem os órgãos da estrutura da Pasta. São as Secretarias, Diretorias, Assessorias, Coordenações-Gerais entre outras.

2.38 **Vulnerabilidades** - 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.

3 PROCESSO DE GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

3.1 O processo de Gestão de Riscos de Segurança da Informação contempla os grupos de processos relacionados ao estabelecimento do contexto da organização, seus objetivos e restrições, passando pela identificação de riscos, pela análise dos riscos identificados e pela definição do tratamento necessário para tais riscos. Também se executa, durante todo o ciclo do processo de gestão de riscos em segurança da informação, os processos de comunicação e monitoramento contínuo dos resultados obtidos.

3.2 As atividades de cada grupo de processo estão detalhadas nos itens seguintes deste Anexo, com a apresentação do objetivo, da descrição, do responsável, das entradas e das saídas.

4 PROCESSO ESTABELECER CONTEXTO

4.1 Este é o processo no qual todos os critérios e predefinições que serão utilizados em todo o processo de GRSIC são definidos, tal como o escopo da GRSIC, suas restrições, as ações, as tomadas de decisão, os papéis e as responsabilidades.

4.2 Essas informações deverão ser consolidadas em um documento denominado de Plano de Contexto, que deverá ser aprovado pela autoridade máxima da unidade, devendo ser comunicado às partes interessadas ao final desta etapa, bem como sempre que houver alguma mudança em tal documento, conforme estabelecido no plano de comunicação.

4.3 A figura abaixo ilustra as atividades do processo de Estabelecer Contexto.

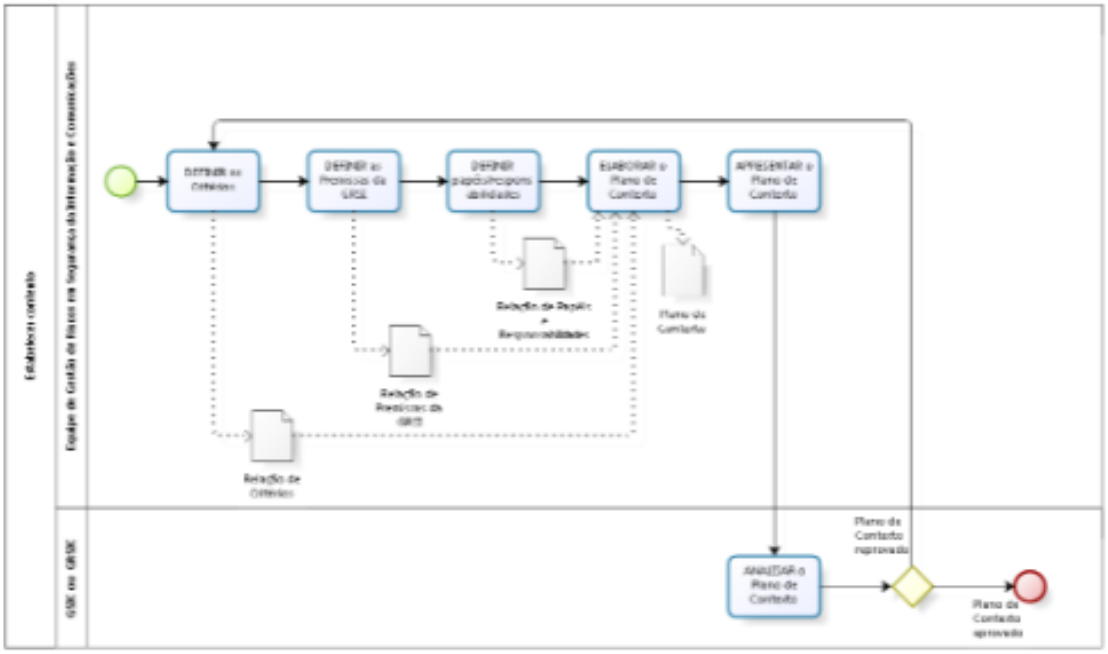


Figura I - Processo Estabelecer Contexto.

4.4 Detalhamento das atividades

4.4.1 Definir os Critérios

4.4.1.1 Objetivo: definir os valores base para a gestão de riscos.

4.4.1.2 Descrição: os critérios básicos para a GRSIC deverão ser definidos nesta atividade. Estes critérios incluem:

a) critério de relevância do ativo;

b) critério de probabilidade de materialização do risco;

c) critério de impacto aos ativos no caso de materialização do risco; e

d) critério de nível de risco.

4.4.1.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

4.4.1.4 Entrada: início do processo de GRSIC determinado pelo Gestor de Segurança da Informação e Comunicações ou pelo Gestor de Riscos em Segurança da Informação e Comunicações.

4.4.1.5 Saída: relação de critérios da GRSIC definida.

4.4.2 Definir as Premissas da GRSIC

4.4.2.1 Objetivo: definir as premissas gerais do processo de GRSIC.

4.4.2.2 Descrição: o que se pretende com a GRSIC, o que será feito e quais suas limitações para isto (técnicas, operacionais, financeiras etc.) deverão ser apontadas nesta tarefa. Deve-se definir as premissas do processo de GRSIC. Elas é que determinarão os limites da GRSIC. Estas premissas incluem:

a) Objetivo da GRSIC;

b) Escopo da GRSIC; e

c) Restrições da GRSIC.

4.4.2.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

4.4.2.4 Entrada: relação de critérios da GRSIC definida.

4.4.2.5 Saída: relação das premissas da GRSIC definida.

4.4.3 Definir os Papéis e Responsabilidades

4.4.3.1 Objetivo: definir os papéis e as responsabilidades no contexto do processo de GRSIC.

4.4.3.2 Descrição: cada um dos atores do processo de GRSIC, bem como suas responsabilidades, deverão ser elencados e consolidados à fim de que não restem dúvidas sobre o papel de cada um no processo. Os papéis e as responsabilidades deverão abranger também os responsáveis e eventuais demandados para operacionalizar alguma atividade. Informações mínimas sobre o papel, a responsabilidade e como foi dada a designação deverão ser relacionadas.

4.4.3.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

4.4.3.4 Entrada: relação das premissas da GRSIC definida.

4.4.3.5 Saída: relação de papéis e responsabilidades definida.

4.4.4 Elaborar o Plano de Contexto

4.4.4.1 Objetivo: elaborar o documento que consolide todas as diretrizes gerais da GRSIC.

4.4.4.2 Descrição: todas as informações produzidas nas atividades anteriores precisam ser consolidadas no Plano de Contexto, que é um documento único, sucinto, de fácil leitura e entendimento. Este documento norteará a execução da GRSIC e deverá ser revisado periodicamente, sempre que alguma das informações sofrer alterações, tais como ampliação do escopo, aumento ou diminuição de restrições, revisão de critérios, níveis de riscos etc.

4.4.4.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

4.4.4.4 Entrada: relação de critérios, relação de premissas da GRSIC e relação de papéis e responsabilidades definidas.

4.4.4.5 Saída: Artefato Plano de Contexto elaborado.

4.4.5 Apresentar o Plano de Contexto

4.4.5.1 Objetivo: apresentar o plano de contexto para a autoridade da unidade.

4.4.5.2 Descrição: a apresentação do Plano de Contexto deverá ser realizada em reunião presencial, ou por outro meio adequado, para que a autoridade tenha conhecimento e possa deliberar sobre o conteúdo do Plano.

4.4.5.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

4.4.5.4 Entrada: Artefato Plano de Contexto elaborado.

4.4.5.5 Saída: Artefato Plano de Contexto apresentado.

4.4.6 Analisar o Plano de Contexto

4.4.6.1 Objetivo: analisar o Plano de Contexto apresentado.

4.4.6.2 Descrição: a análise e a aprovação do Plano de Contexto são etapas fundamentais a serem executada no processo de GRSIC e deve ser realizada pelos Gestores, com apoio da Equipe de Riscos. Esta aprovação deve ser formal, demonstrando o comprometimento da autoridade com o processo de gestão de riscos.

4.4.6.3 Responsável: Gestor de Segurança da Informação e Comunicações ou Gestor de Riscos em Segurança da Informação e Comunicações

4.4.6.4 Entrada: Artefato Plano de Contexto.

4.4.6.5 Saída: Artefato Plano de Contexto aprovado.

5 PROCESSO IDENTIFICAR RISCOS

5.1 Neste processo, todos os elementos relacionados à materialização do risco serão identificados, bem como serão executadas as atividades operacionais de levantamento das possíveis ameaças e das vulnerabilidades dos ativos.

5.2 Este processo é o que mais demanda tempo e dedicação por parte da Equipe de Riscos. Este processo pode ser realizado com apoio técnico especializado, de acordo com o tipo de ativo analisado, bem como pode envolver outras equipes técnicas de diferentes áreas do Ministério.

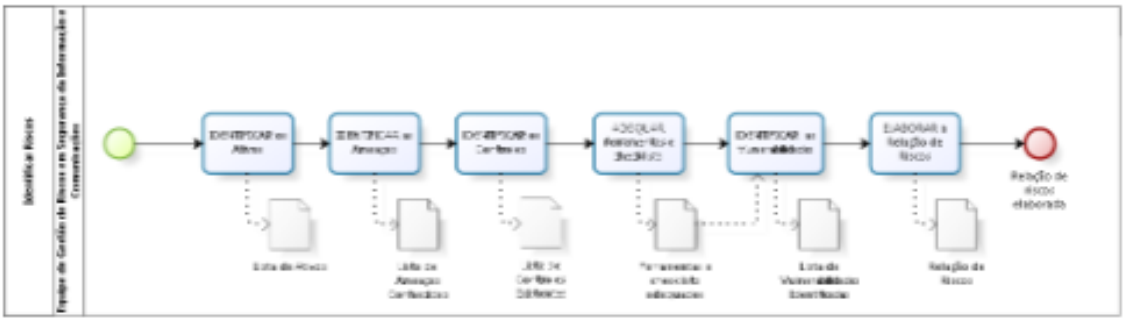


Figura II – Processo Identificar Riscos

5.3 Detalhamento das atividades

5.3.1 Identificar os Ativos

5.3.1.1 Objetivo: identificar os ativos de informação relacionados ao escopo da GRSIC.

5.3.1.2 Descrição: o plano de contexto define o escopo da GRSIC que, por sua vez, precisa ser explorado neste processo. Os ativos de informação que fazem parte do escopo da análise deverão ser identificados e detalhados, de forma que nenhuma informação relevante para a análise de riscos falte, minimizando o risco de comprometer o resultado final da análise. Os resultados da análise são diretamente proporcionais aos níveis de detalhes obtidos em cada um dos ativos de informação. O valor do ativo, de acordo com o plano de contexto, também deverá ser definido nesta etapa.

5.3.1.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

5.3.1.4 Entrada: Artefato Plano de Contexto aprovado.

5.3.1.5 Saída: lista de ativos de informação relacionados ao escopo da GRSIC.

5.3.2 Identificar as Ameaças

5.3.2.1 Objetivo: identificar as ameaças que possam comprometer os ativos de informação da organização.

5.3.2.2 Descrição: as ameaças à que a unidade está exposta devem ser mapeadas, estando ou não relacionadas ao escopo da GRSIC. Ressalta-se que a relação de ameaças pode variar com o tempo, sendo necessário revisá-la em todos os ciclos de análise. Os incidentes de segurança podem fornecer informações sobre as ameaças a que a unidade está sujeita.

5.3.2.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

5.3.2.4 Entrada: lista de ativos de informação relacionados ao escopo da GRSIC.

5.3.2.5 Saída: lista de ameaças conhecidas.

5.3.3 Identificar os Controles

5.3.3.1 Objetivo: identificar os controles de segurança existentes e implementados nos ativos de informação da organização que pertencem ao escopo da GRSIC.

5.3.3.2 Descrição: controles de segurança que já estejam implementados nos ativos de informação relacionados ao escopo em análise devem ser identificados, uma vez que o cálculo do risco considera este elemento como fator para determinar o impacto causado por uma ameaça ao explorar uma vulnerabilidade. Ativos com controles pré-definidos e implementados tendem a representar menos riscos do que aqueles sem controles.

5.3.3.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

5.3.3.4 Entrada: lista de ativos de informação relacionados ao escopo da GRSIC.

5.3.3.5 Saída: lista de ativos de informação relacionados ao escopo da GRSIC e os controles existentes relacionados.

5.3.4 Adequar as ferramentas e as listas de verificação (*checklists)*

5.3.4.1 Objetivo: adequar as ferramentas e elaborar as listas de verificação (*checklists)* que serão utilizados para a identificação das vulnerabilidades dos ativos de informação.

5.3.4.2 Descrição: anteriormente à verificação das vulnerabilidades, deve-se preparar o ferramental para identificação das vulnerabilidades, bem como os controles a serem implementados para atuação junto às vulnerabilidades identificadas. Esta atividade é essencial à análise, pois a qualidade do resultado obtido se dá em função da qualidade das bases de conhecimento utilizadas. É recomendável que, quando possível, se utilize mais de uma ferramenta de coleta automatizada para os ativos de informação, em conjunto com *checklists* manuais que complementarão as análises automatizadas e serão aplicáveis aos demais ativos que não suporte coleta automatizada. Esta atividade requer que a Equipe de Gestão de Riscos em Segurança da Informação e Comunicações tenha um conhecimento técnico sobre todos os processos de negócios e os ativos de TIC previstos no escopo da análise. Caso a Equipe não detenha este conhecimento, é recomendável a utilização de um apoio técnico especializado.

5.3.4.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

5.3.4.4 Entrada: lista de ativos de informação relacionados ao escopo.

5.3.4.5 Saída: ferramentas e listas de verificação (*checklists)* adequados ao escopo.

5.3.5 Identificar as Vulnerabilidades

5.3.5.1 Objetivo: identificar as vulnerabilidades presentes nos ativos de informação relacionados ao escopo da GRSIC.

5.3.5.2 Descrição: os ativos de informação podem conter vulnerabilidades que, se exploradas por uma ameaça, comprometem o ativo e as respectivas informações geradas, tratadas ou armazenadas. As ferramentas utilizadas para este levantamento devem ser adequadas ao escopo. Quanto mais bem detalhado for a lista de ativos, melhor serão os resultados da identificação de vulnerabilidades.

5.3.5.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

5.3.5.4 Entrada: lista de ativos e ferramentas e listas de verificação adequados ao escopo da análise.

5.3.5.5 Saída: lista de vulnerabilidades dos ativos de informação relacionados ao escopo da análise.

5.3.6 Elaborar a Relação de Riscos

5.3.6.1 Objetivo: relacionar os riscos identificados nos ativos de informação que fazem parte do escopo da análise.

5.3.6.2 Descrição: ao final do processo, todas as informações relacionadas aos ativos, suas ameaças, vulnerabilidades e controles existentes deverão ser organizadas de tal forma que os riscos relacionados estejam aptos a serem analisados e ter o tratamento devido priorizado no próximo processo. A relação de riscos, neste contexto, nada mais é do que a correlação de informações já identificadas nas etapas anteriores.

5.3.6.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

5.3.6.4 Entrada: lista de ativos de informação relacionados ao escopo da GRSIC e suas ameaças conhecidas, vulnerabilidades identificadas e controles existentes.

5.3.6.5 Saída: Artefato Relação de Riscos.

6 PROCESSO ANALISAR RISCOS

6.1 O processo de analisar os riscos é o processo em que se avalia a probabilidade de materialização do risco e o impacto que ele possa causar aos ativos de informação.

6.2 A critério do Gestor de Riscos em Segurança da Informação, pode-se utilizar a matriz de valor do ativo, probabilidade e impacto, resultando na mensuração do risco ou apenas a matriz de valor de probabilidade e impacto. Orienta-se que o valor do ativo seja utilizado no cálculo do

risco quando houver variedade de ativos no escopo, de modo que a sua valoração aprimore o cálculo do risco.

6.3 Deste modo, tem-se duas fórmulas de cálculo de risco possíveis:

a) VR = VA x VP x VI, no qual VR é valor do risco; VA é valor do ativo; VP é valor da probabilidade; e VI é valor do impacto. Os valores do ativo, probabilidade e impacto podem variar de 1 a 5, conforme definição no Plano de Contexto. Deste modo, o valor do risco poderá ser de 1 a 125.

b) VR = VP x VI, no qual VR é valor do risco; VA é valor do ativo; VP é valor da probabilidade; e VI é valor do impacto. Os valores de probabilidade e impacto podem variar de 1 a 5, conforme definição no Plano de Contexto. Deste modo, o valor do risco poderá ser de 1 a 25.

6.4 Ao final do cruzamento de tais informações, um mapa de riscos deverá ser elaborado para que a organização conheça os riscos à que está sujeita e consiga definir mais facilmente os tratamentos necessários.

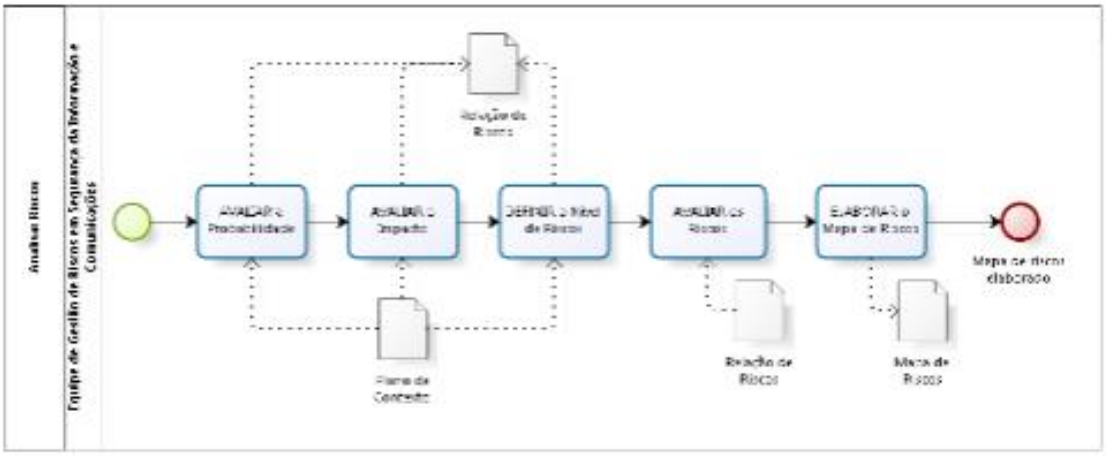


Figura III – Processo Analisar Riscos

6.5 Detalhamento das atividades

6.5.1 Avaliar a Probabilidade

6.5.1.1 Objetivo: avaliar a probabilidade de materialização dos riscos identificados na análise.

6.5.1.2 Descrição: a probabilidade (ou estimativa de frequência) de ocorrência de um evento que possa incorrer em um risco para a organização deverá ser determinada para cada um dos riscos identificados no decorrer da análise. Os valores a serem utilizados para determinar esta ocorrência deverão estar de acordo com os padrões predefinidos no plano de contexto.

6.5.1.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

6.5.1.4 Entrada: Artefato Plano de Contexto e Artefato Relação de Riscos.

6.5.1.5 Saída: Artefato Relação de Riscos atualizado.

6.5.2 Avaliar o Impacto

6.5.2.1 Objetivo: avaliar o impacto dos riscos identificados na análise.

6.5.2.2 Descrição: o impacto, resultante ou decorrente de um evento relacionado aos ativos de informação em análise, deve ser determinado para cada um dos riscos identificados. Os valores a serem utilizados para determinar esta ocorrência deverão estar de acordo com os padrões predefinidos no plano de contexto. Para cada risco identificado deverá ser avaliado o impacto na confidencialidade, integridade e/ou disponibilidade da informação ou do ativo de informação.

6.5.2.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

6.5.2.4 Entrada: Artefato Plano de Contexto e Artefato Relação de Riscos.

6.5.2.5 Saída: Artefato Relação de Riscos atualizado.

6.5.3 Definir o Nível de Riscos

6.5.3.1 Objetivo: definir o nível dos riscos identificados na análise, conforme estabelecido no Plano de Contexto.

6.5.3.2 Descrição: o nível de risco para a organização deverá ser determinado para cada um dos riscos identificados. Os valores utilizados deverão estar de acordo com os padrões predefinidos no Artefato Plano de Contexto.

6.5.3.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

6.5.3.4 Entrada: Artefato Plano de Contexto e Artefato Relação de Riscos.

6.5.3.5 Saída: Artefato Relação de Riscos atualizado.

6.5.4 Avaliar os Riscos

6.5.4.1 Objetivo: avaliar os riscos identificados na análise e compará-los com os requisitos e predefinições estipuladas para o processo de GRSIC.

6.5.4.2 Descrição: após a definição de todos os valores relacionados aos cálculos do risco e à identificação do valor do risco para cada risco, uma avaliação dos riscos deve ser realizada por meio da verificação dos resultados dos cálculos executados e dos resultados obtidos e compará-

los com os parâmetros predefinidos no plano de contexto. Esta etapa pressupõe uma atividade menos mecânica e mais analítica, inclusive contemplando uma avaliação mais subjetiva que tem por objetivo verificar se os resultados identificados realmente fazem sentido dentro do contexto da GRSIC.

6.5.4.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

6.5.4.4 Entrada: Artefato Plano de Contexto e Artefato Relação de Riscos.

6.5.4.5 Saída: Artefato Relação de Riscos atualizado.

6.5.5 Elaborar o Mapa de Riscos

6.5.5.1 Objetivo: elaborar o Artefato Mapa de Riscos, com os riscos identificados na análise.

6.5.5.2 Descrição: o Artefato Mapa de Riscos deverá ser elaborado por meio do cruzamento dos valores possíveis entre o valor do ativo, a probabilidade e o impacto por meio de um gráfico, onde será possível identificar claramente a quantidade de riscos para cada nível de risco levantado anteriormente. O mapa de riscos também deverá conter toda e qualquer informação que possa ser resgatada da lista de riscos e que possa ser apresentada de forma gráfica, auxiliando, assim, os Gestores e a organização na tomada de decisões em relação ao tratamento dos riscos. Dependendo da ferramenta utilizada, o Artefato Mapa de Riscos pode ser uma atualização do Artefato Relação de Riscos.

6.5.5.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

6.5.5.4 Entrada: Artefato Plano de Contexto e Artefato Relação de Riscos.

6.5.5.5 Saída: Artefato Mapa de Riscos elaborado.

7 PROCESSO TRATAR RISCOS

7.1 Este é o processo em que tudo aquilo que for necessário, aplicável e que estiver ao alcance da organização para tratar os riscos deverá ser definido e ter sua execução planejada e, por fim, executada.

7.2 Avaliar a possibilidade de aplicação dos controles do ponto de vista operacional, financeiro e de recursos humanos são atividades essenciais nesta etapa, uma vez que nem sempre o tratamento poderá evitar ou reduzir de fato os riscos, o que remete a maneiras diferentes de lidar com eles, inclusive compartilhando-os, se for o caso.

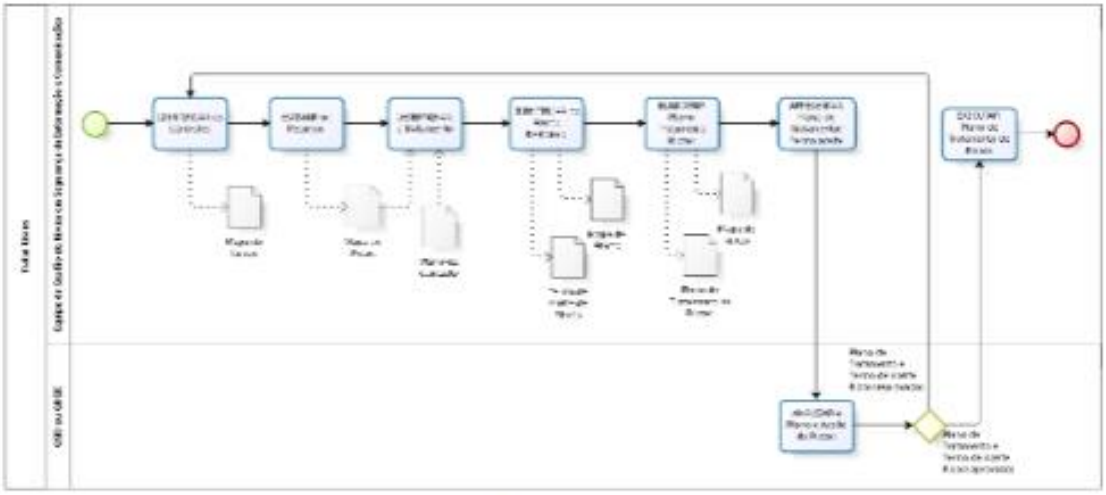


Figura IV – Processo Tratar os Riscos

7.3 Detalhamento das atividades

7.3.1 Identificar os Controles

7.3.1.1 Objetivo: identificar os controles necessários para a redução ou eliminação dos riscos indicados.

7.3.1.2 Descrição: identificar os controles necessários para eliminar os riscos ou diminuir seu impacto ou probabilidade é um dos objetivos de uma análise de riscos. Sistemas automatizados de detecção de vulnerabilidades normalmente trazem sugestões de controles para a correção dos problemas, mas estas sugestões não diminuem a importância de um trabalho analítico e minucioso para definir quais os controles mais eficazes e efetivos.

7.3.1.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

7.3.1.4 Entrada: Artefato Relação de Riscos, Artefato Mapa de Riscos, ferramentas e listas de verificação.

7.3.1.5 Saída: relação de controles identificados.

7.3.2 Estimar os Recursos

7.3.2.1 Objetivo: estimar os recursos necessários ao tratamento dos riscos.

7.3.2.2 Descrição: após identificar os controles aplicáveis, é necessário identificar os recursos necessários para a efetiva implementação dos controles, tais como os recursos humanos (quem vai fazer), financeiros (quanto custa para fazer), operacionais (como vai fazer) e de tempo (quando vai fazer). Esta tarefa é essencial para que a organização possa decidir sobre a

implementação dos controles ou não, uma vez que nem sempre há recursos humanos disponíveis ou o custo acaba sendo tão elevado a ponto de inviabilizar sua implementação, o que faz com que a organização passe a aceitar esses riscos.

7.3.2.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

7.3.2.4 Entrada: Artefato Relação de Riscos, Artefato Mapa de Riscos, ferramentas e listas de verificação.

7.3.2.5 Saída: relação de recursos necessários estimados.

7.3.3 Determinar o Tratamento

7.3.3.1 Objetivo: determinar, dentre as possibilidades, aquela que melhor se encaixa como opção para o tratamento.

7.3.3.2 Descrição: após definir os controles a serem aplicados e os recursos necessários, é necessário realizar um trabalho analítico acerca das possibilidades de tratamento para cada risco identificado. Os riscos poderão ser modificados, retidos, evitados ou compartilhados. O tratamento dos riscos deve considerar, ainda, o estabelecido no plano de contexto. Abaixo, descrição de cada tratamento.

a) Reduzir o risco:

- objetivo: definir os controles, dentre os possíveis, com intuito de diminuir o nível de risco identificado, sem eliminá-lo por completo.

- descrição: reduzir o risco significa diminuir a sua probabilidade ou o seu impacto, caso se materialize. Contudo, não evita o risco por completo. A redução como forma de tratamento de um risco geralmente ocorre por limitação de recursos. Nesta situação, apenas uma parte dos controles aplicáveis é implementada e seu residual deverá ser aceito e monitorado.

b) Aceitar o risco:

- objetivo: determinar que os riscos identificados serão aceitos pela organização.

- descrição: aceitar um risco não irá interferir em seu valor nem em seu potencial impacto ou probabilidade de ocorrer. O risco continua existindo do mesmo modo, contudo, é aceito pela organização. A retenção geralmente ocorre por conta da limitação de recursos para a implementação de controles ou pelo baixo nível que representa, de modo que os recursos alocados podem fazer com que se torne mais dispendioso tratá-lo. Riscos retidos devem ser monitorados constantemente e formalmente aceitos.

c) Evitar o risco;

- objetivo: definir os controles, dentre os possíveis, com intuito de eliminar por completo os riscos identificados.

- descrição: evitar um risco irá eliminá-lo por completo e não apenas alterar seu valor. Sempre que possível, os riscos deverão ser evitados. Porém, considerando sempre as condições para que isto possa ocorrer, sem que a organização seja penalizada por ter alocado recursos excessivos, o que pode trazer prejuízos. Controles efetivos não estão diretamente relacionados à grande alocação de recursos, mas sim à capacidade analítica da equipe responsável por determinar o tratamento dos riscos.

d) Transferir o risco;

- objetivo: transferir a terceiros os impactos ocasionados pela possível materialização dos riscos identificados.

- descrição: transferir o risco é uma forma de tratá-lo repassando a outrem a responsabilidade no caso de sua materialização. Seguros que cubram as consequências de materialização de um risco podem ser uma maneira de terceirizar um risco.

7.3.3.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

7.3.3.4 Entrada: Artefato Relação de Riscos, Artefato Mapa de Riscos, ferramentas e listas de verificação.

7.3.3.5 Saída: tratamento dos riscos definidos

7.3.4 Identificar os Riscos Residuais

7.3.4.1 Objetivo: identificar quais são os riscos residuais após a definição de tratamento de riscos e elaborar o termo de aceite de riscos.

7.3.4.2 Descrição: após definido o tratamento para os riscos e este tratamento ser considerado satisfatório do ponto de vista legal, operacional, financeiro, de recursos humanos e tempo, podem restar riscos residuais. Os riscos residuais são todos os riscos assim determinados pelo plano de contexto com nível de risco mínimo para tratamento, além dos riscos resultantes do tratamento de redução. Normalmente riscos muito baixos são considerados riscos residuais pois os custos de implementação de controles ultrapassam o benefício que possa ser gerado. Os riscos residuais deverão ser relacionados, formalmente aceitos pela organização e monitorados.

7.3.4.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

7.3.4.4 Entrada: Artefato Relação de Riscos, Artefato Mapa de Riscos, ferramentas e listas de verificação.

7.3.4.5 Saída: riscos residuais identificados e Artefato Termo de Aceite de Riscos.

7.3.5 Elaborar o Plano de Tratamento de Riscos

7.3.5.1 Objetivo: consolidar o plano de tratamento de riscos e as ações a serem adotadas.

Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		21/27

7.3.5.2 Descrição: o plano de tratamento dos riscos é um consolidado geral com a definição de tratamento para cada risco, contendo, assim, informações sobre os responsáveis pela implementação dos controles, o prazo para tal implementação, os recursos necessários e o status de tais atividades. O plano de tratamento não é imutável, devendo ser reavaliado quando necessário. O plano deve ser implementado para que os riscos sejam efetivamente tratados.

7.3.5.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

7.3.5.4 Entrada: Artefato Relação de Riscos, Artefato Mapa de Riscos, ferramentas e listas de verificação, Artefato Termo de Aceite de Riscos.

7.3.5.5 Saída: Artefato Plano de Tratamento de Riscos elaborado.

7.3.6 Apresentar Plano de Tratamento / Termo de Aceite

7.3.6.1 Objetivo: apresentar o plano de tratamento e o termo de aceite para a autoridade da unidade.

7.3.6.2 Descrição: a apresentação do plano de tratamento e do termo de aceite deverá ser realizada em reunião presencial, ou por outro meio adequado, para que a autoridade tenha conhecimento e possa deliberar sobre o conteúdo do plano e do termo.

7.3.6.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

7.3.6.4 Entrada: Artefato Plano de Tratamento de Riscos e Artefato Termo de Aceite de Riscos.

7.3.6.5 Saída: Artefato Plano de Tratamento de Riscos e Artefato Termo de Aceite de Riscos apresentados.

7.3.7 Analisar Plano de Tratamento / Termo de Aceite

7.3.7.1 Objetivo: analisar o plano de tratamento e o termo de aceite apresentados.

7.3.7.2 Descrição: é fundamental a análise e aprovação do plano de tratamento e do termo de aceite pelo Gestor de Segurança da Informação e Comunicações ou Gestor de Riscos em Segurança da Informação e Comunicações, com apoio da Equipe de Riscos. Esta aprovação deve ser formal, demonstrando o comprometimento da autoridade com o processo de gestão de riscos.

7.3.7.3 Responsável: Gestor de Segurança da Informação e Comunicações ou Gestor de Riscos em Segurança da Informação e Comunicações.

7.3.7.4 Entrada: Artefato Plano de Tratamento de Riscos e Artefato Termo de Aceite de Riscos.

7.3.7.5 Saída: Artefato Plano de Tratamento de Riscos e Artefato Termo de Aceite de Riscos aprovados.

Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		22/27

7.3.8 Executar Plano de Tratamento de Riscos

7.3.8.1 Objetivo: executar o plano de tratamento de riscos, com o intuito de tratar os riscos conforme as definições do próprio plano.

7.3.8.2 Descrição: esta atividade consiste no tratamento dos riscos, por meio da execução do plano de tratamento. Deve-se estar atento à execução fiel do plano, para que os riscos sejam tratados (reduzir, evitar, reter ou compartilhar) conforme o planejado e aprovado. Durante a execução do plano podem surgir necessidades de ajustes ao plano, o que deverá ser feito pelo Equipe de Riscos e aprovado pelo Gestor.

7.3.8.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

7.3.8.4 Entrada: Artefato Plano de Tratamento de Riscos.

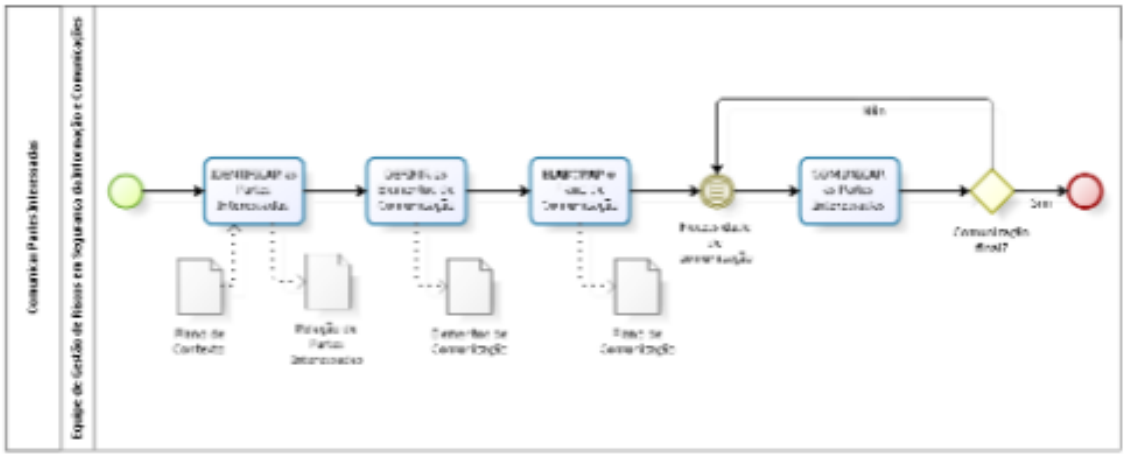
7.3.8.5 Saída: Artefato Termo de Conclusão do Plano de Tratamento de Riscos.

8 PROCESSO COMUNICAR PARTES INTERESSADAS

8.1 O processo de comunicação é transversal e tem como finalidade comunicar as partes interessadas, a qualquer momento, o status do processo de GRSIC. Por ser um processo transversal, ocorre desde o início do processo, durante o estabelecimento do contexto, até o término do tratamento dos riscos.

8.2 Portanto, a comunicação deverá ocorrer de maneira formal sempre que necessário, tanto em relação à execução do processo e seus resultados, como em relação ao gerenciamento do processo.

8.3 O plano de comunicação deve ser elaborado em paralelo ao plano de contexto, de modo que seja possível identificar todas as partes interessadas, bem como os elementos de comunicação, no início de cada ciclo de análise, possibilitando uma comunicação adequada.



Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		23/27

Figura V – Processo Comunicar Partes Interessadas

8.4 Detalhamento das atividades

8.4.1 Identificar as Partes Interessadas

8.4.1.1 Objetivo: identificar as partes que devem ser comunicadas sobre o andamento e os resultados do processo.

8.4.1.2 Descrição: a comunicação dentro do processo de GRSIC é elemento essencial e, para que seja efetiva, deve ser realizada de forma organizada e direcionada apenas às partes interessadas. Para tanto, deve-se identificar, nos diversos níveis da unidade, quais são as pessoas que devem ser comunicadas.

8.4.1.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

8.4.1.4 Entrada: organograma da unidade, lista de recursos, plano de contexto.

8.4.1.5 Saída: relação de partes interessadas.

8.4.2 Definir os Elementos de Comunicação

8.4.2.1 Objetivo: identificar o que deve ser comunicado às partes interessadas sobre o andamento, gerenciamento e os resultados do processo.

8.4.2.2 Descrição: após definir a quem comunicar, é necessário definir o que quer comunicar, quando comunicar, por que meios comunicar e se será necessária alguma interação com as partes comunicadas, além do controle do status de cada comunicado, formando, assim, um plano de comunicação formal.

8.4.2.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

8.4.2.4 Entrada: relação das partes interessadas, Artefato Plano de Contexto.

8.4.2.5 Saída: relação de partes interessadas.

8.4.3 Elaborar o Plano de Comunicação

8.4.3.1 Objetivo: elaborar o plano de comunicação, documento que auxilia todas as comunicações realizadas no âmbito do processo de GRSIC.

8.4.3.2 Descrição: após identificar as partes interessadas e definir os elementos necessários para a comunicação, é necessário unir todos estes itens no Plano de Comunicação que deverá servir de controle sobre as comunicações a serem realizadas pelo processo de GRSIC. O Plano deve ser atualizado sempre que necessário.

8.4.3.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

8.4.3.4 Entrada: relação das partes interessadas, Artefato Plano de Contexto.

8.4.3.5 Saída: Artefato Plano de Comunicação elaborado.

8.4.4 Necessidade de Comunicação

8.4.4.1 Após a elaboração do plano de comunicação, o processo irá aguardar a ocorrência do evento "necessidade de comunicação" para seguir para a próxima atividade. Todas as necessidades de comunicação estarão descritas no plano de comunicação, tal como a comunicação sobre o plano de contexto, mapa de riscos, plano de tratamento. Assim, quando surgir a necessidade de comunicação, o plano deverá ser acionado para a realização da comunicação.

8.4.5 Comunicar as Partes Interessadas

8.4.5.1 Objetivo: efetuar a comunicação das partes interessadas conforme a necessidade de comunicação, em atenção ao plano de comunicação.

8.4.5.2 Descrição: elaborado o plano de comunicação, as partes interessadas deverão ser comunicadas conforme o planejamento, respeitando o destinatário da comunicação, o prazo, seu conteúdo e a necessidade ou não de a parte interessada dar um feedback sobre o conteúdo comunicado. A comunicação é o ato formal que faz a organização tomar conhecimento acerca da GRSIC e de seu processo como um todo. As partes deverão ser comunicadas, conforme previsão do plano de comunicação, do início ao fim do processo de gestão de riscos. Deste modo, sempre que houver a necessidade, a atividade de comunicar as partes interessadas deverá ser realizada.

8.4.5.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

8.4.5.4 Entrada: Artefato Plano de Comunicação.

8.4.5.5 Saída: comunicação às partes interessadas realizada.

9 PROCESSO MONITORAR PROCESSOS

9.1 O processo de monitorar o processo é transversal e tem como objetivo acompanhar as atividades os resultados gerados em cada ciclo do processo, bem como acompanhar o processo em si, visando o seu aprimoramento.

9.2 Por meio do monitoramento, a organização passa a ter conhecimento sobre o andamento da gestão de riscos como um todo, podendo, assim, identificar pontos de falhas e melhorias a serem implementadas para que os resultados esperados possam ser plenamente alcançados, além de monitorar os resultados propriamente ditos e saber se estão de acordo com o planejado.

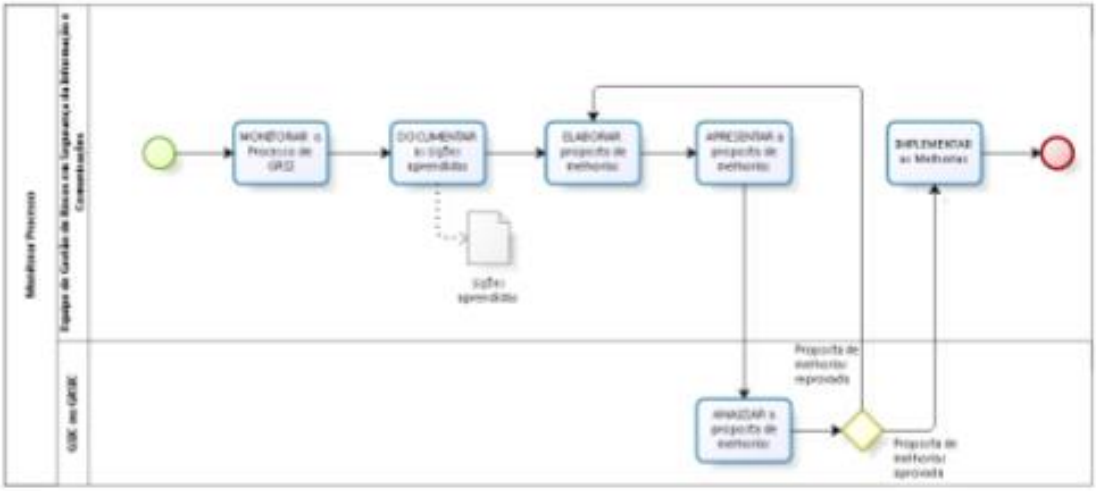


Figura VI – Processo Monitorar Riscos

9.3 Detalhamento das atividades

9.3.1 Monitorar o Processo de GRSIC

9.3.1.1 Objetivo: monitorar o fluxo do processo de GRSIC, avaliando sua estrutura, fluxo de trabalho e artefatos.

9.3.1.2 Descrição: monitorar todas as atividades de todos os processos da gestão de riscos de segurança da informação e verificar as inconsistências e as eventuais necessidades de ajustes, tanto para correção quanto para aprimoramento do processo ou de seus artefatos. Por se tratar de um processo transversal, deverá ser executado sempre que possível e à períodos de tempo pré-determinados preferencialmente.

9.3.1.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

9.3.1.4 Entrada: processo de GRSIC e artefatos.

9.3.1.5 Saída: processo de GRSIC e artefatos revisados.

9.3.2 Documentar as lições aprendidas

9.3.2.1 Objetivo: documentar as lições aprendidas em cada processo no intuito de aprimorar o processo de gestão de riscos em segurança da informação, bem como cada atividade desenvolvida.

9.3.2.2 Descrição: durante a execução dos ciclos de análise de riscos, é possível que ocorram situações que não estavam previstas e que requeiram uma atuação da Equipe de Riscos e, eventualmente, dos Gestores. Assim, estes eventos devem ser formalmente documentados para

que em próximos ciclos esteja previsto e ocorram melhorias. Do mesmo modo, a cada ciclo também será possível identificar outros tipos de melhorias a serem realizadas, tanto no processo de gestão quanto em cada atividade. Todas essas lições devem ser formalmente documentadas, formando uma base de conhecimento.

9.3.2.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

9.3.2.4 Entrada: processo de GRSIC e artefatos.

9.3.2.5 Saída: Artefato Lições Aprendidas.

9.3.3 Elaborar proposta de melhorias

9.3.3.1 Objetivo: identificar melhorias no processo de GRSIC e seus artefatos que possam torná-lo mais efetivo e elaborar uma proposta de melhorias.

9.3.3.2 Descrição: identificar, após avaliação periódica e sistêmica, as possibilidades de melhoria, ajustes e/ou correções aplicáveis aos processos de GRSIC e seus artefatos que possam representar melhorias efetivas aos mesmos. As melhorias podem estar relacionadas aos fluxos de trabalho, documentos complementares, atores dos processos, tempos de execução, documentos de controle, meios de comunicação ou quaisquer outros artefatos. A proposta deve envolver a autoridade e, eventualmente, as partes interessadas, declarando de maneira clara os benefícios trazidos pelas melhorias propostas. A proposta de implementação das melhorias deve ser formal e deve contar com a aprovação da autoridade da unidade.

9.3.3.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

9.3.3.4 Entrada: lições aprendidas, processo de GRSIC e artefatos.

9.3.3.5 Saída: Artefato Proposta de Melhorias.

9.3.4 Apresentar a proposta de melhorias

9.3.4.1 Objetivo: propor, formalmente, à autoridade da unidade, as melhorias identificadas no processo de GRSIC e seus artefatos que possam torná-lo mais efetivo e eficaz.

9.3.4.2 Descrição: propor à autoridade da unidade a implementação das melhorias identificadas e aplicáveis aos processos de GRSIC.

9.3.4.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

9.3.4.4 Entrada: Artefato Proposta de Melhorias.

9.3.4.5 Saída: Artefato Proposta de Melhorias apresentada.

Número da Norma Complementar	Revisão	Emissão	Folha
04/CSIC/MCTIC	00		27/27

9.3.5 Analisar Proposta de Melhorias

9.3.5.1 Objetivo: analisar a proposta de melhorias apresentada.

9.3.5.2 Descrição: a análise e aprovação da proposta de melhorias é necessária para a execução das melhorias previstas. Esta aprovação deve ser formal, demonstrando o comprometimento da autoridade com o processo de gestão de riscos.

9.3.5.3 Responsável: Gestor de Segurança da Informação e Comunicações ou Gestor de Riscos em Segurança da Informação e Comunicações.

9.3.5.4 Entrada: Artefato Proposta de Melhorias.

9.3.5.5 Saída: Artefato Proposta de Melhorias aprovada.

9.3.6 Implementar as Melhorias

9.3.6.1 Objetivo: implementar, formalmente, as melhorias aprovadas no processo de GRSIC e seus artefatos, no intuito de torná-lo mais efetivo.

9.3.6.2 Descrição: implementar as melhorias identificadas após a aprovação das propostas. A implementação das melhorias deve seguir o formalismo da organização em relação às alterações processuais. A implementação das melhorias deverá ser comunicada antes e depois de serem realizadas, garantindo a ideal preparação e consequente adaptação da organização em razão de tais ajustes em seus processos.

9.3.6.3 Responsável: Equipe de Gestão de Riscos em Segurança da Informação e Comunicações.

9.3.6.4 Entrada: Artefato Proposta de Melhorias.

9.3.6.5 Saída: Processo de GRSIC com melhorias ou ajustes implementados.