MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - MGR-SISP v 2.0

Conforme
Instrução Normativa Conjunta
CGU/MP n° 01/2016

Agosto de 2016

MINISTÉRIO DO PLANEJAMENTO, DESENVOLVIMENTO E GESTÃO

Secretaria de Tecnologia da Informação

Presidente da República
Michel Temer

Ministro do Ministério do Planejamento, Desenvolvimento e Gestão – MP
Dyogo Oliveira

Secretário de Tecnologia da Informação – STI/MP
Marcelo Pagotti

Diretor do Departamento de Segurança da Informação, Infraestrutura de Serviços de TI – DESIN
Leonardo Boselli da Motta

Elaboração

Coordenação-Geral de Segurança da Informação – CGSIN/DESIN/STI/MP
José Ney de Oliveira Lima (coordenador)
Anderson S. Araújo (líder de projeto)
Jansen Araújo da Fonseca
Juliana Rocha Munita Moreira
Loriza Andrade Vaz de Melo
Luiz Henrique do Espírito Santo Andrade
Rodrigo de Souza Maeda
Tássio Correia da Silva

Centro de Tecnologia da Informação Renato Archer – CTI/MCTIC
Fábio Sato Ikuno
Miguel de Teive e Argollo Junior
Paulo Marcos Siqueira Bueno

Sumário

Lista de Figuras

Lista de Tabelas

1 – INTRODUÇÃO

Uma abordagem sistemática para a gestão da Segurança da Informação e Comunicações (SIC) é importante para que as organizações identifiquem possíveis ameaças ao seu negócio e estabeleçam medidas de proteção eficazes. A missão da organização e os seus objetivos principais devem ser a base para o estabelecimento de práticas para a promoção da SIC.

Um elemento importante nos esforços voltados à SIC é abordar os riscos de maneira efetiva e no tempo certo. A gestão de riscos deve integrar o sistema de gestão de SIC e deve ser alinhada às práticas gerais de gestão de riscos da organização.

A Gestão de Riscos de SIC deve ser um processo contínuo, bem estruturado e sistemático. O objetivo deste processo é de assegurar uma proteção adequada para os elementos de valor da organização, tais como:

- Pessoas.
- Informações.
- Processos de Negócio.
- Soluções de Tecnologia da Informação e Comunicação.

Essa proteção é necessária para evitar prejuízos a esses elementos de valor, que podem ocorrer como consequência de violações de segurança. O caráter estruturado e sistemático permite também priorizar a alocação de recursos para os elementos mais importantes, obtendo assim maior retorno dos investimentos em SIC.

Este documento apresenta a **Metodologia de Gestão de Riscos de Segurança da Informação e Comunicações do Sistema de Administração de Recursos da Tecnologia da Informação – SISP do Poder Executivo Federal (MGR-SISP)**. A metodologia visa padronizar e sistematizar a gestão de riscos de SIC na Administração Pública Federal (APF). Almeja-se assim atingir níveis satisfatórios de SIC e, ao mesmo tempo, racionalizar os investimentos, pela priorização de ações e por evitar redundâncias na gestão de riscos.

A MGR-SISP é compatível com iniciativas anteriores voltadas à SIC na APF, como a **Norma Complementar nº 04/IN01/DSIC/GSIPR**, do Gabinete de Segurança Institucional da Presidência da República, publicada em 15 de fevereiro de 2013, que estabelece diretrizes para o processo de Gestão de Riscos de SIC (GRSIC) e, mais recentemente, a **Instrução Normativa Conjunta n° 1, de 10 de maio de 2016**, publicada pela então Controladoria-Geral da União (CGU) e pelo Ministério do Planejamento, Orçamento e Gestão, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal (**INC CGU/MP n° 1/2016**). Esta INC tornou obrigatória ao órgãos e entidades do Poder Executivo Federal a adoção de medidas para a sistematização de práticas relacionadas à **gestão de riscos**, aos controles internos e à governança.

Embora desenvolvida com foco na Gestão de Riscos de SIC, a MGR-SISP pode ser facilmente adaptada para ser utilizada para realização de processos de gestão de riscos em geral.

Para o desenvolvimento da MGR-SISP buscou-se também o respaldo de padrões bem aceitos, como ISO/IEC 27005 (2011), IT Grundschutz BSI *Standard* 100-2 (2008) e NIST SP 800-39, (2011), que forneceram elementos para a definição da MGR-SISP, descrita neste documento.

No contexto deste documento a Gestão de Riscos de SIC é referida pela sigla GRSIC, ou em alguns pontos, apenas como “Gestão de Riscos”. A aplicação da MGR-SISP em organizações pode ser apoiada por uma ferramenta computacional, muito embora a metodologia seja independente de quaisquer ferramenta.

O restante deste documento esta organizado do seguinte modo:

- a Seção 2 apresenta termos e definições fundamentais;
- a Seção 3 lista as normas e legislações relacionadas;
- a Seção 4 trata do escopo de aplicação e das principais características da metodologia;

- a Seção 5 apresenta uma visão geral da MGR-SISP;
- a Seção 6 descreve a metodologia, detalhando os processos, as atividades, as tarefas e as informações tratadas;
- a Seção 7 traz as referências bibliográficas;
- o ANEXO a apresenta as Considerações sobre o tratamento de Ativos de Informação constantes da NC 10 IN01/DSIC/GSI/PR e da MGR-SISP.

2 – TERMOS E DEFINIÇÕES

Aceitação do risco: decisão de aceitar o risco residual.

Ameaça: causa potencial de um incidente indesejado, que possui potencial para comprometer ativos através da exploração das vulnerabilidades.

Análise do risco: estimar o risco baseado na probabilidade e em seu respectivo impacto.

Ataque: evento decorrente da exploração de uma vulnerabilidade por uma ameaça.

Ativo: qualquer elemento que tenha valor para a organização.

Ativos de informação: os meios de armazenamento, transmissão, processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que têm acesso a eles.

Autenticidade: a propriedade de ser genuíno e passível de verificação. Confiança na validade de uma transmissão, de uma mensagem ou de um emissor de mensagem.

Confidencialidade: garantia de que a informação seja legível somente para pessoas autorizadas.

Consequência: resultado certo ou incerto de um evento que afeta os objetivos. Elas podem ser expressas de forma qualitativa ou quantitativa.

Controle: medida que está modificando o risco. Os controles podem incluir: políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. Controle também pode ser utilizado como um sinônimo para proteção ou contramedida.

Criptografia: métodos para prover sigilo da informação.

Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação sempre que necessário.

Estimativa de risco: processo utilizado para atribuir valores à probabilidade e à consequência de um risco.

Evento: ocorrência ou mudança em um conjunto específico de circunstâncias.

Gestão de Riscos de SIC: conjunto de processos que permitem identificar e implementar medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibra-los com os custos operacionais e financeiros envolvidos.

Identificação do risco: processo de localizar, listar e caracterizar elementos de risco.

Impacto: medida numérica das consequências que afetam os objetivos de negócio.

Incidentes de SIC: evento, ou série de eventos indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a SIC.

Integridade: garantia de que a informação não foi alterada de maneira não autorizada ou desconhecida.

Mapa de Riscos: informações relacionadas a cada risco, definidas no decorrer das atividades de cada processo tais como: ativos, ameaças, controles, vulnerabilidades, consequências, probabilidades, níveis de risco, etc.

Probabilidade de ocorrência: fator do risco baseado na análise da probabilidade de que uma dada ameaça seja capaz de explorar uma dada vulnerabilidade.

Redução do risco: ações tomadas para reduzir a probabilidade ou as consequências negativas associadas a um risco.

Retenção do risco: aceitação do ônus ou do benefício associado a um risco.

Risco: combinação da probabilidade de um evento e sua consequência.

Risco de SIC: potencial de uma ameaça explorar vulnerabilidades de um ativo ou conjunto de ativos e, desse modo, causar dano à organização.

Risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco.

Sistema Estruturante: sistema com suporte de tecnologia da informação fundamental e imprescindível para planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações do Estado, além de outras atividades

auxiliares, desde que comum a dois ou mais órgãos da Administração e que necessitem de coordenação central.

Transferência do risco: compartilhamento com outra entidade do ônus ou do benefício associado a um risco.

Unidade da Organização: refere-se a um domínio ou a um perímetro da organização (como um processo, um andar, uma sala, um projeto, um conjunto de ativos, um sistema, etc.) que permite dividir a organização em partes, para fins de gestão de riscos de SIC. Unidade pode também se referir a uma unidade organizacional (divisão, departamento, etc.), mas isto não é obrigatório.

Vulnerabilidade: Fraqueza de um determinado ativo ou controle que pode ser explorado por uma ameaça.

3 – NORMAS E REGULAMENTAÇÕES RELACIONADAS

INSTRUÇÃO NORMATIVA CONJUNTA CGU/MP nº 1, de 10 de maio de 2016, dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

NORMA COMPLEMENTAR nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de SIC e Comunicações. 2008.

NORMA COMPLEMENTAR nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de SIC e Comunicações nos Órgãos e Entidades da Administração Pública Federal. 2009.

NORMA COMPLEMENTAR nº 04/IN01/DSIC/GSIPR, e seu anexo, (Revisão 01). Diretrizes para o processo de Gestão de Riscos de SIC e Comunicações - GRSICC nos órgãos e entidades da Administração Pública Federal. 2013.

NORMA COMPLEMENTAR nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. 2009

NORMA COMPLEMENTAR nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. 2009

NORMA COMPLEMENTAR nº 07/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à SIC e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. 2014.

NORMA COMPLEMENTAR nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

NORMA COMPLEMENTAR nº 09/IN01/DSIC/GSIPR, (Revisão 02) Estabelece orientações específicas para o uso de recursos criptográficos em SIC e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. 2014.

NORMA COMPLEMENTAR nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. 2012.

NORMA COMPLEMENTAR nº 11/IN01/DSIC/GSIPR**,** Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à SIC e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. 2012.

NORMA COMPLEMENTAR nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à SIC e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. 2012.

NORMA COMPLEMENTAR nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à SIC e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). 2012.

NORMA COMPLEMENTAR nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à SIC e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. 2012.

NORMA COMPLEMENTAR nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de SIC e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. 2012.

NORMA COMPLEMENTAR nº 16/IN01/DSIC/GSIPR. Estabelece as diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. 2012.

NORMA COMPLEMENTAR nº 17/IN01/DSCI/GSIPR, Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de SIC e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). 2013.

NORMA COMPLEMENTAR nº 18/IN01/DSIC/GSIPR, Estabelece as Diretrizes para as Atividades de Ensino em SIC e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). 2013.

NORMA COMPLEMENTAR nº 19/IN01/DSIC/GSIPR, Estabelece Padrões Mínimos de SIC e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. 2014.

NORMA COMPLEMENTAR nº 20/IN01/DSIC/GSIPR, (Revisão 1) Estabelece as Diretrizes de SIC e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

NORMA COMPLEMENTAR nº 21/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

INSTRUÇÃO NORMATIVA GSI Nº 1, de 13 de junho de 2008. Disciplina a Gestão de SIC e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

INSTRUÇÃO NORMATIVA GSI Nº 2, de 5 de fevereiro de 2013. Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

INSTRUÇÃO NORMATIVA GSI Nº 3, de 6 de março de 2013. Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

INSTRUÇÃO NORMATIVA SLTI/MP Nº 4, de 11 de setembro de 2014. Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal.

DECRETO Nº 8.135, DE 4 DE NOVEMBRO DE 2013. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

PORTARIA INTERMINISTERIAL MP/MC/MD Nº 141, DE 2 DE MAIO DE 2014. Dispõe que as comunicações de dados da Administração Pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observando o disposto nesta Portaria.

GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO. Versão 01 – Nov./2010.

PORTARIA Nº 14 – CDN DE 11 DE MAIO DE 2015. A Estratégia de SIC e Comunicações e de Segurança Cibernética da Administração Pública Federal.

4 – ESCOPO DE APLICAÇÃO E PRINCIPAIS CARACTERÍSTICAS

4.1 – Introdução

Esta seção apresenta uma visão geral da MGR-SISP. É apresentado o escopo de aplicação da metodologia e sua integração com outras iniciativas voltadas à SIC na APF. São descritos aspectos organizacionais importantes para a implementação da metodologia, assim como os três níveis de atuação para a gestão de riscos e proteção:

- Organização;
- Processos de Negócio;
- Ativos Tecnológicos.

A MGR-SISP é compatível com a Norma Complementar nº 04/IN01/DSIC/GSIPR, que estabelece diretrizes para o processo de Gestão de Riscos de SIC e descreve com maior detalhamento de processos, atividades e técnicas a serem utilizadas.

Segundo a **INC CGU/MP n° 1/2016** são objetivos da gestão de riscos:

- I – assegurar que os responsáveis pela tomada de decisão, em todos os níveis do órgão ou entidade, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;
- II – aumentar a probabilidade de alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis; e
- III – agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização.

Assim sendo, a MGR-SISP visa ser uma plataforma integradora de iniciativas do Estado Brasileiro, com o objetivo de aprimorar a SIC na APF e fazer cumprir os objetivos da gestão de riscos nos órgãos públicos federais. O alvo é contemplar os aspectos de segurança, conceitos e práticas, tratados em Normas Complementares (NC) e em

Instruções normativas (IN) que sejam relacionadas à gestão de riscos de SIC. Por exemplo, a metodologia destaca a importância do estabelecimento de:

- Uma Política de SIC (Norma Complementar nº 03/IN01/DSIC/GSIPR).
- Direcionar o gestor de riscos a implementar de Controles de Acesso (Norma Complementar nº 07/IN01/DSIC/GSIPR).
- Enfatiza que se respeitem diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação (Norma Complementar nº 10/IN01/DSIC/GSIPR).

Outro ponto importante é que a MGR-SISP pode sistematizar e padronizar a gestão de riscos na APF, destacando boas práticas e o reuso de soluções. As medidas de segurança previstas contra as ameaças identificadas (chamadas de proteções ou controles) são baseadas em padrões bem aceitos, tais como: ISO/IEC 27005, IT Grundschutz BSI *Standard* 100-2 e NIST SP 800-39. Elas também permitem que se atinjam níveis satisfatórios de SIC e ao mesmo tempo se racionalizem os investimentos, pela priorização de ações e por evitar redundâncias.

4.2 – Requisitos Desejáveis

Almeja-se que a metodologia seja adaptável e customizável de forma a apoiar organizações da APF cujas naturezas, características e objetivos apresentam variações. Em particular, busca-se oferecer apoio eficaz à gestão de riscos, independentemente do nível de maturidade em SIC em que a organização encontra-se (em termos de cultura e de práticas de segurança adotadas e institucionalizadas) e do nível de segurança requerido pela organização (associado à criticidade dos ativos de informação da organização).

Alguns requisitos mínimos, em termos de estrutura organizacional para a SIC, são esperados para a implementação da gestão de riscos. Prevê-se o envolvimento de profissionais com os seguintes perfis:

- **Autoridades competentes**, representantes da alta gestão da organização, que devem aprovar pontos importantes relativos à gestão de riscos e para prover os recursos necessários.

- **Responsáveis pela gestão de SIC**, que executarão as atividades de gestão de riscos e coordenarão esforços para identificar e estimar riscos, bem como propor melhorias necessárias para mitigar riscos, além de comunicar os resultados de análises a todos os interessados.
- **Responsáveis por avaliar as informações** produzidas pela gestão de riscos, acompanhar a realização das melhorias necessárias e zelar pela fiel utilização da metodologia.
- **Responsáveis pelas áreas da organização** nas quais a metodologia de gestão de riscos será implementada. Possuem o papel de coletar as informações necessárias à identificação e a estimação de riscos e realizar melhorias necessárias quando as análises indicarem esta necessidade.

Segundo a **INC CGU/MP n° 1/2016**:

Art. 19. O dirigente máximo da organização é o principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de riscos,... .

Art. 20. Cada risco mapeado e avaliado deve estar associado a um agente responsável formalmente identificado.

§ 1° O agente responsável pelo gerenciamento de determinado risco deve ser o gestor com alçada suficiente para orientar e acompanhar as ações de mapeamento, avaliação e mitigação do risco.

§ 2° São responsabilidades do gestor de risco:

I – assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos da organização;

II – monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos; e

III – garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da organização.

É desejável também que a organização realize análises internas voltadas a estabelecer as condições iniciais apropriadas para a implementação da metodologia de gestão de riscos. Isso envolve, por exemplo:

- Definir o propósito dos investimentos em SIC. O propósito deve estar associado à missão e aos objetivos da organização e deve ser documentado e aprovado por representantes da Alta Administração da organização. Tipicamente, este documento é denominado **Política de SIC** da organização [Norma Complementar nº 03/IN01/DSIC/GSIPR].
- Para a gestão de riscos será necessário identificar os setores da organização (divisões, departamentos, projetos, processos, etc.) que tratam com atividades e informações que envolvem requisitos de segurança, isto é, atividades e informações para as quais é importante que haja disponibilidade, integridade e confidencialidade. Para facilitar esta tarefa, o ideal é que a organização mapeie os seus **processos de negócio** e suas informações.
- Identificar profissionais com os perfis adequados aos papéis necessários à implantação da gestão de riscos (citados acima). É importante destacar que a metodologia apoia os profissionais na identificação de eventos adversos que podem ocorrer e causar danos aos ativos, às pessoas ou à organização. Ela auxilia na identificação de medidas de proteção e alternativas para evitar esses eventos ou reduzir o impacto que eles causam. Entretanto, a metodologia não substitui a *expertise* humana, necessária para decidir sobre alternativas de tratamento e para adaptar e implementar as medidas de segurança.

Além disso, a **INC CGU/MP n° 1/2016** trata, em seu art. 16, da **Estrutura do Modelo de Gestão de Riscos**.

> **Art. 16. Na implementação e atualização do modelo de gestão de riscos, a alta administração, bem como seus servidores ou funcionários, deverá observar os seguintes componentes da estrutura de gestão de riscos: ...**

...

I – ambiente interno: inclui, entre outros elementos, integridade, valores éticos e competência das pessoas, maneira pela qual a gestão delega autoridade e responsabilidades, estrutura de governança organizacional e políticas e práticas de recursos humanos. O ambiente interno é a base para todos os outros componentes da estrutura de gestão de riscos, provendo disciplina e prontidão para a gestão de riscos;

II – fixação de objetivos: todos os níveis da organização (departamentos, divisões, processos e atividades) devem ter objetivos fixados e comunicados. A explicitação de objetivos, alinhados à missão e à visão da organização, é necessária para permitir a identificação de eventos que potencialmente impeçam sua consecução;

III – identificação de eventos: devem ser identificados e relacionados os riscos inerentes à própria atividade da organização, em seus diversos níveis;

IV – avaliação de riscos: os eventos devem ser avaliados sob a perspectiva de probabilidade e impacto de sua ocorrência. A avaliação de riscos deve ser feita por meio de análises qualitativas, quantitativas ou da combinação de ambas. Os riscos devem ser avaliados quando à sua condição de inerentes e residuais;

V – resposta a riscos: o órgão/entidade deve identificar qual estratégia seguir (evitar, transferir, aceitar ou tratar) em relação aos riscos mapeados e avaliados. A escolha da estratégia dependerá do nível de exposição a riscos previamente estabelecido pela organização em confronto com a avaliação que se fez do risco;

VI – atividades de controles internos: são as políticas e os procedimentos estabelecidos e executados para mitigar os riscos que a organização tenha optado por tratar. Também denominadas de procedimentos de controle, devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão preventivos e detectivos, bem como a preparação prévia de planos de contingência e resposta à materialização dos riscos;

VII – informação e comunicação: informações relevantes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e condições externas, ...

VII ... que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam que a informação flua em todos os sentidos; e

VIII – **monitoramento:** tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos.

Parágrafo Único. Os gestores são os responsáveis pela avaliação dos riscos no âmbito das unidades, processos e atividades que lhes são afetos. A alta administração deve avaliar os riscos no âmbito da organização, desenvolvendo uma visão de riscos de forma consolidada.

4.3 – Níveis de Atuação da Metodologia

A gestão de riscos pode ocorrer em diferentes níveis de detalhamento, abordando medidas de proteção mais gerais, aplicáveis à organização como um todo ou a setores dessa. Cada setor, por sua vez, pode ser decomposto em processos de negócio e informações, permitindo estabelecer proteções mais específicas voltadas a esses processos e informações. Caso necessário, cada processo de negócio pode ser decomposto nos ativos que o apoiam, tal como: equipamentos de hardware, redes, locais físicos e software. Nesse nível mais detalhado, as medidas de proteção são específicas para cada elemento (cada componente de software, hardware, etc).

O conceito acima é ilustrado na **Figura 1** que mostra os três níveis para a gestão de riscos e para a adoção de medidas de proteção: gestão de aspectos gerais da segurança de informação (1º Nível), gestão de SIC voltada a processos de negócio e informações específicas (2º Nível) e gestão de SIC para tratar cada elemento tecnológico da organização (3º Nível).

O conceito ilustrado na **Figura 1** pode ser compreendido mais concretamente a partir da análise da **Tabela 1**. Essa tabela exemplifica, para cada nível de atuação (organização,

processos de negócio e ativos de tecnologia), ameaças, vulnerabilidades associadas às ameaças e controles que podem aumentar o nível de proteção dos ativos às ameaças.

Figura 1. Níveis de atuação para a gestão de riscos.

NÍVEIS	AMEAÇA	VULNERABILIDADE	CONTROLE/PROTEÇÃO
NÍVEL 1 ORGANIZAÇÃO	Vazamento de informação classificada	Acesso não autorizado às dependências da organização	Implementar controle de acesso nas dependências da organização
NÍVEL 2 PROCESSO DE NEGÓCIO	Ataque de negação de serviço do sistema de voto eletrônico no dia da eleição	Falta de monitoramento do tráfego de rede	Implementar monitoramento de rede
NÍVEL 3 ATIVOS DE TIC	Tentativa de um atacante invadir um servidor de E-mail	Serviço de E-mail desatualizado e sem aplicações de segurança	Atualizar o serviço de E-mail e aplicar o *Hardening* no servidor

Tabela 1: Exemplos de ameaças, vulnerabilidades e controles, por nível de atuação

Observe que o exemplo de ameaça de nível 1, na Tabela 1, pode trazer consequências negativas para organização como um todo, do ponto de vista de seu referencial estratégico (missão, visão, valores, imagem da organização). Já o exemplo de ameaça de nível 2 traz consequências negativas para o negócio da organização, podendo impossibilitar a entrega de um produto ou serviço finalístico específico da organização.

No caso da ameaça de nível 3, a consequência se restringe a um ativo de tecnologia específico ou um serviço meio da organização.

A **Figura 2** ilustra a atuação da gestão de segurança nos diversos níveis. No nível 1: organização como um todo ou unidades da organização isoladamente; no nível 2, no qual processos de negócio e informações são o alvo da gestão; e no nível 3, que trata individualmente de ativos como: servidores, computadores pessoais, notebooks, dispositivos de rede, serviços, etc.

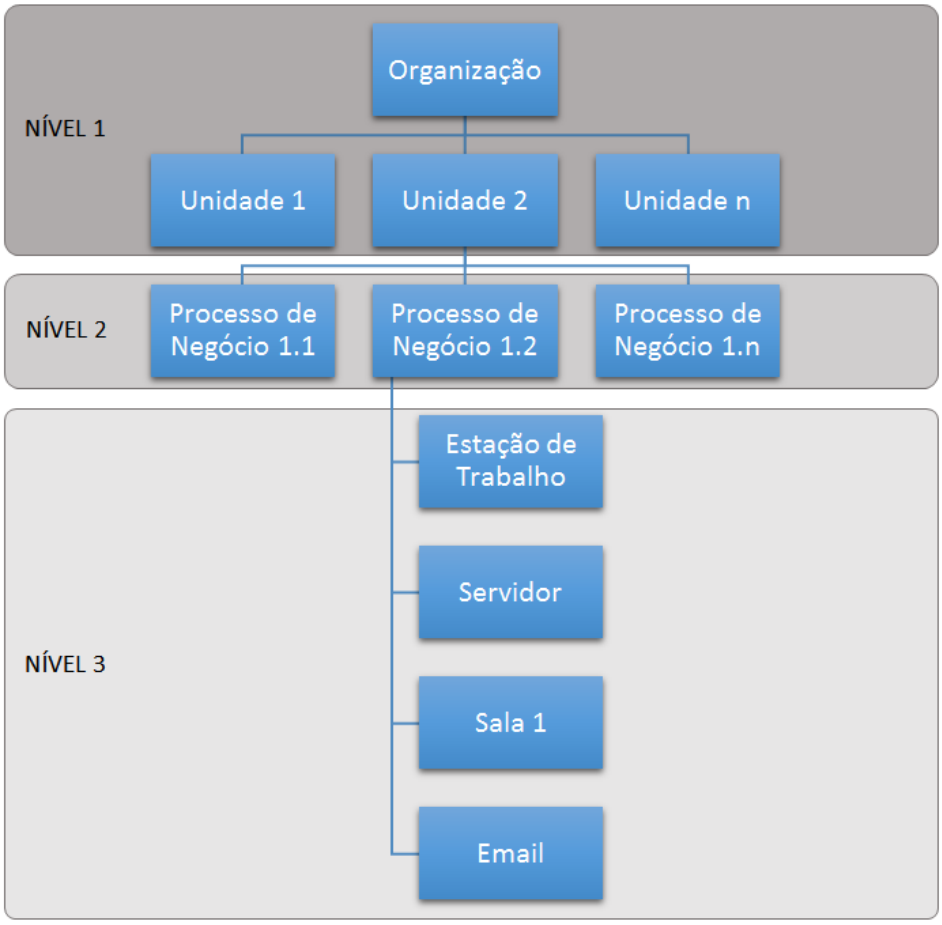

Figura 2. Níveis de atuação para a gestão de riscos e elementos da organização

5 – VISÃO GERAL DA MGR-SISP

5.1 – Estruturação e Apresentação da MGR-SISP

A MGR-SISP é composta por um conjunto de processos. Os processos, por sua vez, definem conjuntos de atividades estruturadas para que sejam atingidos os objetivos parciais da GRSIC. Já as atividades são decompostas em um conjunto de tarefas bem definidas. Na MGR-SISP, os processos são numerados. As atividades são numeradas em subníveis relacionados aos processos. Já as tarefas são nomeadas em ordem alfabética em relação às atividades conforme o exemplo abaixo.

Processo 1: primeiro processo a ser executado.

Atividade 1.1: primeira atividade a ser executada no Processo 1.

Tarefa 1.1-A: primeira tarefa a ser executada quando da realização da Atividade 1.1 do Processo 1.

Cada atividade é descrita pelos seguintes elementos:

- Nome.
- Descrição.
- Diagrama de fluxo de tarefas.
- Tarefas e respectivos responsáveis.
- Condição para ser realizada.
- Informações utilizadas.
- Informações produzidas.
- Condição para ser finalizada.
- *Templates* e exemplos.

Os processos, as atividades e as tarefas são ordenados, ou seja, há relações de precedência, sendo que os resultados produzidos por um processo ou atividade são normalmente utilizados para a realização de processos ou atividades seguintes.

Há também situações que envolvem a repetição de processos, atividades ou tarefas, isto é, processos, atividades ou tarefas são realizadas mais de uma vez até que uma condição alvo seja atingida. Da mesma forma, existem também paralelismos na realização de processos, atividades e tarefas. Alguns processos, atividades ou tarefas podem, e algumas devem, ser realizadas ao mesmo tempo.

5.2 – Resumo da MGR-SISP

Ao longo das atividades do processo de gestão de riscos devem ser estabelecidos o contexto, o escopo e os objetivos para cada **Projeto de Gestão de Riscos de Segurança da Informação e Comunicações (Projeto de GRSIC)**; devem ser identificados os riscos existentes, a probabilidade que estes de fato ocorram, assim como a extensão e gravidade dos efeitos negativos produzidos. Pode-se, desse modo, decidir sobre ações preventivas a serem tomadas para reduzir os riscos para níveis aceitáveis. Esse processo é importante também para gerar informações que permitam a comunicação e a tomada de decisões sobre as prioridades para a alocação de recursos de SIC.

Busca-se racionalizar o uso de recursos, evitando proteções redundantes e privilegiando a proteção dos recursos vitais.

Os órgãos da APF apresentam grande variedade no tocante às características, aos requisitos e ao nível de maturidade em SIC. Desse modo, a MGR-SISP estabelece atividades de pré-análise, visando direcionar a implantação da metodologia em cada organização específica.

A MGR-SISP possui um total de **65 tarefas agrupadas em 16 atividades organizadas em 7 processos**. A **Tabela 2** apresenta uma estatística da MGR-SISP. A **Tabela 3** apresenta um resumo da MGR-SISP com seus processos, tarefas e atividades. A **Tabela 4** apresenta as tarefas da MGR-SISP organizadas por papéis.

PROCESSO	ATIVIDADES	TAREFAS
1	2	10
2	2	8
3	3	15
4	1	4
5	3	14
6	3	6
7	2	8
TOTAL	**16**	**65**

Tabela 2: Estatísticas da MGR-SISP

PROCESSO	ATIVIDADE	TAREFA
1 ESTABELECER CONTEXTO	**1.1 Iniciar Projeto de GRSIC**	1.1-A: Definir Gestor de Riscos. 1.1-B: Identificar Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC. 1.1-C: Validar Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC. 1.1-D: Definir Responsáveis Pelas Unidades da Organização. 1.1-E: Definir Responsáveis Por Ativos.
	1.2 Realizar Pré-Análise do Escopo do Projeto de GRSIC	1.2-A: Elaborar Questionário. 1.2-B: Identificar os Profissionais Para Responder ao Questionário. 1.2-C: Obter Respostas. 1.2-D: Consolidar Resultados. 1.2-E: Validar Resultados.
2 IDENTIFICAR RISCOS	**2.1 Identificar Ativos**	2.1-A: Definir Abordagem da GRSIC 2.1-B: Cadastrar Ativos 2.1-C: Validar Informações Sobre os Ativos

	2.2 Identificar Ameaças, Controles e Vulnerabilidades	2.2-A: Solicitar Identificação de Ameaças, Controles e Vulnerabilidades 2.2-B: Obter Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade 2.2-C: Informar Ameaças, Controles e Vulnerabilidades dos Ativos 2.2-D: validar Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade 2.2-E: Validar Informações Sobre as Ameaças, Controles e Vulnerabilidades
3 ESTIMAR RISCOS	**3.1 Avaliar Impactos**	3.1-A: Solicitar Análise de Impactos 3.1-B: Obter Informações Sobre as Consequências 3.1-C: Identificar Consequências 3.1-D: Definir Impactos 3.1-E: Validar Análise de Impactos
	3.2 Avaliar Probabilidades	3.2-A: Solicitar Avaliação de Probabilidades 3.2-B: Solicitar Definição de Probabilidades 3.2-C: Definir Probabilidades 3.2-D: Avaliar Probabilidades 3.2-E: Validar Avaliações de Probabilidades
	3.3 Estimar Nível de Risco	3.3-A: Solicitar Estimativas de Riscos de Cada Unidade 3.3-B: Solicitar Estimativas de Riscos 3.3-C: Definir Estimativas de Riscos 3.3-D: Avaliar Estimativas de Riscos da Unidade 3.3-E: Validar as Estimativas de Riscos do Projeto de GRSIC
4 AVALIAR RISCOS	**4.1 Classificar os Riscos**	4.1-A: Realizar a Classificação dos Riscos 4.1-B: Registrar Ciência da Classificação de Riscos 4.1-C: Solicitar Validação da Classificação de Riscos 4.1-D: Validar Classificação de Riscos
5 TRATAR RISCOS	**5.1 Estimar Recursos Para o Tratamento dos Riscos**	5.1-A: Solicitar Estimativas de Tratamento 5.1-B: Estimar Custos, Esforços, Prazos e Restrições 5.1-C: Validar Estimativas
	5.2 Definir Resposta aos Riscos	5.2-A: Definir Tratamento 5.2-B: Definir Controles e Monitoramento 5.2-C: Analisar Resposta aos Riscos

		5.2-D: Solicitar Validação das Respostas aos Riscos 5.2-E: Validar Respostas aos Riscos
	5.3 Implementar Resposta aos Riscos	5.3-A: Solicitar Planos de Tratamento de Riscos 5.3-B: Elaborar Plano de Tratamento de Riscos 5.3-C: Avaliar Planos de Tratamento de Riscos 5.3-D: Validar Planos de Tratamento de Riscos 5.3-E: Iniciar Tratamento de Riscos 5.3-F: Executar Plano de Tratamento de Riscos
6 COMUNICAR RISCOS	**6.1 Planejar Comunicação de Riscos**	6.1-A: Elaborar Plano de Comunicação de Riscos 6.1-B: Validar Plano de Comunicação de Riscos
	6.2 Executar Plano de Comunicação de Riscos	6.2-A: Obter Informações Sobre a GRSIC 6.2-B: Enviar Informações Sobre a GRSIC às Partes Interes.
	6.3 Validar Informações Estratégicas	6.3-A: Obter Informações Estratégicas Sobre a GRSIC 6.3-B: Avaliar Informações Estratégicas Sobre a GRSIC
7 MONITORAR RISCOS	**7.1 Monitorar a Gestão de Riscos de SIC**	7.1-A: Verificar Alterações que Impactam a GRSIC 7.1-B: Comunicar Alterações que Impactam a GRSIC 7.1-C: Solicitar Atualização da GRSIC 7.1-D: Atualizar Informações da GRSIC
	7.2 Monitorar o Tratamento de Riscos	7.2-A: Validar Tratamentos 7.2-B: Monitorar Execução dos PTRs 7.2-C: Monitorar Estrategicamente 7.2-D: Verificar Necessidades de Alteração no Trat. dos Riscos

Tabela 3: Resumo da MGR-SISP

PAPEL	TAREFA
AUTORIDADE COMPETENTE	1.1-A: Definir Gestor de Riscos. 1.1-C: Validar Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC. 1.2-E: Validar Resultados. 4.1-D: Validar Classificação de Riscos 5.2-E: Validar Respostas aos Riscos 5.3-D: Validar Planos de Tratamento de Riscos 6.1-B: Validar Plano de Comunicação de Riscos 6.3-A: Obter Informações Estratégicas Sobre a GRSIC 6.3-B: Avaliar Informações Estratégicas Sobre a GRSIC 7.1-A: Verificar Alterações que Impactam a GRSIC 7.1-B: Comunicar Alterações que Impactam a GRSIC 7.1-D: Atualizar Informações da GRSIC 7.2-C: Monitorar Estrategicamente
GESTOR DE RISCOS	1.1-B: Identificar Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC. 1.1-D: Definir Responsáveis Pelas Unidades da Organização. 1.2-A: Elaborar Questionário. 1.2-B: Identificar os Profissionais Para Responder ao Questionário. 1.2-C: Obter Respostas. 1.2-D: Consolidar Resultados. 2.1-A: Definir Abordagem da GRSIC 2.1-C: Validar Informações Sobre os Ativos 2.2-A: Solicitar Identificação de Ameaças, Controles e Vulnerabilidades 2.2-E: Validar Informações Sobre as Ameaças, Controles e Vulnerabilidades 3.1-A: Solicitar Análise de Impactos 3.1-E: Validar Análise de Impactos 3.2-A: Solicitar Avaliação de Probabilidades 3.2-E: Validar Avaliações de Probabilidades 3.3-A: Solicitar Estimativas de Riscos de Cada Unidade 3.3-E: Validar as Estimativas de Riscos do Projeto de GRSIC 4.1-A: Realizar a Classificação dos Riscos 4.1-C: Solicitar Validação da Classificação de Riscos 5.1-A: Solicitar Estimativas de Tratamento 5.1-C: Validar Estimativas 5.2-A: Definir Tratamento 5.2-B: Definir Controles e Monitoramento 5.2-D: Solicitar Validação das Respostas aos Riscos 5.3-A: Solicitar Planos de Tratamento de Riscos 5.3-C: Avaliar Planos de Tratamento de Riscos

	6.1-A: Elaborar Plano de Comunicação de Riscos 6.2-A: Obter Informações Sobre a GRSIC 6.2-B: Enviar Informações Sobre a GRSIC às Partes Interessadas 7.1-A: Verificar Alterações que Impactam a GRSIC 7.1-B: Comunicar Alterações que Impactam a GRSIC 7.1-C: Solicitar Atualização da GRSIC 7.1-D: Atualizar Informações da GRSIC 7.2-B: Monitorar Execução dos PTRs 7.2-D: Verificar Necessidades de Alteração no Trat. dos Riscos
RESPONSÁVEL PELA UNIDADE DA ORGANIZAÇÃO	1.1-E: Definir Responsáveis Por Ativos. 2.1-A: Definir Abordagem da GRSIC 2.1-B: Cadastrar Ativos 2.2-B: Obter Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade 2.2-D: validar Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade 3.1-B: Obter Informações Sobre as Consequências 3.1-D: Definir Impactos 3.2-B: Solicitar Definição de Probabilidades 3.2-D: Avaliar Probabilidades 3.3-B: Solicitar Estimativas de Riscos 3.3-D: Avaliar Estimativas de Riscos da Unidade 4.1-B: Registrar Ciência da Classificação de Riscos 5.1-B: Estimar Custos, Esforços, Prazos e Restrições 5.2-C: Analisar Resposta aos Riscos 5.3-B: Elaborar Plano de Tratamento de Riscos 5.3-E: Iniciar Tratamento de Riscos 7.1-A: Verificar Alterações que Impactam a GRSIC 7.1-B: Comunicar Alterações que Impactam a GRSIC 7.1-D: Atualizar Informações da GRSIC 7.2-A: Validar Tratamentos
RESPONSÁVEL POR ATIVOS	2.2-C: Informar Ameaças, Controles e Vulnerabilidades dos Ativos 3.1-C: Identificar Consequências 3.2-C: Definir Probabilidades 3.3-C: Definir Estimativas de Riscos 5.3-F: Executar Plano de Tratamento de Riscos 7.1-A: Verificar Alterações que Impactam a GRSIC 7.1-B: Comunicar Alterações que Impactam a GRSIC 7.1-D: Atualizar Informações da GRSIC

Tabela 4: Tarefas da MGR-SISP organizadas por papéis.

6 – METODOLOGIA DE GESTÃO DE RISCOS DE SIC DO SISP

6.1 – Introdução

Esta seção apresenta a MGR-SISP, seus processos, atividades e tarefas de forma estruturada, bem como as informações produzidas em formato de *template* e alguns exemplos.

A MGR-SISP é composta pelos seguintes processos:

1. **Estabelecer Contexto**
2. **Identificar Riscos**
3. **Estimar Riscos**
4. **Avaliar Riscos**
5. **Tratar Riscos**
6. **Comunicar Riscos**
7. **Monitorar Riscos**

A **Figura 3** ilustra o processo subjacente à MGR-SISP. É mostrado o fluxo de execução dos processos, destacando a execução sequencial dos Processos: 1 – Estabelecer Contexto; 2 – Identificar Riscos; 3 – Estimar Riscos; e 4 – Avaliar Riscos.

O primeiro ponto de decisão ocorre após o **Processo 4 – Avaliar Riscos**, no qual é avaliada a necessidade de mais informações em termos de abrangência e de nível de detalhe, situação na qual estes processos são reexecutados. O fluxo segue com o tratamento de riscos e em um segundo ponto de decisão, caso o tratamento não seja suficiente, ou seja, situação em que o risco residual é superior ao aceitável, ocorre a reexecução dos processos. Embora não explicitado na **Figura 3**, é previsto que a execução de cada processo seja seguida de uma avaliação dos resultados produzidos. Essa avaliação pode indicar a necessidade de revisar informações ou reexecutar atividades.

Embora apareçam com a numeração ordinal 6 e 7, os **Processos 6 – Comunicar Riscos** e **7 – Monitorar Riscos** devem ser executados simultaneamente aos processos 1 a 5.

Figura 3. Processo da MGR-SISP

Cada processo é descrito resumidamente e é mostrado como um fluxo de atividades por meio de diagramas. Tem-se então a descrição das atividades constituintes do processo.

Para cada atividade é fornecida uma descrição e são apresentadas as tarefas que compõem a atividade, os responsáveis pela execução das tarefas, as informações necessárias e condição de início para a atividade, assim como as informações produzidas e condição de finalização. As atividades também são representadas por meio de diagramas. *Templates* e exemplos associados às atividades são apresentados.

Os processos, atividades e tarefas são executados por papéis organizacionais. São eles:

- Autoridade Competente
- Gestor de Riscos
- Responsável Pela Unidade da Organização
- Responsável Por Ativos

Nos fluxos de tarefas das atividades esses papéis são representados por cores: preto para a Autoridade Competente, azul para o Gestor de Riscos, verde para o Responsável Pela Unidade da Organização e laranja para o Responsável Por Ativos.

- **Autoridade Competente:** responsável por prover os recursos necessários à gestão de riscos; identificar responsáveis; iniciar as atividades de gestão de riscos; aprovar pontos importantes relativos à gestão de riscos tais como: objetivo, restrições e aprimoramentos da MGR-SISP.

- **Gestor de Riscos:** responsável por executar as atividades de gestão de riscos e coordenar esforços para identificar e estimar riscos, propor melhorias necessárias para mitigar riscos, além de comunicar os resultados de análises a todos os interessados.
- **Responsável Pela Unidade da Organização:** responsável por uma área da organização na qual a metodologia será implementada ou por uma área que deve prover informações para a gestão de riscos. Tem o papel de coordenar o fornecimento das informações necessárias à identificação e à estimativa de riscos e realizar melhorias necessárias quando as análises indicarem.
- **Responsável Por Ativos:** responsável por fornecer informações sobre os ativos que fazem parte da análise de riscos. Essas informações auxiliam a tomada de decisões sobre controles a serem implementados.

É importante ressaltar que a alocação de pessoas aos papéis descritos acima deve levar em conta o escopo onde a MGR-SISP será aplicada. A **Autoridade Competente**, por exemplo, depende do nível de organização considerada (ver Figura 2 – nível de atuação da GRSIC). Dessa forma, ela pode ser a **Autoridade Máxima do Órgão Público** ou o chefe do departamento (se considerarmos apenas o departamento como organização, por exemplo).

Dessa forma, a definição de quem é a **Autoridade Competente** deve levar em conta esse conceito, bem como as competências dispostas nos arts. 19 e 20 da **INC CGU/MP n° 1/2016**.

6.2 – Critérios da GRSIC

6.2.1 – Introdução

No processo de gestão de riscos são necessários critérios para avaliar o nível dos riscos e para decidir sobre qual tratamento que deve ser realizado. Para tanto, são utilizados critérios que sistematizam esse processo tais como: critérios para a avaliação de riscos e de impactos e critérios para a aceitação de riscos. Os critérios definidos serão utilizados em momentos posteriores do processo de gestão de riscos.

A metodologia MGR-SISP propõe o uso de análises semiquantitativas como uma forma de critério, conforme descrito a seguir.

6.2.2 – Critérios Para Avaliação de Probabilidades

Os critérios para avaliar as probabilidades de riscos definem um nível de probabilidade que as ameaças possuem de se concretizarem e de provocarem danos em ativos, na organização ou em pessoas. Isso é feito por meio da definição de classes de probabilidade que caracterizam o quão frequentemente espera-se que uma ameaça ocorra e o quão facilmente as vulnerabilidades serão exploradas no ativo.

As classes de probabilidades previstas na MGR-SISP são as seguintes:

- **Probabilidade Muito Baixa (MB):** é altamente improvável que o evento ocorra;
- **Probabilidade Baixa (B):** é improvável que o evento ocorra;
- **Probabilidade Moderada (M):** é provável que o evento ocorra;
- **Probabilidade Alta (A):** é altamente provável que o evento ocorra;
- **Probabilidade Muito Alta (MA):** é quase certo que o evento vai ocorrer.

Para definição do que é altamente improvável, improvável, provável, altamente provável ou quase certo, o **Gestor de Riscos** deve estabelecer intervalos de ocorrência de eventos, considerando o universo e o histórico de ocorrências anteriores.

Como exemplo, podemos supor que:

- improvável é quando um evento ocorre menos que uma vez a cada ano e mais do que uma vez a cada 10 anos;
- provável é quando um evento ocorre entre 1 e 10 vezes por ano;
- altamente provável é quando um evento ocorre entre 10 e 100 vezes ao ano; e
- quase certo é quando um evento ocorre mais do que 100 vezes ao ano.

Observe que para definir estes intervalos é necessário uma série histórica, uma *expertise* ou alguma referência anterior.

É preciso observar também as **adequações necessárias ao intervalo numérico** apresentado acima (1-10, 10-100), bem como tempo (10 anos). Por exemplo, para um evento do tipo “perda da recurso humano”: se o número de profissionais da organização é apenas 50, não faz sentido o intervalo máximo de 100. Nesse caso, o 100 deve ser

normalizado para 50 e os respectivos intervalos devem ser revistos. Um **raciocínio idêntico deve ser aplicado ao tempo** (10 anos, 5 anos, etc.).

Além disso, o **Gestor de Riscos** deve definir também **questões de apoio e descrições para a avaliação de probabilidades**. Uma questão exemplificativa seria: qual é a estimativa de probabilidade de que a ameaça ao ativo ocorra em um prazo aproximado de um ano? Resposta: MB, B, M, A ou MA.

6.2.3 – Critérios Para Avaliação de Impactos

A concretização de uma ameaça pode trazer consequências aos ativos e à organização. As consequências impactam direta ou indiretamente nos ativos, na organização e nas pessoas. Assim, é preciso avaliar o impacto que a concretização de uma ameaça pode trazer para ativos, pessoas e organização. Cada classe de impacto deve refletir a extensão do dano causado pela perda de atributos de segurança (confidencialidade, integridade, disponibilidade e/ou autenticidade) associados ao ativo, caso a ameaça concretize-se.

As classes de impactos previstas na MGR-SISP são as seguintes:

- **Muito Baixo (MB):** nenhum serviço ou atividade é afetado;
- **Baixo (B):** poucos serviços ou atividades de menor importância são afetados, pode provocar atrasos desprezíveis;
- **Moderado (M):** alguns serviços ou atividades são afetados, podendo causar atrasos significativos;

- **Alto (A):** serviços essenciais são afetados, provocando atrasos graves e danos elevados;
- **Muito Alto (MA):** serviços essenciais são afetados severamente, gerando danos muito elevados e atrasos intoleráveis.

A avaliação de impactos requer a definição de questões de apoio e descrições de classes. O **Gestor de Riscos** deve definir questões de apoio e descrições para a avaliação de consequências de cada atributo de segurança (confidencialidade, integridade, disponibilidade e autenticidade). Uma questão exemplificativa seria: qual o impacto da ameaça ao ativo em relação à disponibilidade? Resposta: MB, B, M, A ou MA.

6.2.4 – Critérios de Tratamento e de Aceitação de Riscos

Como será detalhado à frente no **Processo 3 – Estimar Riscos**, o nível de cada risco (uma dada ameaça a um ativo) é calculado a partir das estimativas feitas para impactos e probabilidades. Assim sendo, os critérios de tratamento e de aceitação de riscos devem considerar basicamente dois aspectos:

- definição de faixas de valores para os níveis de riscos; e
- definição de ações a serem tomadas para o tratamento de riscos em cada faixa.

A **Tabela 5** apresenta a definição de faixas de valores para os níveis de riscos e ilustra o critério de classificação para o tratamento e aceitação de riscos da MGR-SISP. A linha superior mostra a classificação de probabilidades e a coluna à esquerda mostra a classificação de impacto. Os valores interiores representam os níveis de risco estimados em cada situação e combinam os efeitos da probabilidade e do impacto dos riscos. As letras interiores definem as diferentes classes para o tratamento de riscos (MB: Muito Baixo; B: Baixo; M: Moderado; A: Alto; MA: Muito Alto). Cada classe de risco é sinalizada com uma cor diferente.

	Probabilidade	Muito Baixa	Baixa	Moderada	Alta	Muito alta
Impacto	Muito baixo	1 (MB)	2 (MB)	3 (B)	4 (B)	5 (M)
	Baixo	2 (MB)	3 (B)	4 (B)	5 (M)	6 (A)
	Moderado	3 (B)	4 (B)	5 (M)	6 (A)	7 (A)
	Alto	4 (B)	5 (M)	6 (A)	7 (A)	8 (MA)
	Muito alto	5 (M)	6 (A)	7 (A)	8 (MA)	9 (MA)

Tabela 5: Critério de classificação para o tratamento e aceitação de riscos da MGR-SISP.

Desse modo, as faixas (ou classes) definidas pelos critérios de avaliação de riscos e de aceitação de riscos neste caso estabelecem:

- **Risco Muito Baixo (MB):** nível de risco entre 1 e 2;
- **Risco Baixo (B):** nível de risco entre 3 e 4;
- **Risco Moderado (M):** nível de risco igual a 5;
- **Risco Alto (A):** nível de risco entre 6 e 7;
- **Risco Muito Alto (MA):** nível de risco entre 8 e 9.

É preciso também à definição de ações a serem tomadas para o tratamento de riscos em cada faixa. Esse aspecto estabelece a estratégia da organização para tratar os riscos, dependendo dos resultados obtidos na estimativa de riscos. Aspectos como custo-benefício de tratamentos também devem ser levados em conta.

A MGR-SISP adota a estratégia de tratamento de riscos baseada em Canongia e outros, 2010. Essa estratégia pode ser modificada pelo **Gestor de Riscos**.

- **Risco Muito Baixo (MB):** risco tolerável - nenhuma ação é necessária;
- **Risco Baixo (B):** risco tolerável - nenhuma ação imediata é necessária, porém o risco deve ser monitorado;

Recomenda-se tratar os riscos nesta classe apenas se restrições (como custo e esforço de tratamento) não forem significativas.

- **Risco Moderado (M):** situação de atenção. Se possível o risco deve ser tratado em médio prazo. O risco deve ser monitorado frequentemente.

Restrições (como custo e esforço de tratamento) podem ser consideradas para priorizar o tratamento de riscos nessa classe.

- **Risco Alto (A):** risco intolerável, situação de grande preocupação. Ações devem ser tomadas rapidamente e os resultados precisam ser monitorados frequentemente para avaliar se a situação mudou com as ações.

Recomenda-se o tratamento de riscos independentemente de restrições (como custo e esforço de tratamento).

- **Risco Muito Alto (MA):** risco intolerável. Requer ações de tratamento imediatas. As ações devem ser monitoradas continuamente para avaliar se os efeitos são os esperados.

Os riscos devem ser tratados independentemente de restrições (como custo e esforço de tratamento).

6.3 – Processo 1 – Estabelecer Contexto

6.3.1 – Descrição do Processo

Este processo trata de pontos a serem definidos nas etapas iniciais da implementação e utilização da metodologia de gestão de riscos. A **Figura 4** mostra o fluxo de atividades do processo.

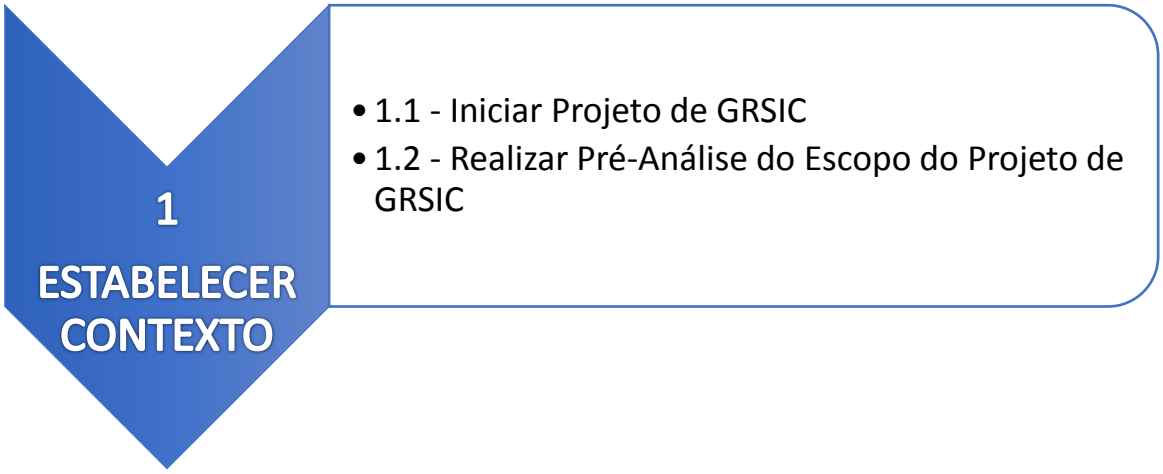

Figura 4: Fluxo de atividades do Processo 1 – Estabelecer Contexto

6.3.2 – Atividade 1.1 – Iniciar Projeto de GRSIC

Esta atividade consiste na abertura do **Projeto de Gestão de Riscos de SIC.** Para isso, é necessário definir os responsáveis pela GRSIC, alocando pessoas para os papéis previstos na MGR-SISP. Devem ser localizados profissionais que apresentam perfil adequado para assumir esses papéis. São previstos os seguintes papéis:

- **Autoridade Competente;**
- **Gestor de Riscos;**

- **Responsável Pela Unidade da Organização;**
- **Responsável Por Ativos.**

Também definimos nesta atividade os objetivos e o escopo do **Projeto de GRSIC**, tendo em vista os objetivos estratégicos da organização. Tipicamente os projetos de GRSIC e seus respectivos escopos e objetivos são parte de uma política de SIC [Norma Complementar nº 03/IN01/DSIC/GSIPR]. O objetivo da GRSIC deve estar alinhado a aspectos importantes da governança da organização como a missão, visão e valores estipulados por ela. Além disso, o objetivo da GRSIC deve também estar alinhado à atuação da organização em termos de serviços prestados à sociedade e aos cidadãos. Os objetivos e restrições devem ser a base para os passos posteriores do **Projeto de GRSIC** e para a tomada de decisões.

Exemplos de objetivos para adoção da GRSIC:

- Garantir que sistemas estruturantes possuam padrões mínimos de SIC [Norma Complementar nº 19/IN01/DSIC/GSPR].
- Assegurar o cumprimento da INC n° 1, da Controladoria Geral da União – CGU, de 10 de Maio de 2016, no que tange aos requisitos para a Gestão de Riscos de SIC.
- Promover alta confiabilidade para tratar informação em termos de confidencialidade, integridade, disponibilidade e autenticidade.
- Proteger a qualidade da informação utilizada para decisões importantes.
- Garantir a satisfação de requisitos legais e de regulação.
- Reduzir o custo de incidentes de segurança.
- Garantir a continuidade do trabalho.
- Garantir uma boa reputação para o público em geral.
- Preservar o valor do investimento em tecnologia, informação, processos e conhecimento.
- Proteger o valor das informações mais importantes.
- Proteger a qualidade da informação utilizada para decisões importantes.
- Garantir a satisfação de requisitos legais e de regulação.
- Reduzir o custo de incidentes de segurança.
- Garantir a continuidade do trabalho.

O escopo do **Projeto de GRSIC** deve ser definido explicitando quais unidades da organização (divisões, setores, departamentos, processos, sistemas, etc.) devem ser tratados pela gestão de riscos e quais unidades estão não serão tratados. Essa análise deve focar na natureza das atividades e das informações em cada unidade e as justificativas para a escolha das unidades devem ser documentadas.

É importante notar que, mesmo as unidades que não tratam com informações e processos críticos, possuem influência na SIC em aspectos relacionados aos recursos humanos, aos aspectos jurídicos, etc.

É necessário também especificar as premissas e as restrições que podem afetar o **Projeto de GRSIC**, tais como: regulamentações específicas, restrições financeiras, restrições de prazo, restrições técnicas, etc. De acordo com os objetivos e a complexidade da organização, essa atividade deve considerar também o envolvimento de setores como: segurança patrimonial, jurídico, recursos humanos, financeiro e de planejamento.

A **Figura 5** mostra o fluxo de tarefas da atividade.

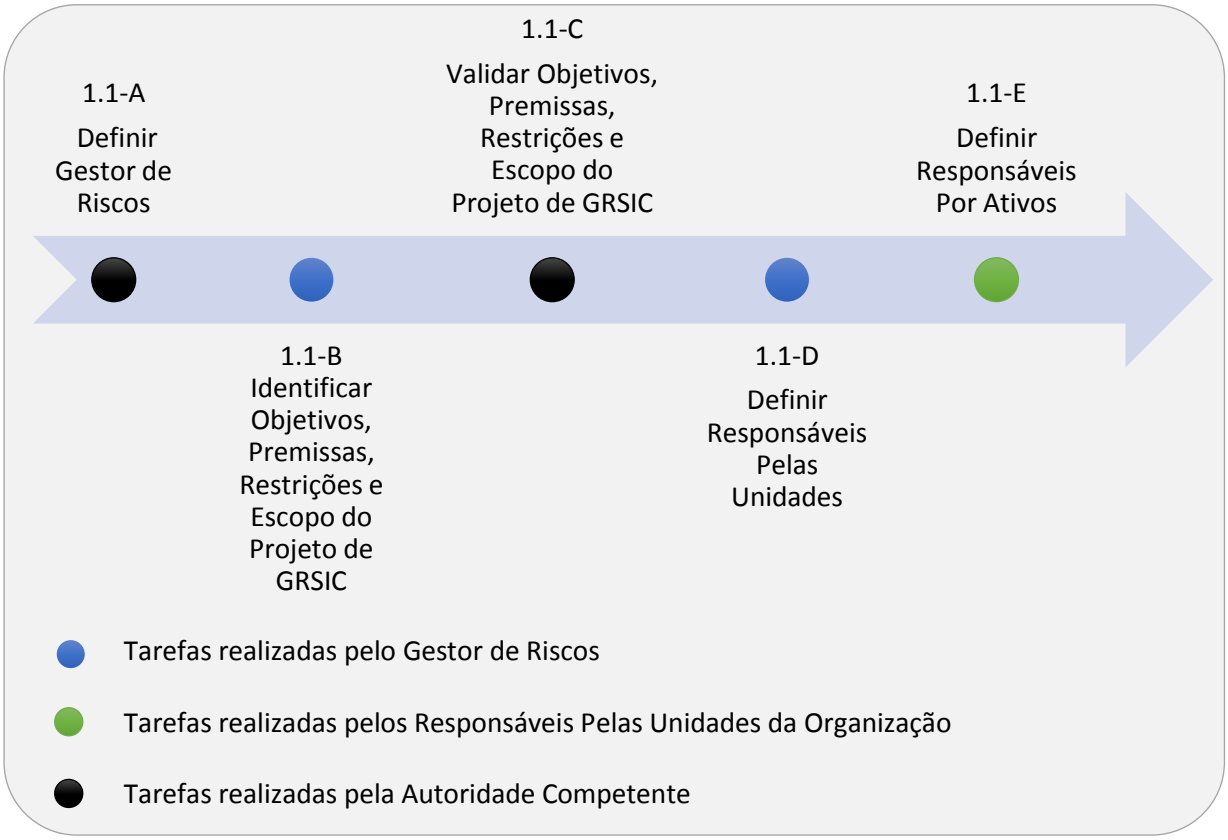

Figura 5: Fluxo de tarefas da Atividade 1.2 – Iniciar Projeto de GRSIC

TAREFAS DA ATIVIDADE 1.1 – Iniciar Projeto de GRSIC

Tarefa 1.1-A: Definir Gestor de Riscos.

A Autoridade Competente deve designar formalmente um Gestor de Riscos para a condução das próximas atividades da GRSIC. Caso necessário mais de um Gestor de Riscos pode ser identificado. Posteriormente, a Autoridade Competente deve notificar o Gestor de Riscos para realização da Tarefa 1.1-B: Definir Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC e informar o respectivo prazo para a conclusão da atividade.

Responsável: Autoridade Competente.

Tarefa 1.1-B: Identificar Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC.

O Gestor de Riscos deve iniciar o Projeto de GRSIC e informar os objetivos genéricos (de alto nível, como os listados na descrição da atividade) e os objetivos específicos da organização (tais como os relacionados aos seguintes pontos: informações confidenciais, sistemas que requerem alta disponibilidade, sistemas e informações cruciais para a tomada de decisões, etc.).

Além disso, o Gestor de Riscos deve identificar os tipos de restrições que se apliquem (tais como: técnicas, jurídicas, financeiras, de prazos, etc.) e deve descrever em detalhes as restrições e premissas, informando, se necessário, valores como de prazo ou de orçamento.

O Gestor de Riscos deve identificar também as unidades dentro do escopo do Projeto de GRSIC e também as que estão fora do escopo do projeto. Devem ser identificados também o Responsável Por Cada Unidade identificada no escopo. Posteriormente, o Gestor de Riscos deve notificar a Autoridade Competente das informações disponíveis para realização da Tarefa 1.1-C: Validar Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC e informar o respectivo prazo para conclusão da tarefa.

Responsável: Gestor de Riscos com apoio da Autoridade Competente.

Tarefa 1.1-C: Validar Objetivos, Premissas, Restrições e Escopo do Projeto de GRSIC.

A Autoridade Competente deve verificar se as informações definidas nas tarefas anteriores são estratégicas e se estão alinhadas às necessidades e às expectativas da organização. Caso estejam de acordo, a Autoridade Competente deve registrar a aprovação do Projeto de GRSIC e notificar o Gestor de Riscos para realização da Tarefa 1.1-D: Definir Responsáveis Pelas Unidades da Organização e informar o prazo para conclusão da tarefa. Caso contrário, a Autoridade Competente deve notificar o Gestor de Riscos da necessidade de reexecutar uma ou mais das tarefas anteriores e informar o prazo para conclusão das tarefas e as orientações para

aprimoramento das informações.

Responsável: Autoridade Competente.

Tarefa 1.1-D: Definir Responsáveis Pelas Unidades da Organização.

O Gestor de Riscos deve identificar os profissionais que assumirão os papéis de Responsável Pela Unidade da Organização. Posteriormente, o Gestor de Riscos deve notificar os Responsáveis Pelas Unidades da Organização para realização da Tarefa 1.1-E: Definir Responsáveis Por Ativos e informar o prazo para conclusão da tarefa**.**

Responsável: Gestor de Riscos com apoio da Autoridade Competente.

Tarefa 1.1-E: Definir Responsáveis Por Ativos.

Os Responsáveis Pelas Unidades da Organização devem identificar os profissionais que assumirão os papéis de Responsáveis Por Ativos em cada unidade. Posteriormente, o Responsável Pela Unidade da Organização deve notificar o Gestor de Riscos e encerra-se, dessa forma, a Atividade 1.1 – Definir Responsáveis, Objetivos, Escopo e Restrições do Projeto de GRSIC.

Responsável: Responsável Pela Unidade da Organização.

Condição para início:

- decisão para implementar a MGR-SISP.

Informações necessárias:

- informações sobre profissionais da organização e organograma;
- objetivos da organização;
- regulamentações específicas;
- restrições financeiras;
- restrições de prazo;
- restrições técnicas;
- informações estratégicas de outros setores (exemplos: segurança patrimonial; jurídico; recursos humanos; financeiro; e de planejamento).

Condição para ser finalizada:

- profissionais identificados e papéis atribuídos;
- objetivos, premissas e restrições do Projeto de GRSIC identificadas, documentadas e validadas pela Autoridade Competente.

Informações produzidas:

- profissionais identificados, objetivos, premissas, restrições e escopo do Projeto de GRSIC identificadas e documentadas.

***Templates* da Atividade 1.1 – Definir Responsáveis, Objetivos, Escopo e Restrições do Projeto de GRSIC.**

O *template* na **Figura 6** ilustra a associação de profissionais específicos para os papéis e destaca responsabilidades específicas. A **Figura 7** apresenta um *template* para o registro das informações tratadas nas **Tarefas 1.1-D a 1.1-G**.

PROFISSIONAIS, PAPÉIS E RESPONSABILIDADES					
Nome	**Unidade**	**Telefone**	**e-mail**	**Papel**	**Responsabilidades**
Nome 1	Unidade 1	Telefone 1	e-mail 1	Gestor de Riscos	Responsabilidades específicas 1
Nome 2	Unidade 2	Telefone 2	e-mail 2	Responsável Pela Unidade	Responsabilidades específicas 2
...	**...**	**...**	**...**	**...**	**...**
Responsável pela informação: **Data:**					

Figura 6: *Template* do registro de profissionais e papéis.

OBJETIVOS, ESCOPO, PREMISSAS E RESTRIÇÕES DO PROJETO DE GRSIC	
Objetivos do Projeto de GRSIC:	Descrição dos Objetivos
Escopo do Projeto de GRSIC:	Descrição do Escopo
Premissas do Projeto de GRSIC:	Descrição das Premissas
Restrições do Projeto de GRSIC:	Descrição das Restrições

Responsável pela informação:
Responsável pela aprovação do Projeto de GRSIC:
Data:

Figura 7: *Template* para o registro de objetivos, escopo, premissas e restrições do Projeto de GRSIC

6.3.3 – Atividade 1.2 – Realizar Pré-análise do Escopo do Projeto de GRSIC

Esta atividade visa obter uma avaliação inicial e abrangente da situação atual em SIC no escopo do **Projeto de GRSIC**. Essa avaliação é útil para direcionar os passos seguintes na gestão de riscos e indicar pontos fracos a serem priorizados no tratamento. A avaliação pode também ser reaplicada em situações posteriores como uma forma de verificar a evolução na SIC.

A atividade consiste na utilização de um questionário (estilo *checklist*) que aborda de forma ampla pontos de SIC com foco no itens de controle;

Os itens de controle base abordam diferentes categorias:

- Política de Proteção da Informação.
- Gestão do Risco.
- Gestão de Configuração.
- Manutenção.
- Proteção de Mídias.
- Política de Proteção da Informação.
- Gestão do Risco.
- Gestão de Configuração.
- Manutenção.
- Proteção de Mídias;.
- Cultura.
- Gestão de crise.
- Proteção Física e Ambiental.
- Segurança do Pessoal.
- Resposta a incidentes.

- Auditoria e Rastreamento de Responsabilidades.
- Controle de Acesso ao Sistema e Proteção das Comunicações.
- Aplicações.

Cada categoria de controle da lista anterior é associada a vários itens de controle, que focam em pontos específicos da categoria.

Para cada item de controle deve ser definido se o item encontra-se: **implementado, não implementado** ou **não se aplica.**

O questionário pode ser respondido pelo **Gestor de Riscos** ou ele pode identificar outros profissionais mais aptos a responder sobre categorias específicas de controles.

A análise das respostas obtidas permite a quantificação do nível de maturidade da organização, do ponto de vista do escopo do **Projeto de GRSIC**, em cada uma das categorias abordadas.

Também pode-se focar na análise das unidades da organização separadamente de forma a avaliar de forma mais específica os processos de negócio e as informações tratadas na unidade. A importância para a organização dos processos de negócio e das informações tratados nas unidades determina os requisitos de proteção dessas unidades.

Unidades representam as partes em que uma organização pode ser decomposta – divisões, departamentos, setores ou até mesmo processos, sistemas ou perímetros de segurança.

Algumas questões chave podem auxiliar nesta avaliação, por exemplo:

- Existe algum sistema estruturante na organização?
- Quais processos de negócio existem e como eles estão associados aos objetivos da organização?
- Quais processos de negócio dependem do funcionamento correto da infraestrutura de tecnologia da informação?
- Que informação é tratada em cada processo de negócio?

- Que informação é especialmente importante e que requer proteção em termos de confidencialidade, integridade e disponibilidade?
- Quais condições externas que afetam a SIC? Exemplos: requisitos legais (leis e regulações), fatores geográficos, contexto social e cultural, requisitos de clientes, parceiros ou fornecedores e padrões específicos.

O **Responsável pela Unidade da Organização** é o incumbido de prover essas informações. O **Gestor de Riscos** e os **Responsáveis por Ativos** na unidade devem apoiá-lo nesta tarefa.

Nessa avaliação, o responsável pela unidade deve identificar os **ativos primários** da unidade.

Ativos primários são processos de negócio e suas atividades, bem como informações.

Cada processo de negócio e informação no escopo da unidade deve ser identificado e documentado por meio de uma breve descrição. Um questionário deve ser utilizado para determinar a criticidade que cada processo de negócio e que cada informação possui para organização.

Esse nível de criticidade está associado à gravidade e à extensão do dano à organização, às pessoas ou a outras organizações e também está associado às consequências de violações de segurança nos ativos primários. A classificação deve ser feita com respeito a cada atributo separadamente:

- **Confidencialidade;**
- **Integridade;**
- **Disponibilidade;**
- **Autenticidade.**

Cada atributo pode assumir uma das classificações e respectivos pesos abaixo. As questões base para a análise seguem o modelo: “O impacto e a extensão da perda de

[Confidencialidade, Integridade, Disponibilidade, Autenticidade] do ativo primário em análise pode ser definido como:".

- **Muito pouco crítico. (peso 1).** A [Confidencialidade, Integridade, Disponibilidade, Autenticidade] é irrelevante para a organização. Incidentes não causam impactos;
- **Pouco crítico. (peso 2).** A [Confidencialidade, Integridade, Disponibilidade, Autenticidade] é pouco relevante para a organização. Incidentes podem causar impactos muito baixos;
- **Moderadamente crítico. (peso 5).** A [Confidencialidade, Integridade, Disponibilidade, Autenticidade] é relevante para a organização. Incidentes podem causar impactos controláveis, mas não desprezíveis;
- **Crítico. (peso 8).** A [Confidencialidade, Integridade, Disponibilidade, Autenticidade] é altamente relevante para a organização. Incidentes podem causar problemas de grande impacto e extensão;
- **Altamente crítico. (peso 10).** A [Confidencialidade, Integridade, Disponibilidade, Autenticidade] é fundamental para a organização. Incidentes podem causar problemas cuja gravidade coloca em risco pessoas e a organização.

De modo geral, o nível de criticidade é maior quando a unidade da organização possui processos de negócio, atividades e informações associadas aos seguintes aspectos:

- **Sistema estruturante.**
- **Informações pessoais.**
- **Informações classificadas (Lei Federal N° 12.527/2011).**
- **Obrigações legais ou regulatórias.**
- **Interesses econômicos e comerciais.**
- **Atividades que podem afetar a ordem pública.**
- **Políticas e estratégias de negócios e de operação.**
- **Contratos com clientes e fornecedores.**

Depois de respondidos os questionários para todas as unidades e abordando todos os ativos primários, é possível obter **uma lista de ativos primários e respectivos valores de criticidade para cada unidade e para cada um dos atributos, além de valores totais.**

Essa informação é útil para se consolidar o escopo definido para o **Projeto de GRSIC**. Deve ser avaliado se os resultados desta pré-análise estão condizentes com o escopo definido ou se são necessárias alterações (aumentar ou diminuir o escopo do projeto).

A Tabela 6 ilustra como essas informações podem ser representadas. Ela ilustra uma forma como as informações sobre unidade U_A da organização podem ser identificadas. Para cada ativo primário A_{Ti}, são identificados os níveis de criticidade para Confidencialidade (C_{ATi}), Integridade (I_{ATi}), Disponibilidade (D_{ATi}) e Autenticidade (A_{ATi}). A criticidade total do ativo (TA_{Ti}) é calculada por meio de uma função F1 (por exemplo, o máximo entre os valores). A criticidade total da unidade (TU_{Ui}) é calculada por meio de uma função F2 (por exemplo, soma das criticidades dos ativos).

Ao se quantificar a criticidade dos ativos primários de cada unidade, estabelece-se a base para a tomada de decisões estratégicas sobre prioridades na gestão de riscos de segurança.

Unidade	Ativo Primário (Processos de Negócio)	Criticidade				Total Ativo	Total Unidade
		C	I	D	A		
U_A	A_{T1}	C_{AT1}	I_{AT1}	D_{AT1}	A_{AT1}	TA_{T1}=F1(C_{AT1}, I_{AT1}, D_{AT1}, A_{AT1})	TU_{UA}=F2(TA_{T1}, TA_{T2}, TA_{T3})
	A_{T2}	C_{AT2}	I_{AT2}	D_{AT2}	A_{AT2}	TA_{T2}=F1(C_{AT2}, I_{AT2}, D_{AT2}, A_{AT2})	
	A_{T3}	C_{AT3}	I_{AT3}	D_{AT3}	A_{AT3}	TA_{T3}=F1(C_{AT3}, I_{AT3}, D_{AT3}, A_{AT3})	

Tabela 6: Informações de resultado da pré-análise do escopo do Projeto de GRSIC

A **Figura 8** mostra o fluxo de tarefas da atividade.

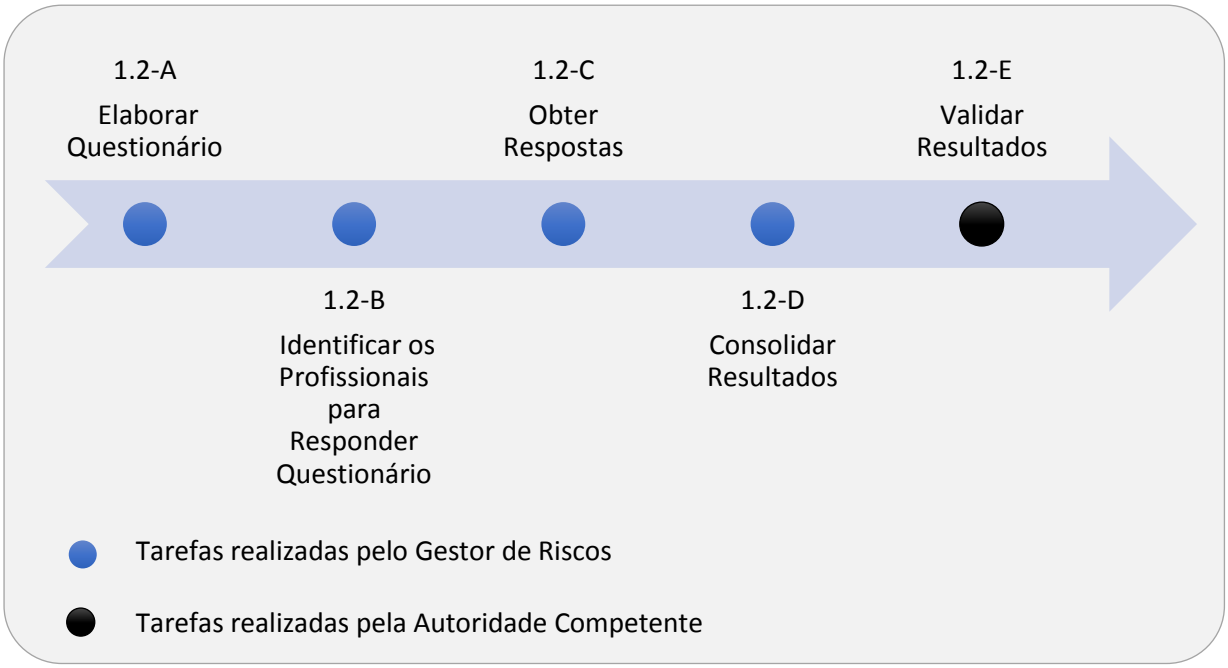

Figura 8: Fluxo de tarefas da Atividade 1.2 – Realizar Pré-análise do Escopo do Projeto de GRSIC

TAREFAS DA ATIVIDADE 1.2 – Realizar Pré-análise do Escopo do Projeto de GRSIC

Tarefa 1.2-A: Elaborar Questionário.

O Gestor de Riscos deve elaborar os Questionários de Pré-análise de forma a avaliar o nível de maturidade da organização em SIC do ponto de vista do escopo do Projeto de GRSIC e a criticidade dos ativos primários de cada unidade dentro do escopo do Projeto de GRSIC.

O Questionário de Pré-análise deve focar Itens de Controle e responder, para cada questão, qual o grau de implementação do Item de Controle: implementado / não implementado / não aplicável.

Para se realizar a avaliação da criticidade, uma lista de ativos primários para cada unidade deve ser elaborada. Posteriormente, para cada ativo, deve-se preencher os respectivos valores de criticidade e realizar os cálculos dos valores totais, conforme modelo proposto.

Responsável: Gestor de Riscos.

Tarefa 1.2-B: Identificar os Profissionais Para Responder ao Questionário.

O Gestor de Riscos deve identificar e comunicar os profissionais que irão responder ao Questionário de Pré-análise. É importante destacar que um ou mais profissionais podem ser escolhidos e que o próprio Gestor de Riscos pode também responder ao questionário.

Responsável: Gestor de Riscos.

Tarefa 1.2-C: Obter Respostas.

O Gestor de Riscos deve aplicar o questionário aos profissionais designados. Caso necessário, esses devem ser orientados sobre as respostas possíveis para cada questão.

Responsável: Gestor de Riscos.

Tarefa 1.2-D: Consolidar Resultados.

O Gestor de Riscos deve consolidar as respostas dos Questionários de Pré-análise. Posteriormente, o Gestor de Riscos deve notificar a Autoridade Competente sobre as informações disponíveis para realização da Tarefa 1.2-E: Validar Resultados e informar o respectivo prazo para conclusão da tarefa.

Responsável: Gestor de Riscos.

Tarefa 1.2-E: Validar Resultados.

A Autoridade competente deve analisar os Resultados da Pré-análise e registrar ciência dos resultados. Caso conveniente, ações de divulgação podem ser realizadas.

Responsável: Autoridade competente.

Condição para início:

- papéis para gestão de riscos definidos e respectivos profissionais identificados.

Informações necessárias:

- políticas da organização;
- procedimentos da organização;
- conhecimento de profissionais da organização.

Condição para ser finalizada:

- questionários respondidos, respostas compiladas e resumidas.

Informações produzidas:

- resultados da pré-análise;
- quantificação do nível de maturidade da organização em SIC do ponto de vista do escopo do Projeto de GRSIC em cada uma das categorias abordadas;
- identificação de pontos fortes e pontos para melhoria.

***Templates* da Atividade 1.2 – Realizar Pré-análise do Escopo do Projeto de GRSIC.**

A **Figura 9** mostra um modelo de **questionário de pré-análise**, o qual aborda categorias de controle. Cada categoria de controle está associada a vários itens de controle a serem classificados por grau de implementação.

A **Figura 10** ilustra um modelo de relatório com os resultados da pré-análise que identifica: unidades, ativos primários, valores de criticidades definidos na análise, totais de criticidade por ativo e por unidade.

A **Figura 11** apresenta um exemplo deste mesmo relatório.

QUESTIONÁRIO DE PRÉ-ANALISE **Nível de maturidade da organização em SIC, do ponto de vista do Escopo do Projeto de GRSIC**		
Categoria de Controle	**Itens de Controle**	**Grau de Implementação (Implementado / Não Implementado / NA)**
Categoria 1	Categoria 1 – Item 1	*Grau de Implementação*
	Categoria 1 – Item 2	*Grau de Implementação*
	...	**...**
	...	**...**
Categoria 2	Categoria 2 – Item 1	*Grau de Implementação*
	...	**...**
	...	**...**
Responsável pela informação: **Data:**		

Figura 9: Modelo de questionário de pré-análise

RESULTADOS DA PRÉ-ANÁLISE Criticidade dos Ativos Primários de Cada Unidade								
Unidade	**Ativo Primário (Processo de Negócio)**		**Criticidade**				**Total Ativo (Máximo valor de C,I,D,A)**	**Total Unidade (soma de criticidades dos ativos da unidade)**
	Identificador	**Descrição**	**C**	**I**	**D**	**A**		
U_A	A_{T1}	Descrição A_{T1}	C_{AT1}	I_{AT1}	D_{AT1}	A_{AT1}	TA_{T1}= max (C_{AT1}, I_{AT1}, D_{AT1}, A_{AT1})	TU_{UA}=(TA_{T1}+ +TA_{T2}+TA_{T3}+ **…**)
	A_{T2}	Descrição A_{T2}	C_{AT2}	I_{AT2}	D_{AT2}	A_{AT2}	TA_{T2}= max (C_{AT2} , I_{AT2}, D_{AT2}, A_{AT2})	
	A_{T3}	Descrição A_{T3}	C_{AT3}	I_{AT3}	D_{AT3}	A_{AT3}	TA_{T3}= max (C_{AT3}, I_{AT3}, D_{AT3}, A_{AT3})	
…	…	…	…	…	…	…	…	…
Responsável pela informação: **Data:**								

Figura 10: Modelo de relatório dos resultados da pré-análise

RESULTADOS DA PRÉ-ANÁLISE Criticidade dos Ativos Primários de Cada Unidade								
Unidade	**Ativo Primário**		**Criticidade**				**Total Ativo**	**Total Unidade**
	ID	**Descrição**	**C**	**I**	**D**	**A**		
Divisão de Planejamento	A_{T1}	Documento preliminar de planejamento estratégico	10	8	5	8	**10**	**15**
	A_{T2}	Processo de reserva de salas / equipamentos	1	2	5	2	**5**	
Divisão de Operações	A_{T3}	Controle de suprimentos	5	10	10	8	10	**10**

Responsável pela informação: Sr. Cláudio Santos
Data: 10/05/2015

Figura 11: Exemplo de relatório dos resultados da pré-análise

6.4 – Processo 2 – Identificar Riscos

6.4.1 – Descrição do Processo

Esse processo trata da identificação e descrição de riscos no espoco do **Projeto de GRSIC** e das consequências adversas resultantes. Busca-se compreender possíveis ameaças e vulnerabilidades existentes e avaliar a extensão e a adequação dos controles utilizados.

Recomenda-se que seja feita uma priorização, focando os esforços e recursos primeiro em setores mais críticos e, depois, nos sucessivamente menos críticos. Importante destacar que existem ameaças e vulnerabilidades que impactam a organização como um todo e, dessa forma, deve-se priorizar o tratamento dessas ameaças também.

As atividades desse processo e do processo seguinte (**Processo 3 – Estimar Riscos**) geram informações que são consolidadas no **Mapa de Riscos**.

O Mapa de Riscos agrupa as informações sobre riscos geradas de forma incremental em cada atividade.

A **Figura 12** mostra o fluxo de atividades do processo.

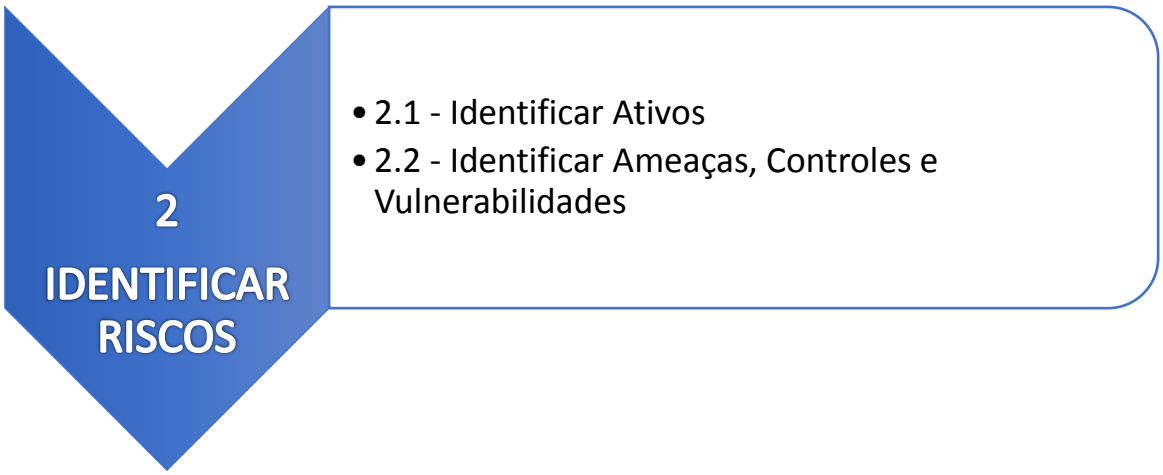

Figura 12: Fluxo de atividades do Processo 2 – Identificar Riscos

6.4.2 – Atividade 2.1 – Identificar Ativos

Nesta atividade são identificados os ativos que estão no escopo do **Projeto de GRSIC**.

Os resultados da pré-análise podem servir como base para priorizar a identificação de ativos de unidades mais críticas. Esses resultados também indicam o nível de detalhe requerido para a identificação dos ativos. Em unidades menos críticas pode ser suficiente identificar apenas alguns ativos primários (informações ou processos de negócio). Já para unidades que requerem maior nível de proteção, pode ser necessário identificar os ativos que suportam processos de negócio como hardware, software, salas, etc.).

Ativo é tudo que tem valor para a organização e que deve estar no escopo do Projeto de GRSIC.

De modo geral os tipos ativos para a identificação e o registro são:

Ativos primários:

- Processos de negócio e suas atividades;
- Informações;

Ativos de suporte:

- **Hardware**, por exemplo:
    - Equipamentos de processamento fixos (microcomputadores, servidores, etc);
    - Equipamentos de processamento móveis (notebooks, celulares, etc);
    - Periféricos;
    - Mídias de dados (pen-drive, cd, etc.);
    - Outras mídias não eletrônicas (documentos em papel);
- **Software**, por exemplo:
    - Sistemas operacionais;
    - Software de administração;
    - Pacotes de software;

- Aplicações de negócio.

- **Redes**, por exemplo:
  - Mídias e apoio (equipamentos e protocolos, como Ethernet, protocolos e equipamento WiFi, Bluetooth, Firewall, etc.);
  - Equipamentos intermediários (roteadores, hub, switch);
  - Interfaces de comunicação (adaptadores);
- **Pessoal**, por exemplo:
  - Tomadores de decisão (proprietários de ativos, responsáveis por unidades, representantes da Alta Administração...);
  - Usuários (pessoal que interage com os ativos, recursos humanos, terceirizados, etc.);
  - Pessoal de operação e manutenção (administrador do sistema, administrador de banco de dados, *help desk*, etc.);
  - Desenvolvedores (analistas, programadores, etc.);
- **Locais/recursos**, por exemplo:
  - Ambiente externo (outras organizações, casas de pessoas, etc.);
  - Zonas, locais (prédios, áreas de escritório, salas reservadas, etc.);
  - Serviços essenciais (energia elétrica);
  - Comunicações (telefone);
  - Utilidades (nobreaks, ar-condicionado, etc.);
- **Organização**, por exemplo:
  - Autoridades (líderes, representantes da Alta Administração);
  - Estrutura da organização (gerenciamento de RH, financeiro...);
  - Projetos da organização (migração de sistemas, desenvolvimentos...);
  - Subcontratados (gerenciamento externo, consultores...).

Deve-se notar que esta lista de tipos de **Ativos de Suporte** é abrangente. Espera-se que uma boa parte das organizações que utilizarão a MGR-SISP terá necessidade de tratar apenas um subconjunto desses tipos de ativos.

Sugere-se uma abordagem “top-down” para a análise e cadastro dos ativos. Inicialmente devem ser cadastrados os processos de negócio; as atividades; e as

informações. Depois de cadastrados esses ativos primários, devem ser cadastrados os ativos de apoio aos básicos (espaços físicos, hardware, software, etc.).

A **Figura 13** mostra o fluxo de tarefas desta atividade.

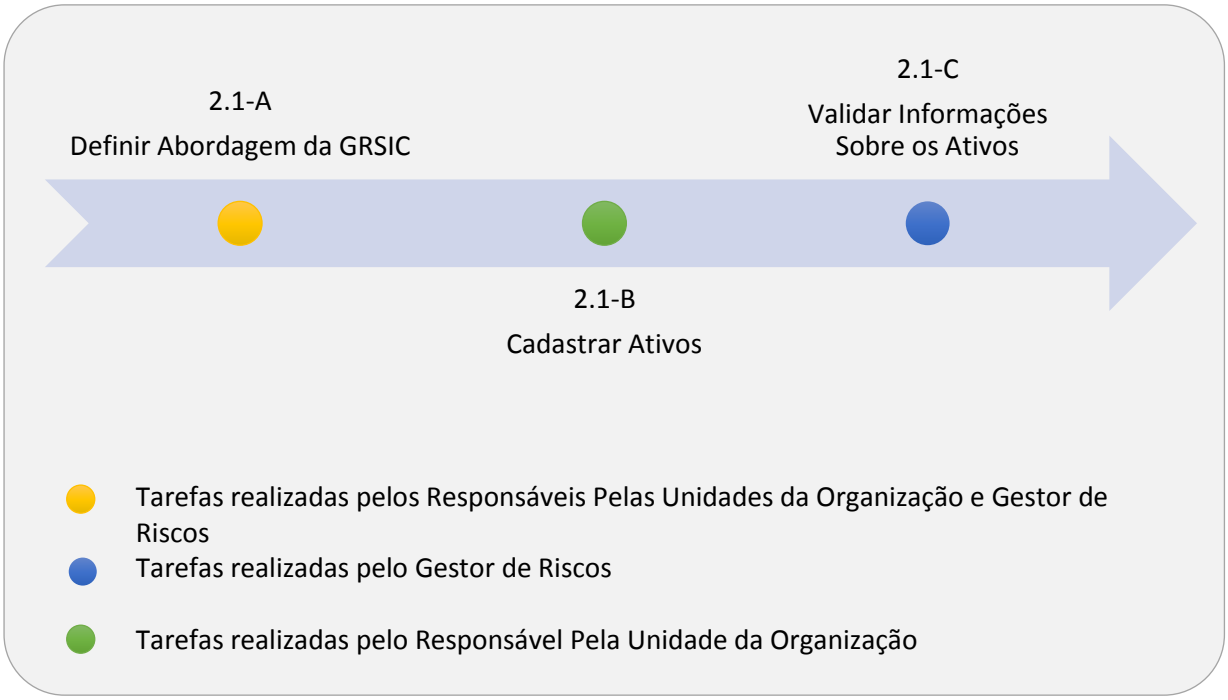

Figura 13: Fluxo de tarefas da Atividade 2.1 – Identificar Ativos

TAREFAS DA ATIVIDADE 2.1 – Identificar Ativos

Tarefa 2.1-A: Definir Abordagem da GRSIC.

Cada Responsável Pela Unidade da Organização, juntamente com o Gestor de Riscos, devem retomar as informações geradas nas atividades do Processo 1 – Estabelecer Contexto para definir como abordar a gestão de riscos em cada unidade no espoco do Projeto de GRSIC. Deve ser decidido, para cada unidade, o nível de detalhamento a ser adotado na identificação de ativos. Posteriormente, devem ser notificados os Responsáveis Pelas Unidades da Organização onde a MGR-SISP será aplicada para que os ativos sejam identificados segundo a abordagem definida e nos prazos estabelecidos.

Responsável: Responsável Pela Unidade da Organização e Gestor de Riscos.

Tarefa 2.1-B: Cadastrar Ativos.

Os Responsáveis Pelas Unidades da Organização devem identificar e registrar no Mapa de Riscos cada ativo que faz parte do escopo do Projeto de GRSIC. Informações de ativos primários já cadastrados na Atividade 1.2 – Realizar Pré-análise do Escopo do Projeto de GRSIC devem ser

revisadas. Outros ativos primários e os ativos de suporte devem ser identificados e cadastrados.

Informações típicas que caracterizam os ativos são:

- natureza (primário ou suporte);
- tipo (hardware, software, etc.);
- subtipo (notebook, pen-drive, etc.);
- descrição; responsável pelo ativo;
- responsável pela unidade que abriga o ativo;
- data de cadastro;
- localização física;
- valor de reposição.

Esta tarefa é realizada em cada unidade da organização no escopo do Projeto de GRSIC. Ela pode ser realizada em série (uma unidade após a outra, em ordem priorizada por criticidade) ou em paralelo (realizada simultaneamente em todos os setores).

O resultado da tarefa é o cadastro de cada ativo em cada unidade da organização que faz parte do escopo do Projeto de GRSIC.

Posteriormente, o Responsável Pela Unidade da Organização deve notificar o Gestor de Riscos das informações disponíveis para realização da Tarefa 2.1-C: Validar Informações Sobre os Ativos.

Responsável: Responsável Pela Unidade da Organização com apoio dos Responsáveis Por Ativos e do Gestor de Riscos.

Tarefa 2.1-C: Validar Informações Sobre os Ativos.

O Gestor de Riscos deve avaliar as informações sobre ativos no Mapa de Riscos. Caso esteja de acordo, o Gestor de Riscos deve registrar a aprovação e encerra-se, dessa forma, a Atividade2.1 – Identificar Ativos. Caso contrário, o Gestor de Riscos deve notificar o Responsável Pela Unidade da Organização da necessidade de reexecutar a Tarefa 2.1-B: Cadastrar Ativos e informar o prazo para conclusão da tarefa, bem como as orientações para aprimoramento das informações. Esse ciclo se repete até que Gestor de Riscos aprove as informações e registre este fato.

Responsável: Gestor de Riscos.

Condição para início:

- atividades do Processo 1 – Estabelecer Contexto finalizadas.

Informações necessárias:

- objetivos e premissas e restrições do Projeto de GRSIC;

- escopo do Projeto de GRSIC;
- resultados da pré-análise;
- critérios de avaliação de riscos e de aceitação de riscos.

Condição para ser finalizada:

- ativos identificados.

Informações produzidas:

- Mapa de Riscos com informações sobre os ativos.

***Template* e exemplo da Atividade 2.1 – Identificar Ativos.**

A **Figura 14** mostra o **Mapa de Riscos** com as informações relativas aos ativos e ao cadastro realizado na atividade. A **Figura 15** mostra um exemplo.

MAPA DE RISCOS								
Ativos								
ID	**Natureza**	**Tipo - Subtipo**	**Unidade**	**Responsá-vel**	**Descrição**	**Localização**	**Data**	**Responsável Pelo Cadastro**
A01	Nature za A01	Tipo A01	Unidad e A01	Respon-sável A01	Descrição A01	Localiza-ção A01	Data de Cadas-tro A01	Responsá-vel Cad. A01
A02	Nature za A02	Tipo A02	Unidad e A02	Respon-sável A02	Descrição A02	Localiza-ção A02	Data de Cadas-tro A02	Responsá-vel Cad. A02
...	**...**	**...**	**...**	**...**	**...**	**...**	**...**	**...**

Figura 14: *Template* do Mapa de Riscos – ativos

MAPA DE RISCOS								
Ativos								
ID	**Natureza**	**Tipo - Subtipo**	**Unidade**	**Responsável**	**Descrição**	**Localização**	**Data**	**Responsável Pelo Cadastro**
A01	Primário	Processo Negócio	DMPS	João Silva	Processo avaliação RDA	DMPS – Sala 15	09/06 /15	Maria da DMPS
A02	Suporte	Sala	DSSI	Miguel Souza	Sala 31 da DSSI	Prédio 3, andar 2	09/06 /15	Gestor de Riscos José Carlos
A03	Suporte	Hardwar e Servidor	DSC	Paulo Oliveira	Servidor Dell Modelo XY	Prédio 3, andar 2, Datacenter1	09/06 /15	Paulo da DSC

Figura 15: Exemplo de Mapa de Riscos - ativos

6.4.3 – Atividade 2.2 – Identificar Ameaças, Controles e Vulnerabilidades

Para cada ativo identificado na Atividade 2.1, devem ser analisadas e identificadas as ameaças, os controles e as vulnerabilidades associadas a cada ativo identificado.

Identificando Ameaças

Ameaças tem o potencial de causar prejuízo aos ativos da organização. Elas podem possuir origem humana ou natural e podem ser acidentais ou propositais.

Deve ser realizada a identificação de ameaças para cada ativo identificado no escopo do **Projeto de GRSIC**. Em geral um tipo de ativo (processo, hardware, software, informação, etc.) está sujeito a um subconjunto de ameaças dentre todas as ameaças existentes. Além disso, uma mesma ameaça pode impactar vários ativos de certo tipo ou ativos de tipos diferentes.

Uma ameaça existente para um ativo caracteriza a presença de um risco.

As ameaças que se aplicam ao ativo em análise devem ser identificadas e documentadas para consideração em etapa posterior **Processo 3 – Estimar de Riscos**.

Para auxiliar na identificação de ameaças, devem ser utilizados catálogos de ameaças típicas (como os fornecidos em IT-*Grundschutz*, ou ISO/IEC 27005).

Tipos de ameaça incluem:

- **Dano físico:** fogo, destruição de equipamentos...
- **Eventos naturais:** enchente, terremotos...
- **Falta de serviços essenciais:** perda de energia, perda de telecomunicações...
- **Comprometimento da informação:** roubo de mídias, revelação de sigilos, falsificação por software, fontes não confiáveis...
- **Falhas técnicas:** falha de equipamentos, falha de software...
- **Ações não autorizadas:** adulteração de dados, uso não autorizado de equipamentos...
- **Comprometimento de funções:** erro em uso, abuso de direitos...

As ameaças que se aplicam ao ativo em análise devem ser identificadas com auxílio do catálogo de ameaças. Deve ser feita uma descrição de como a ameaça gera impacto no ativo.

Caso seja identificada uma possível ameaça ao ativo que não esteja no catálogo, essa nova ameaça deve ser inserida no catálogo. Deve-se também associar a ameaça ao ativo e descrever o impacto que a ameaça causa a ele.

Essa informação será utilizada no **Processo 3 – Estimar Riscos** para auxiliar a estimativa dos riscos identificados no processo anterior.

Identificando Controles

Ao se identificar as ameaças que podem existir em relação aos ativos ou à organização, deve-se estabelecer controles para protegê-los contra essas ameaças.

Controles protegem o ativo e evitam que ameaças explorem suas vulnerabilidades e cause danos a ele e ao seu contexto.

Um controle é "uma forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas, estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal".

Controles de modo geral tem o efeito de reduzir os riscos por meio de dois fatores:

- **Realizam uma redução da exposição de um ativo ao risco, protegendo-o e diminuindo assim a probabilidade de que incidentes ocorram.**
- **Realiza uma redução da gravidade da consequência em termos abrangência, de duração e de impacto na organização.**

Esta atividade trata da identificação dos controles associados aos ativos e ameaças identificados nas atividades anteriores.

Cada ativo pode estar sujeito a uma ou mais ameaças. Um par [ativo, ameaça] caracteriza um risco para o qual um ou mais controles podem ser aplicados.

Para auxiliar na identificação de possíveis controles, devem ser utilizados catálogos de controles existentes associados às ameaças, como os fornecidos em IT-*Grundschutz* ou ISO/IEC 27002.

Recomenda-se realizar, para cada ativo e cada ameaça associada, a seguinte análise junto ao **Responsável pelo Ativo**:

- **Identificar os controles aplicáveis para proteger o ativo da ameaça (utilizar catálogo).**
- **Para cada controle, avaliar por meio de investigações e análises a existência (ou não) do controle implementado na organização.**

Na MGR-SISP a situação da implementação do controle pode ser classificada em uma das seguintes categorias:

a) **Não implementado;**
b) **Implementado;**
c) **Não se aplica ou desnecessário.**

Posteriormente, deve-se justificar as classificações. Caso o responsável pela análise idealize algum controle não presente no catálogo, mas que possa proteger o ativo, esse controle deve ser inserido no catálogo de controles, associando-se o novo controle ao ativo e ameaça.

O resultado dessa análise permite identificar, para cada ameaça e ativo, a existência (no estado atual da organização) de controles para proteger o ativo e a efetividade desses controles. Essa informação é útil para a tomada de decisões em etapas posteriores.

Identificando Vulnerabilidades

A definição de vulnerabilidades é uma consequência do mapeamento das ameaças ao ativo.

Quando um ativo apresenta uma ameaça e não há controles implementados para proteger o ativo desta ameaça, tem-se uma vulnerabilidade exposta.

Uma vulnerabilidade é definida como "fraqueza de um determinado ativo ou controle que pode ser explorado por uma ameaça.".

Quando uma vulnerabilidade de um ativo é explorada por uma ameaça pode ocorrer uma violação da segurança.

As vulnerabilidades podem ser exploradas por ameaças e causar danos aos ativos ou à organização. Esta atividade tem o propósito de identificar essas vulnerabilidades. Elas podem estar associadas a diferentes áreas como: organização, processos e procedimentos, rotinas de gerenciamento, recursos humanos, ambiente físico, configuração dos sistemas de informação, hardware, software, etc. Para auxiliar na identificação de vulnerabilidades, devem ser utilizados catálogos de vulnerabilidades como os fornecidos em IT-*Grundschutz* ou em ISO/IEC 27005. Recomenda-se realizar, para cada ativo e cada ameaça associada, a seguinte análise junto ao **Responsável Pelo Ativo**:

- Identificar os **controles não implementados** para proteger o ativo da ameaça (resultado da atividade anterior).
- Para cada controle, avaliar por meio de investigações e análises a existência (ou não) de **vulnerabilidades associadas ao ativo**. A lista de vulnerabilidades pode ser utilizada.

Adicionalmente, caso seja identificada alguma vulnerabilidade não presente no catálogo consultado, essa nova vulnerabilidade deve ser inserida no catálogo de vulnerabilidades.

Importante destacar que quaisquer vulnerabilidades devem ser documentadas, sejam elas relacionadas ou não a controles não implementados. A **Figura 16** mostra o fluxo de tarefas da atividade.

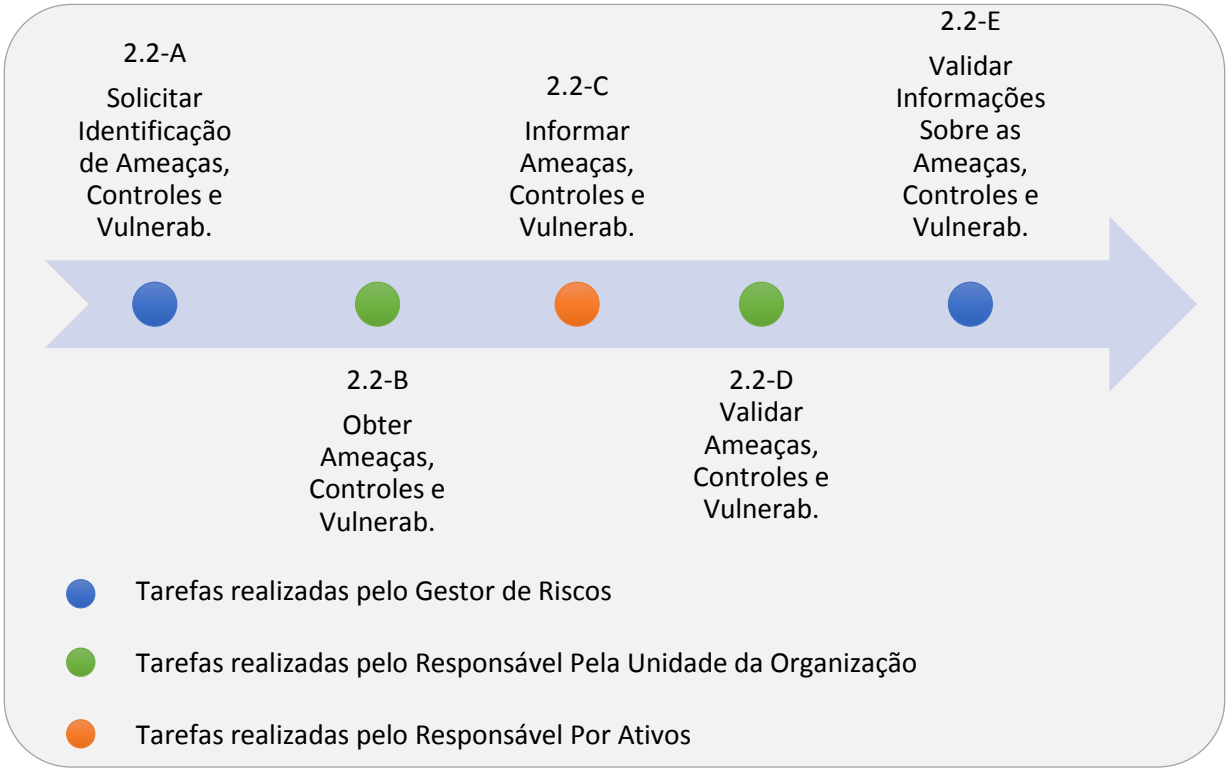

Figura 16: Fluxo de tarefas da Atividade 2.2 – Identificar Ameaças, Controles e Vulnerabilidades.

TAREFAS DA ATIVIDADE 2.2 – Identificar Ameaças, Controles e Vulnerabilidades

Tarefa 2.2-A: Solicitar Identificação de Ameaças, Controles e Vulnerabilidades.

O Gestor de Riscos notifica os Responsáveis Pelas Unidades da Organização para realização da Tarefa 2.2-B: Obter Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade e informa o

prazo para conclusão da tarefa.

Responsável: Gestor de Riscos.

Tarefa 2.2-B: Obter Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade.

O Responsável pela Unidade da Organização notifica os Responsáveis Por Ativos para realização da Tarefa 2.2-C: Informar Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade e informa o prazo para conclusão da tarefa.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 2.2-C: Informar Ameaças, Controles e Vulnerabilidades dos Ativos.

O Responsável pela Unidade da Organização deve acompanhar e apoiar os Responsáveis Por Ativos da sua Unidade na realização desta tarefa.

O Responsável Por Ativos deve, para cada ativo identificado na atividade anterior, identificar, no Mapa de Riscos, as ameaças existentes (a partir de uma lista), bem como descrever essas ameaças. Além disso, devem ser informados os controles aplicáveis e a situação de implementação de cada controle (Implementado ou Não Implementado). A partir da análise dos controles, devem ser identificadas, no Mapa de Riscos, as vulnerabilidades para as quais não há controles implementados. Posteriormente, o Responsável Por Ativos deve notificar o Responsável Pela Unidade da Organização das informações disponíveis para realização da Tarefa 2.2-D: Validar Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade.

Responsável: Responsável Por Ativos com apoio do Responsável pela Unidade da Organização.

Tarefa 2.2-D: Validar Ameaças, Controles e Vulnerabilidades dos Ativos da Unidade.

O Responsável pela Unidade da Organização deve avaliar, no Mapa de Riscos, as informações das ameaças, controles e vulnerabilidades relacionadas aos ativos da unidade. Caso estejam de acordo, o Responsável Pela Unidade da Organização deve notificar o Gestor de Riscos das informações disponíveis para realização da Tarefa 2.2-E: Validar Informações Sobre as Ameaças, Controles e Vulnerabilidades. Caso contrário, o Responsável Pela Unidade da Organização deve realizar, juntamente com o Responsável Por Ativos, as alterações necessárias no Mapa de Riscos e notificar o Gestor de Riscos das informações disponíveis para realização da Tarefa 2.2-E: Validar Informações Sobre as Ameaças, Controles e Vulnerabilidades.

Responsável: Responsáveis pelas Unidades da Organização. O Gestor de Riscos pode apoiar.

Tarefa 2.2-E: Validar Informações Sobre as Ameaças, Controles e Vulnerabilidades.

O Gestor de Riscos deve avaliar as informações no Mapa de Riscos. Caso estejam de acordo, o Gestor de Riscos deve registrar a aprovação e encerra-se, dessa forma, a Atividade 2.2 – Identificar Ameaças, Controles e Vulnerabilidades. Caso contrário, o Gestor de Riscos deve notificar o Responsável Pela Unidade da Organização da necessidade de reexecutar uma ou mais das tarefas anteriores e informar o prazo para conclusão das tarefas, bem como as orientações para aprimoramento das informações. Nesse caso, devem ser realizadas novamente as Tarefas 2.2-B a 2.2-E até que Gestor de Riscos aprove as informações e registre esse fato.

Responsável: Gestor de Riscos.

Condição para início:

- identificação de ativos realizada. (Mapa de Riscos com o ativo)

Informações necessárias:

- informações sobre ativos, sobre ameaças e sobre controles.

Condição para ser finalizada:

- ameaças, controles e vulnerabilidades identificadas e documentadas.

Informações produzidas:

- Mapa de Riscos com informações sobre os ativos, respectivas ameaças e os status de implementação de controles. Cada ativo pode estar sujeito a mais de uma ameaça. Para cada par [ativo, ameaça] podem existir zero ou mais controles implementados.
- Novos controles identificados inseridos no catálogo de controles.

***Template* e exemplo da Atividade 2.2 – Identificar Ameaças, Controles e Vulnerabilidades.**

A **Figura 17** mostra o Mapa de Riscos com as informações relativas aos ativos, às respectivas ameaças e aos controles para cada ameaça tais como: descrição do controle, situação de implementação e justificativas.

A **Figura 18** apresenta um exemplo.

MAPA DE RISCOS					
Ativos		**Ameaças**		**Controles**	
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Situação / Justificativa**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	Descrição Controle 1	Situação / Justificativa Controle 1
				Descrição Controle 2	Situação / Justificativa Controle 2
				...	...
		Tipo Ameaça 2	Descrição Ameaça 2	Descrição Controle 1	Situação / Justificativa Controle 1
				Descrição Controle 2	Situação / Justificativa Controle 2
				...	...
A02	Descrição A02	Tipo Ameaça 1	Descrição Ameaça 1	...	...
		Tipo Ameaça 2	Descrição Ameaça 2	...	...

Figura 17: *Template* do Mapa de Riscos – ativos, ameaças e controles

MAPA DE RISCOS					
Ativos		**Ameaças**		**Controles**	
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Situação / Justificativa**
A01	Processo avaliação RDA	Comprometi-mento da informação	Extravio do documento sigiloso RDA-YZ.doc	Conscientização “mesa limpa”	Não Implementado
				Fechadura mecânica	Implementado
				Câmara monitoramento.	Não Implementado
		Ações não autorizadas	Acesso de não autorizados no ambiente físico	Política e procedimentos de controle acesso	Não Implementado

		RdaR	Fechadura mecânica	Implementado
			Câmara monitoramento.	Implementado
	Falhas técnicas	Sistema de apoio RDA-AB pouco confiável	Realizar teste de software	Não Implementado
	Comprometi-mento de funções	Abuso de diretos de acesso ao sistema RDA- CD	Realizar teste de segurança	Implementado

Figura 18: Exemplo de Mapa de Riscos – ativos, ameaças e controles

A **Figura 19** mostra o Mapa de Riscos com as informações relativas aos ativos, às respectivas ameaças, aos controles para cada ameaça e às vulnerabilidades (descrição da vulnerabilidade, se existente). As vulnerabilidades são associadas a controles não implementados ou a controles implementados inadequadamente.

A **Figura 20** apresenta um exemplo.

MAPA DE RISCOS						
Ativos		**Ameaças**		**Controles**		**Vulnerabilidades**
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Situação / Justificativa**	**Descrição**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	Descrição Controle 1	Situação / Justificativa Controle 1	Descrição da Vulnerabilidade 1
				Descrição Controle 2	Situação / Justificativa Controle 2	Descrição da Vulnerabilidade 2
				...	...	...
		Tipo Ameaça 2	Descrição Ameaça 2	Descrição Controle 1	Situação / Justificativa Controle 1	Descrição da Vulnerabilidade 1
				Descrição Controle 2	Situação / Justificativa	Descrição da Vulnerabilidade 2

				Controle 2		
				...	...	...
A02	Descrição A02	Tipo Ameaça 1	Descrição Ameaça 1	...	...	...
		Tipo Ameaça 2	Descrição Ameaça 2	...	...	...
...	...	...	...	...	...	...

Figura 19: *Template* do Mapa de Riscos – ativos, ameaças, controles e vulnerabilidades

MAPA DE RISCOS						
Ativos		**Ameaças**		**Controles**		**Vulnerabilidades**
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Situação / Justificativa**	**Descrição**
A01	Processo avaliação RDA	Compro-metimento da informação	Extravio do documento sigiloso RDA-YZ.doc	Conscientização “mesa limpa”	Não Implementado	Maior probabilidade do extravio de documentos e equipamentos
				Fechadura mecânica	Implementado	Nenhuma
				Câmara monitoramento	Não Implementado	Risco de não ter desempenho adequado
		Ações não autorizadas	Acesso de não autorizados no ambiente físico RdaR	Política e procedimentos de controle acesso	Não Implementado	Risco de procedimentos não serem seguidos
				Fechadura mecânica	Implementado	Nenhuma
				Câmara monitoramento	Não Implementado	Impedimento de identificar responsáveis por invasões.
		Falhas técnicas	Sistema de apoio RDA-AB pouco	Realizar teste de software	Não Implementado	Problemas de disponibilidade e integridade de

		confiável			informações sensíveis
	Comprome-timento de funções	Abuso de diretos de acesso ao sistema RDA- CD	Realizar teste de segurança	Implementado	Nenhuma

Figura 20: Exemplo de Mapa de Riscos – ativos, ameaças, controles e vulnerabilidades

6.5 – Processo 3 – Estimar Riscos

6.5.1 – Descrição do Processo

Este processo trata da estimação dos riscos identificados no processo anterior (**Processo 2 – Identificar Riscos**). A estimação visa compreender o impacto das consequências provocadas caso as ameaças aos ativos ocorram de fato e definir quantitativamente o nível de impacto. Trata também de ponderar sobre quais são as chances de que as ameaças se tornem realidade. A **Figura 21** mostra o fluxo de atividades do processo.

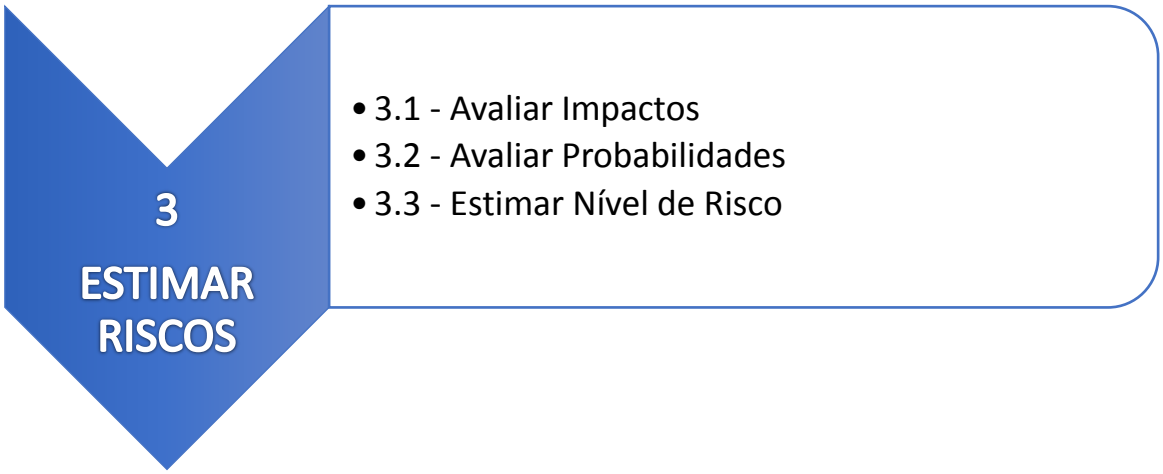

Figura 21: Fluxo de atividades do Processo 3 – Estimar Riscos

6.5.2 – Atividade 3.1 – Avaliar Impactos

Nesta atividade são avaliadas o impacto das possíveis consequências de riscos quando as ameaças se tornam realidade e provocam danos em ativos.

As consequências podem ter impacto nos ativos, na organização e nas pessoas.

Essa avaliação deve ser feita para cada ativo no escopo do **Projeto de GRSIC** e para cada ameaça ao ativo. O resultado da análise deve refletir a extensão do dano causado pela perda de atributos de segurança (confidencialidade, integridade, disponibilidade e autenticidade) associados ao ativo caso a ameaça se concretize (violação de segurança).

Devem ser considerados impactos diretos e indiretos. Custo de reposição do ativo roubado, por exemplo, é um impacto direto enquanto a divulgação de informações pessoais presentes no equipamento roubado e o comprometimento da imagem da organização podem ser exemplos de impactos indiretos.

O foco deve ser nos processos de negócio considerados críticos para a organização.

A avaliação deve considerar diferentes tipos consequências como, por exemplo:

- Violação da legislação.
- Violação de contratos.
- Problemas jurídicos.
- Prejuízo no desempenho.
- Prejuízo para a reputação e credibilidade.
- Violação de informações pessoais.
- Violação de informações confidenciais.
- Prejuízo à ordem pública.
- Perdas financeiras.
- Interrupção de serviços.
- Custos em termos de equipamentos, pessoal, especialistas.
- Danos materiais.
- Perigo à saúde e à vida.
- Perda de clientes ou fornecedores.

O responsável pela estimativa de riscos deve considerar as seguintes fontes de informação em sua análise:

- A lista de possíveis tipos de consequências (como a anterior);
- Informações históricas sobre incidentes. O conhecimento sobre o impacto para a organização em situações anteriores em que incidentes ocorreram (ameaças que se concretizaram afetando ativos do tipo em questão);
- O conhecimento dos responsáveis pelo ativo e informações;
- Controles existentes: importante notar que o nível de impacto quando uma consequência ocorre também é influenciado pelo estado atual dos controles implementados na organização. Isto é, o responsável pela estimativa de impacto deve levar em conta os controles já estabelecidos para refletir o fato de que o impacto é menor se controles eficazes existem e maior caso contrário.

Nessa análise, o responsável pela estimativa deve avaliar o impacto, para a organização e para pessoas, de incidentes de segurança associados ao ativo (perda de confidencialidade, perda de integridade, perda de disponibilidade ou perda de autenticidade).

A MGR-SISP classifica o impacto de violação de segurança (incidente) provocada pela ameaça ao ativo em uma das opções abaixo:

- **Muito Baixo (MB).**
- **Baixo (B).**
- **Moderado (M).**
- **Alto (A).**
- **Muito Alto (MA).**

Cada atributo de segurança (confidencialidade, integridade, disponibilidade e autenticidade) é contemplado separadamente, portanto, o responsável pela atividade realizará quatro análises distintas para cada ameaça e ativo.

As quatro análises para uma ameaça e ativo (uma para cada atributo de segurança) são consolidadas por meio de uma função:

$$I = F(IC, II, ID, IA)$$

Sendo:

- **I: Impacto.**
- IC: Impacto relativo à **Confidencialidade**.
- II: Impacto relativo à **Integridade**.
- ID: Impacto relativo à **Disponibilidade**.
- IA: Impacto relativo à **Autenticidade**.
- **F: Função de consolidação de impacto.**

A MGR-SISP define que o impacto resulta no maior valor entre IC, II, ID e IA.

$$I = Max\ (IC,II,ID,IA)$$

É importante destacar que os valores IC, II, ID e IA, além do valor I, devem ser registrados, pois esta informação é útil para que se definam os controles a serem aplicados para tratar riscos no **Processo 5 – Tratar Riscos**.

A seguir é fornecido um exemplo de questão e de classificação que podem ser utilizados para guiar a avaliação de impacto em relação ao atributo disponibilidade.

Questão: Em relação a disponibilidade

Classes:

- **Impacto Muito Baixo (MB):** nenhum serviço ou atividade é afetado;
- **Impacto Baixo (B):** poucos serviços ou atividades de menor importância são afetados, pode provocar atrasos desprezíveis;
- **Impacto Moderado (M):** alguns serviços ou atividades são afetados, podendo causar atrasos significativos;
- **Impacto Alto (A):** serviços essenciais são afetados, provocando atrasos graves e danos elevados;
- **Impacto Muito Alto (MA):** serviços essenciais são afetados severamente, gerando danos muito elevados e atrasos intoleráveis.

O resultado desta atividade é a estimativa de impacto para cada risco (uma ameaça a um ativo) e a classificação desse impacto em uma determinada classe – *Muito Baixo (MB); Baixo (B)*; *Moderado (M); Alto (A)*; *Muito Alto (MA)*.

Para cada classificação de impacto, o responsável pela avaliação de consequências deve descrever o motivo da classificação, além de detalhar as consequências do risco para ativos, para a organização, para pessoas ou para outras organizações. Isto é especialmente importante para os riscos com impacto mais alto.

Caso seja possível estimar quantitativamente o impacto, esse valor deve ser documentado. Por exemplo, **custo financeiro de reposição ou reparo do ativo; custo financeiro de operações suspensas; tempo para investigação e reparo; tempo de trabalho perdido.**

A **Figura 22** mostra o fluxo de tarefas da atividade.

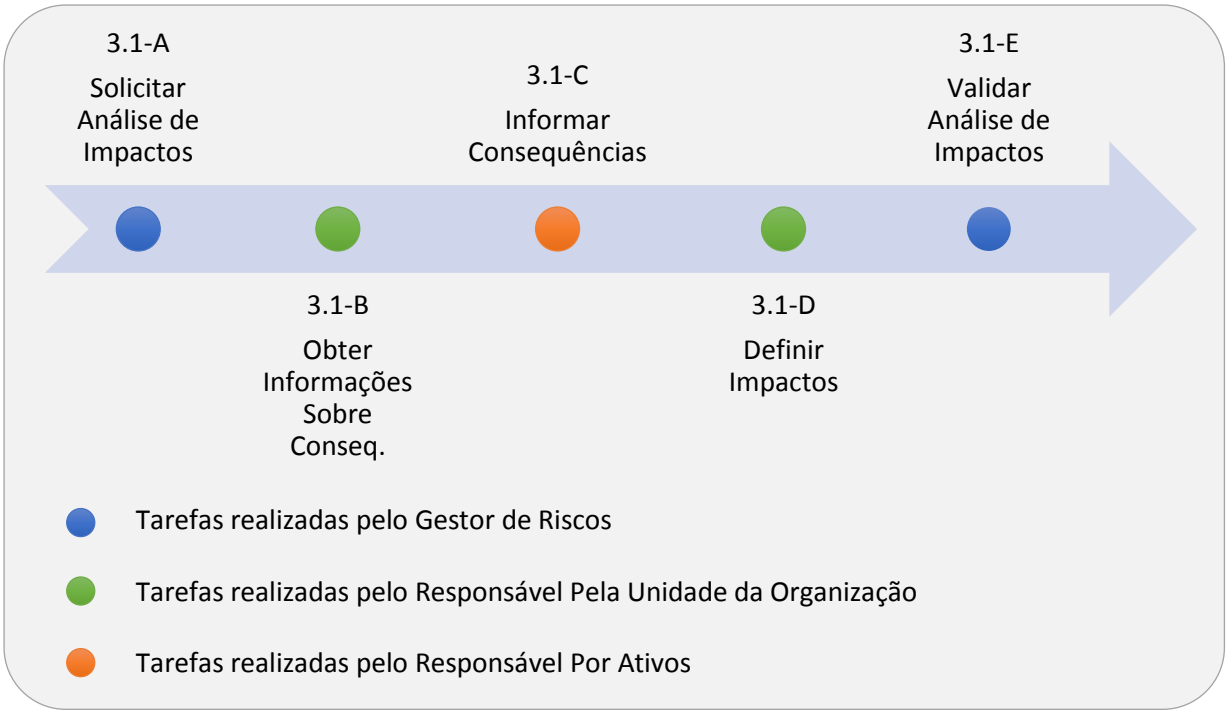

Figura 22: Atividade 3.1 – Avaliar Impactos

TAREFAS DA ATIVIDADE 3.1 – Avaliar Impactos

Tarefa 3.1-A: Solicitar Análise de Impactos.

O Gestor de Riscos notifica os Responsáveis pelas Unidades da Organização para a realização da Tarefa 3.1-B: Obter Informações Sobre Consequências e informa o prazo para realização da tarefa.

Responsável: Gestor de Riscos.

Tarefa 3.1-B: Obter Informações Sobre Consequências.

O Responsável pela Unidade da Organização notifica os Responsáveis Por Ativos para a realização da Tarefa 3.1-C: Identificar Consequências e informa também o prazo para realização da tarefa.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 3.1-C: Identificar Consequências.

O Responsável por Ativos deve identificar as consequências de riscos associadas aos ativos da unidade. Posteriormente, o Responsável por Ativos deve notificar o Responsável pela Unidade da Organização das informações disponíveis para realização da Tarefa 3.1-D: Definir Impactos.

Responsável: Responsável por Ativos.

Tarefa 3.1-D: Definir Impactos.

O Responsável pela Unidade da Organização deve analisar as informações sobre as consequências de riscos associadas aos ativos da unidade e definir o nível de impacto dos riscos no Mapa de Riscos. Como já descrito, devem ser identificadas as consequências e, baseado nelas, deve ser definido no nível de impacto do risco (Muito Baixo (MB); Baixo (B); Moderado (M); Alto (A); Muito Alto (MA)) em relação a cada atributo de segurança (confidencialidade, integridade, disponibilidade e autenticidade). Deve-se também detalhar as consequências e fornecer justificativas de classificação. A análise deve focar nos processos de negócio considerados críticos para organização. Posteriormente, o Responsável Pela Unidade da Organização deve notificar o Gestor de Riscos das informações disponíveis para realização da Tarefa 3.1-E: Validar Análise de Impactos.

Responsável: Responsável Pela Unidade da Organização. O Gestor de Riscos pode apoiar.

Tarefa 3.1-E: Validar Análise de Impactos.

O Gestor de Riscos deve avaliar as informações sobre os impactos de riscos associadas aos ativos das unidades no Mapa de Riscos. Caso estejam de acordo, o Gestor de Riscos deve registrar a aprovação e encerra-se, dessa forma, a Atividade 3.1 – Avaliar Impactos. Caso contrário, o Gestor de Riscos deve notificar o Responsável pela Unidade da Organização da necessidade de reexecutar uma ou mais das tarefas anteriores, informando o prazo para conclusão das tarefas, bem como as orientações para aprimoramento das informações. Nesse caso, devem ser realizadas novamente as Tarefas 3.1-B a 3.1-E até que Gestor de Riscos aprove as informações e registre este fato.

Responsável: Gestor de Riscos.

Condição para início:

- Mapa de Riscos atualizado.

Informações necessárias:

- Mapa de Riscos;
- Informações sobre incidentes de segurança;
- informações sobre os processos de negócio da organização e dos ativos que os suportam.

Condição para ser finalizada:

- impactos dos riscos identificados e estimados.

Informações produzidas:

- Mapa de Riscos atualizado com impactos de cada risco estimados.

***Template* e exemplo da Atividade 3.1 – Avaliar Impactos.**

A **Figura 23** mostra o Mapa de Riscos com as informações relativas aos ativos, às respectivas ameaças e os impactos. Para cada risco (ativo e ameaça) são apresentados os valores estimados de impacto para cada atributo de segurança (confidencialidade, integridade, disponibilidade e autenticidade) os valores totais de impacto e os detalhamentos (tipos e descrições de consequências).

A **Figura 24** apresenta um exemplo.

MAPA DE RISCOS										
Ativos		**Ameaças**		**Impactos**						
ID	**Descrição**	**Tipo**	**Descrição**	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Autenticidade**	**Total – Máximo (CIDA)**	**Tipo**	**Descrição**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	Valor C 1	Valor I 1	Valor D 1	Valor A 1	Max (CIDA) 1	Tipo Impacto 1	Descrição Consequência 1
		Tipo Ameaça 2	Descrição Ameaça 2	Valor C 2	Valor I 2	Valor D 2	Valor A 2	Max (CIDA) 2	Tipo Impacto 2	Descrição Consequência 2

		...	...		...	...	...	...	...	...	...
...	...	...	...		...	...	...	...	...	...	...

Figura 23: *Template* do Mapa de Riscos – ativos, ameaças e impactos

MAPA DE RISCOS											
Ativos		**Ameaças**		**Impactos**							
ID	**Descrição**	**Tipo**	**Descrição**	**Confidencialidade**	**Integridade**	**Disponibilidade**	**Autenticidade**	**Total – Máximo (CIDA)**	**Tipo**	**Descrição**
A01	Processo avaliação RDA	Comprome-timento da informação	Extravio do documen-to sigiloso RDA-YZ.doc	MA	B	A	B	MA	Violação de informações confiden-ciais. Problemas jurídicos.	Informações sigilosas de clientes divulgadas. Risco de processos. Atrasos.
		Ações não autorizadas	Acesso de não autoriza-dos no ambiente físico RdaR	B	MB	M	MB	M	Danos materiais.	Danos aos 2 PCs do ambiente. Atraso não grave
		Falhas técnicas	Sistema de apoio RDA-AB pouco confiável	MB	B	A	MB	A	Prejuízo no desempen-ho	Interrupção do processo RDA-AB. Atrasos sérios.

Figura 24: Exemplo de Mapa de Riscos – ativos, ameaças e impactos

6.5.3 – Atividade 3.2 – Avaliar Probabilidades

Nesta atividade são avaliadas as probabilidades de que ocorra uma violação de segurança, ou seja, uma ameaça se concretizam e provocam danos em ativos. Assim como a avaliação de impactos, realizada na atividade anterior, essa análise deve ser feita para cada ativo no escopo do **Projeto de GRSIC** e para cada ameaça ao ativo.

A avaliação de probabilidade deve refletir o quão frequentemente a ameaça ocorre e o quão facilmente as vulnerabilidades são exploradas no ativo.

Mais precisamente deseja-se estimar a probabilidade conjunta dos acontecimentos:

- a probabilidade de um evento ameaça seja provocado (para ações causadas propositalmente) ou ocorra (para ações causadas acidentalmente); e
- a probabilidade de que o evento, uma vez iniciado, irá resultar em impactos adversos para as operações da organização, seus ativos, pessoas ou outras organizações.

Embora sejam dois acontecimentos distintos, a MGR-SISP trata a probabilidade como um valor único para facilitar a análise.

Esta avaliação pode ser baseada nos seguintes elementos:

- informações estatísticas gerais sobre a probabilidade de incidentes de segurança;
- informações da organização sobre histórico de ocorrência de incidentes de segurança (frequência, ou periodicidade de ocorrência);
- informações da organização sobre a frequência ou a periodicidade de ocorrência de uma ameaça específica e da exploração das vulnerabilidades associadas;

  para ações causadas propositalmente: as fontes de ameaça; características de capacidade da fonte em causar danos; características de intenção e motivação de fonte em causar danos; percepção exterior da atratividade e

vulnerabilidade do ativo; facilidade para converter a exploração da vulnerabilidade do ativo em uma recompensa;

- para ações causadas acidentalmente: fatores geográficos propensos a gerar problemas; fatores que podem favorecer erros humanos ou falhas de equipamentos;
- controles existentes: Importante notar que o nível de probabilidade de um risco se concretizar também é afetado pelo estado atual dos controles implementados na organização. Isto é, o responsável pela estimativa de probabilidades deve levar em conta os controles já estabelecidos para refletir o fato de que as probabilidades são menores se controles eficazes existem, e maiores caso contrário.

O responsável pela avaliação deve fazer a classificação do nível de probabilidade de violação de segurança provocada pela ameaça ao ativo em uma das opções abaixo:

- **Muito Baixa (MB)**
- **Baixa (B)**
- **Moderada (M)**
- **Alta (A)**
- **Muito Alta (MA)**

Segue abaixo um exemplo de diretriz para classificação, configurável no **Processo 1 – Estabelecer Contexto**.

- **Probabilidade Muito Baixa (MB).** Altamente improvável, ocorre menos de 1 vez a cada 10 anos.
- **Probabilidade Baixa (B).** Improvável, ocorre menos que 1 vez a cada ano e mais do que 1 vez a cada 10 anos.
- **Probabilidade Moderada (M).** Provável, ocorre entre 1 e 10 vezes por ano.
- **Probabilidade Alta (A).** Alto. Altamente provável, ocorre entre 10 e 100 vezes ao ano.
- **Probabilidade Muito Alta (MA).** Quase certo, Ocorre mais do que 100 vezes ao ano.

O resultado da avaliação de probabilidade é a atribuição de uma classe de probabilidade para cada risco analisado.

A **Figura 37** mostra o fluxo de tarefas da atividade.

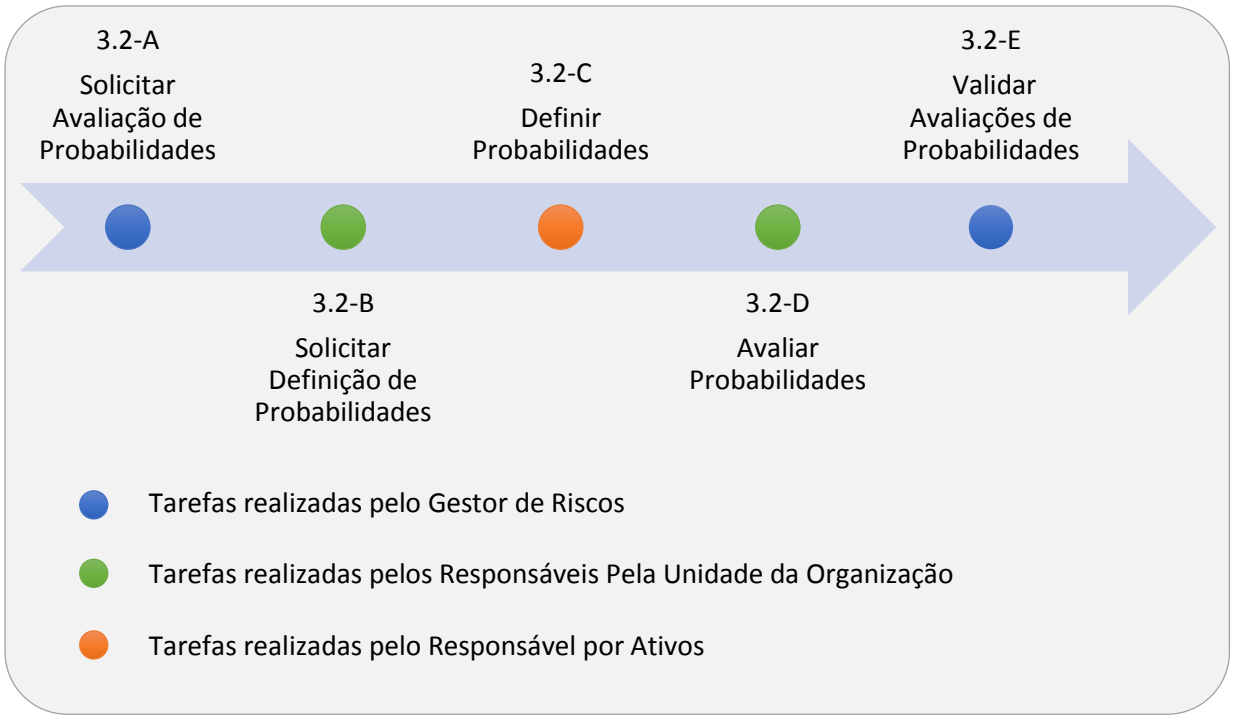

Figura 25: Atividade 3.2 – Avaliar Probabilidades

TAREFAS DA ATIVIDADE 3.2 – Avaliar Probabilidades

Tarefa 3.2-A: Solicitar Avaliação de Probabilidades.

O Gestor de Riscos notifica os Responsáveis Pelas Unidades da Organização para realização da Tarefa 3.2-B: Solicitar Definição de Probabilidades e informa também o prazo para realização da tarefa.

Responsável: Gestor de Riscos.

Tarefa 3.2-B: Solicitar Definição de Probabilidades.

Cada Responsável Pela Unidade da Organização deve notificar os Responsáveis Por Ativos para realização da Tarefa 3.2-C: Definir Probabilidades e informar o prazo para realização da tarefa.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 3.2-C: Definir Probabilidades.

Os Responsáveis Por Ativos definem, no Mapa de Riscos, as probabilidades dos riscos

(probabilidade de que as ameaças concretizem-se e provoquem danos em ativos). Para cada risco deve ser identificada a classe de probabilidade – Muito Baixa (MB); Baixa (B); Moderada (M); Alta (A); Muito Alta (MA). Deve-se também fornecer justificativas de classificação. Posteriormente, os Responsáveis Por Ativos devem notificar o Responsável Pela Unidade da Organização das informações disponíveis no Mapa de Riscos para realização da Tarefa 3.2-D: Avaliar Probabilidades.

Responsável: Responsável Por Ativos. O Responsável pela Unidade deve apoiar.

Tarefa 3.2-D: Avaliar Probabilidades.

O Responsável Pela Unidade da Organização analisa as informações obtidas na tarefa anterior (3.2-C) no Mapa de Riscos e, caso estejam de acordo, notificam o Gestor de Riscos das informações disponíveis para realização da Tarefa 3.2-E: Validar Avaliações de Probabilidades. Caso contrário, o Responsável Pela Unidade da Organização deve notificar os Responsáveis Por Ativos da necessidade de reexecutar a Tarefa 3.2-C: Definir Probabilidades e informar o prazo e as orientações para aprimoramento das informações.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 3.2-E: Validar Avaliações de Probabilidades.

O Gestor de Riscos analisa as informações obtidas na tarefa anterior (3.2-D). Caso estejam de acordo, o Gestor de Riscos deve registrar a aprovação e encerra-se, dessa forma, a Atividade 3.2 – Avaliar Probabilidades. Caso contrário, o Gestor de Riscos deve notificar o Responsável Pela Unidade da Organização da necessidade de reexecutar uma ou mais das tarefas anteriores e informar o prazo para conclusão das tarefas, bem como as orientações para aprimoramento das informações. Nesse caso devem ser realizadas novamente as Tarefas 3.2-C: Definir Probabilidades e 3.2-D: Avaliar Probabilidades até que o Gestor de Riscos aprove as informações e registre o fato.

Responsável: Gestor de Riscos.

Condição para início:

- Mapa de Riscos atualizado.

Informações necessárias:

- Mapa de Riscos.
- Informações estatísticas sobre incidentes.
- Informações históricas de incidentes na organização.

Condição para ser finalizada:

- probabilidades dos riscos identificadas e estimadas.

Informações produzidas:

- Mapa de Riscos atualizado com as probabilidades de cada risco descritas e estimadas.

***Template* e exemplo da Atividade 3.2 – Avaliar Probabilidades.**

A **Figura 26** mostra o Mapa de Riscos com as informações relativas aos ativos, às respectivas ameaças e aos impactos, além de descrições e o total estimado (obtido na atividade anterior). Para cada risco (ativo e ameaça) é mostrada a probabilidade estimada.

A **Figura 27** apresenta um exemplo.

MAPA DE RISCOS						
Ativos		**Ameaças**		**Impactos**		**Probabilidades**
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Total Impacto (Imp)**	**Probabilidade de ocorrência (Prob)**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	Descrição Consequência 1	Imp 1	Prob 1
		Tipo Ameaça 2	Descrição Ameaça 2	Descrição Consequência 2	Imp 2	Prob 2
		...	...	...	...	...
...	...	...	...	...	...	...
...	...	...	...	...	...	...
...	...	...	...	...	...	...

Figura 26: *Template* do Mapa de Riscos – ativos, ameaças, impactos e probabilidades

MAPA DE RISCOS						
Ativos		**Ameaças**		**Impactos**		**Probabilidades**
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Total Impacto (Imp)**	**Probabilidade de ocorrência (Prob)**
A01	Processo avaliação RDA	Comprome-timento da informação	Extravio do documento sigiloso RDA-YZ.doc	Informações sigilosas de clientes divulgadas. Risco de processos. Atrasos.	MA	A
		Ações não autorizadas	Acesso de não autorizados no ambiente físico RdaR	Danos aos 2 PCs do ambiente.	M	B
		Falhas técnicas	Sistema de apoio RDA-AB pouco confiável	Interrupção do processo RDA-AB. Atrasos.	A	A
...	...	...	...	...	...	...

Figura 27: Exemplo de Mapa de Riscos – ativos, ameaças, impactos e probabilidades

6.5.4 – Atividade 3.3 – Estimar Nível de Risco

Esta atividade consolida as estimativas de impacto (**Atividade 3.1**) e as estimativas de probabilidade (**Atividade 3.2**).

O objetivo é obter para cada risco um nível (valor numérico) e uma classe que considerem conjuntamente os impactos e as probabilidades e obter, assim, o nível de gravidade dos riscos.

A atividade consolida os níveis e classes dos riscos de cada unidade da organização separadamente no escopo do **Projeto de GRSIC,** e, portanto, pode ser realizada para cada unidade assim que as estimativas de impacto e de probabilidade tenham sido

finalizadas. Permite-se assim que cada unidade visualize logo que possível os seus riscos. Os riscos consolidados de toda a organização (considerando todas as unidades no escopo do **Projeto de GRSIC**) são gerados quando as estimativas de risco de cada uma das unidades estiverem concluídas.

Para uma dada ameaça a um ativo o nível de risco e a classe são calculados pela aplicação da **Tabela 7**. Como já explicado anteriormente (**Processo 1 – Estabelecer Contexto**), a linha superior mostra a classificação de probabilidade e a coluna à esquerda mostra a classificação de impacto. Os valores interiores representam os níveis de risco estimados em cada situação e as letras e cores internas definem diferentes classes para o tratamento de riscos.

	Probabilidade	Muito Baixa	Baixa	Moderada	Alta	Muito alta
Impacto	Muito baixo	1 (MB)	2 (MB)	3 (B)	4 (B)	5 (M)
	Baixo	2 (MB)	3 (B)	4 (B)	5 (M)	6 (A)
	Moderado	3 (B)	4 (B)	5 (M)	6 (A)	7 (A)
	Alto	4 (B)	5 (M)	6 (A)	7 (A)	8 (MA)
	Muito alto	5 (M)	6 (A)	7 (A)	8 (MA)	9 (MA)

Tabela 7: Tabela classificação de riscos – classes e níveis de risco por classes de impacto e de probabilidade

As seguintes classes de risco e níveis são estabelecidos na tabela:

- **Risco Muito Baixo (MB):** nível de risco entre 1 e 2;
- **Risco Baixo (B):** nível de risco entre 3 e 4;
- **Risco Moderado (M):** nível de risco igual a 5;
- **Risco Alto (A):** nível de risco entre 6 e 7;
- **Risco Muito Alto (MA):** nível de risco entre 8 e 9.

O resultado desta atividade é um **Mapa de Riscos**, com cada risco identificando: ativo, ameaça ao ativo, estimativa de impacto, justificativa para a estimativa de impacto, estimativa de probabilidade, nível de risco (de 1 a 9) e classe de cada risco (MB: Muito Baixo; B: Baixo; M: Moderado; A: Alto; MA: Muito Alto).

A **Figura 28** mostra o fluxo de tarefas da atividade.

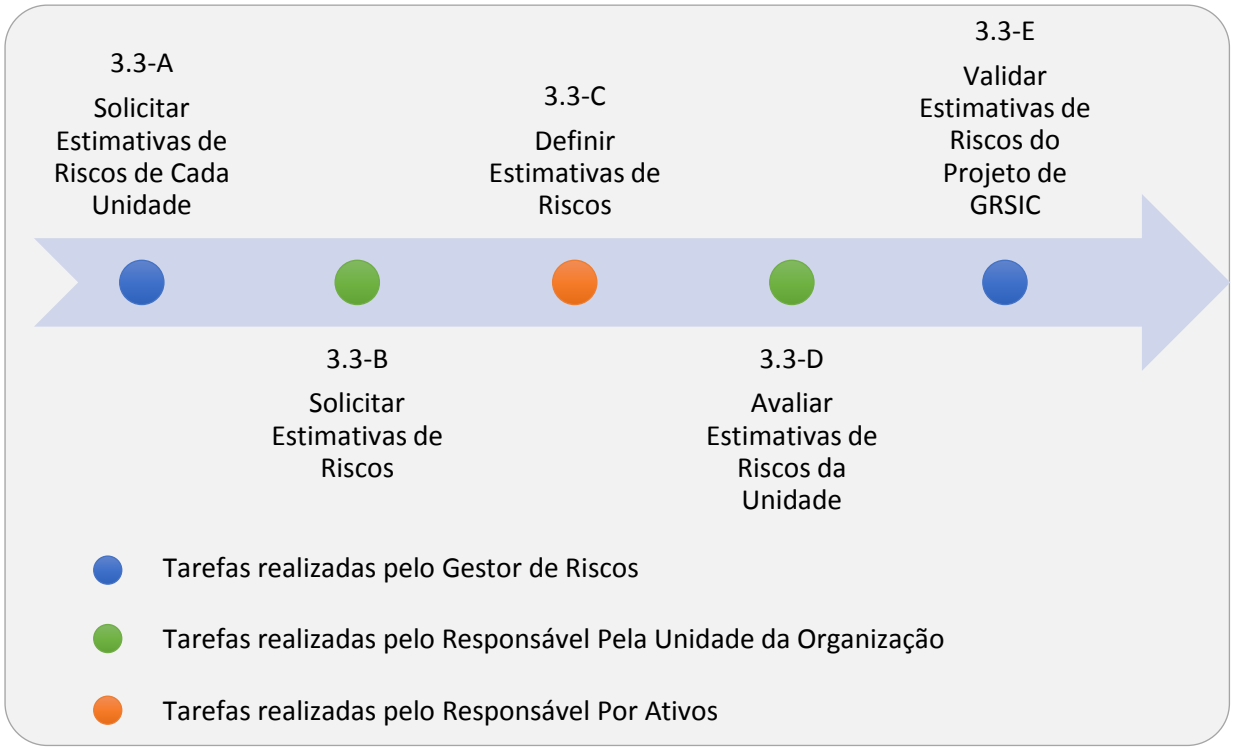

Figura 28: Fluxo de tarefas da Atividade 3.3 – Estimar Nível de Risco

TAREFAS DA ATIVIDADE 3.3 – Estimar Nível de Risco

Tarefa 3.3-A: Solicitar Estimativas de Riscos de Cada Unidade.

O Gestor de Riscos notifica aos Responsáveis Pelas Unidades da Organização para realização da Tarefa 3.3-B: Solicitar Avaliação das Estimativas de Riscos da Unidade e informa o prazo para realização da tarefa.

Responsável: Gestor de Riscos.

Tarefa 3.3-B: Solicitar Estimativas de Riscos.

O Responsável Pela Unidade da Organização notifica os Responsáveis Por Ativos para realização da Tarefa 3.3-C: Definir Estimativas de Riscos da Unidade e informa o prazo para realização da tarefa.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 3.3-C: Definir Estimativas de Riscos.

Os Responsáveis pelas Unidades devem acompanhar e apoiar os Responsáveis Por Ativos na realização desta atividade.

Os Responsáveis por Ativos avaliam as estimativas de riscos da unidade no Mapa de Riscos. Posteriormente, os Responsáveis por Ativos devem notificar o Responsável Pela Unidade da Organização das informações disponíveis para realização da Tarefa 3.3-D: Avaliar Estimativas de Riscos da Unidade.

Responsável: Responsável por Ativos. O Responsável pela Unidade pode apoiar.

Tarefa 3.3-D: Avaliar Estimativas de Riscos da Unidade.

O Responsável Pela Unidade da Organização analisa as informações das estimativas de riscos no Mapa de Riscos geradas na 3.3-C: Definir Estimativas de Riscos. Caso estejam de acordo, o Responsável Pela Unidade da Organização deve notificar o Gestor de Riscos das informações disponíveis para realização da Tarefa 3.3-E: Validar Estimativas de Riscos da Organização.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 3.3-E: Validar as Estimativas de Riscos do Projeto de GRSIC.

O Gestor de Riscos analisa as estimativas de riscos de cada unidade da organização no Mapa de Riscos. Caso estejam de acordo, o Gestor de Riscos deve registrar a aprovação e encerra-se, dessa forma, a Atividade 3.3 – Estimar Nível de Risco. Caso contrário, o Gestor de Riscos deve notificar o Responsável Pela Unidade da Organização da necessidade de reexecutar uma ou mais das tarefas anteriores e informar o prazo para conclusão das tarefas, bem como as orientações para aprimoramento das informações. Nesse caso, devem ser realizadas novamente as Tarefas 3.3-B a 3.3-D até que o Gestor de Riscos aprove as informações e registre este fato.

Responsável: Gestor de Riscos.

Condição para início:

- Mapa de Riscos atualizado.

Informações necessárias:

- Mapa de Riscos atualizado.

Condição para ser finalizada:

- nível de riscos estimado.

Informações produzidas:

- Mapa de Riscos atualizado com as estimativas do nível de cada risco para cada unidade separadamente.

***Template* e exemplo da Atividade 3.3 – Estimar Nível de Risco.**

A **Figura 29** mostra o Mapa de Riscos com as informações relativas aos ativos, às respectivas ameaças e aos impactos, além de descrições e o total estimado, assim como as probabilidades de ocorrência (estimadas na atividade anterior). Para cada risco (ativo e ameaça) é mostrado o nível de risco estimado a partir dos impactos e das probabilidades. A **Figura 30** apresenta um exemplo.

MAPA DE RISCOS							
Ativos		**Ameaças**		**Impactos**		**Probabilidades**	**Riscos**
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Total Impacto (Imp)**	**Probabilidade de ocorrência (Prob)**	**Risco -Rsc (Tabela)**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	Descrição Consequência 1	Imp 1	Prob 1	Rsc 1
		Tipo Ameaça 2	Descrição Ameaça 2	Descrição Consequência 2	Imp 2	Prob 2	Rsc 2
		...	**...**	**...**	**...**	**...**	**...**
A02	Descrição A02	Tipo Ameaça 3	Descrição Ameaça 3	Descrição Consequência 3	Imp 3	Prob 3	Rsc 3
...	**...**	**...**	**...**	**...**	**...**	**...**	**...**
...	**...**	**...**	**...**	**...**	**...**	**...**	**...**

Figura 29: *Template* do Mapa de Riscos – ativos, ameaças, impactos, probabilidades e riscos

MAPA DE RISCOS								
Ativos		**Ameaças**		**Impactos**		**Probabili-dades**	**Riscos**
ID	**Descrição**	**Tipo**	**Descrição**	**Descrição**	**Total Impacto (Imp)**	**Probabilidade de ocorrência (Prob)**	**Risco -Rsc (Tabela)**
A01	Processo avaliação RDA	Compro-meti-mento da informa-ção	Extravio do documen-to sigiloso RDA-YZ.doc	Informações sigilosas de clientes divulgadas. Risco de processos. Atrasos.	MA	A	8 (MA)
		Ações não autoriza-das	Acesso de não autoriza-dos no ambiente físico RdaR	Danos aos 2 PCs do ambiente.	M	B	4 (B)
		Falhas técnicas	Sistema de apoio RDA-AB pouco confiável	Interrupção do processo RDA-AB. Atrasos.	A	A	7 (A)

Figura 30: Exemplo de Mapa de Riscos – ativos, ameaças, impactos, probabilidades e riscos

6.6 – Processo 4 – Avaliar Riscos

6.6.1 – Descrição do Processo

Neste ponto do processo de gestão de riscos, há uma visão mais clara de quais ameaças existem para os ativos no projeto da gestão de riscos e o quanto estes ativos estão protegidos por meio de controles. Além disso, neste ponto já foi estimado o nível dos riscos resultantes de impactos e probabilidades apuradas. As estimativas foram feitas separadamente para cada unidade da organização (no escopo do **Projeto de GRSIC**) no processo anterior. Este processo, ao contrário, trata os riscos de todo o projeto conjuntamente. Isto é, trata-se de um ponto de sincronismo das atividades realizadas

nas unidades. O Mapa de Riscos e as respectivas estimativas de nível são utilizados neste processo para direcionar decisões sobre o tratamento de riscos.

A **Figura 31** mostra o fluxo de atividades processo.

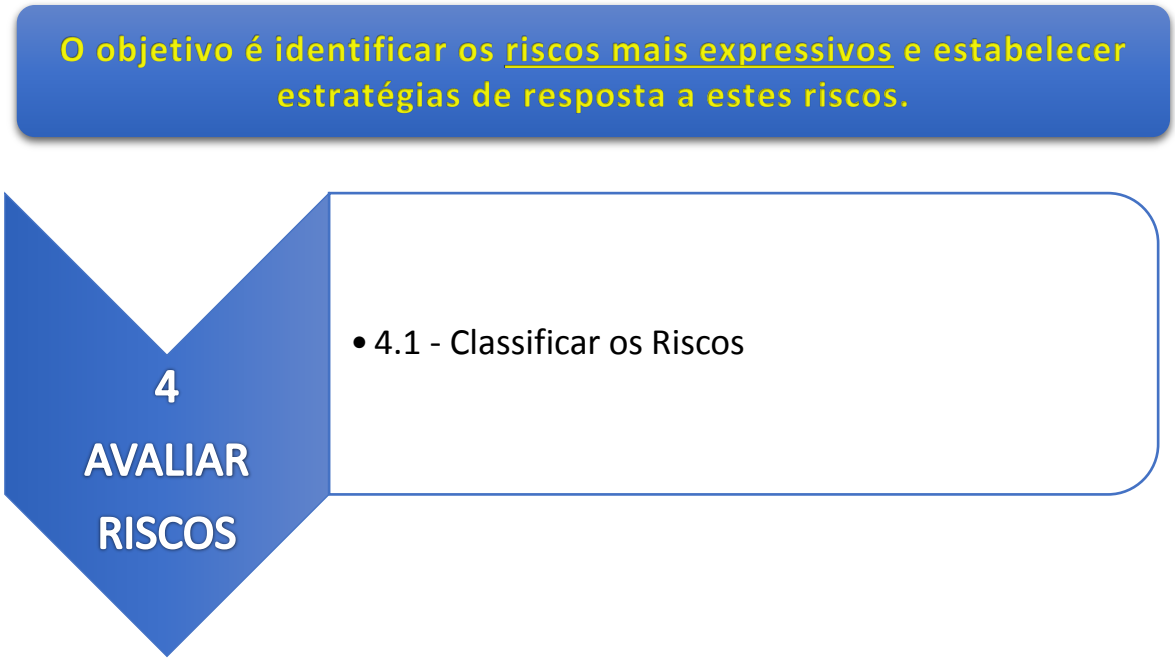

Figura 31: Fluxo de tarefas do Processo 4 – Avaliar Riscos

6.6.2 – Atividade 4.1 – Classificar os Riscos

Nesta atividade é feita a classificação de riscos e é criada uma lista ordenada dos riscos envolvendo todas as unidades da organização no escopo do **Projeto de GRSIC**.

Isso permite distinguir os riscos mais relevantes do projeto como um todo, além de ser uma base para as decisões sobre quais riscos devem ser tratados prioritariamente.

Note que na atividade anterior (Estimar nível de risco) os riscos estão separados por unidades, enquanto que nesta atividade os riscos são tratados de forma conjunta.

A **Figura 32** mostra o fluxo de tarefas da atividade.

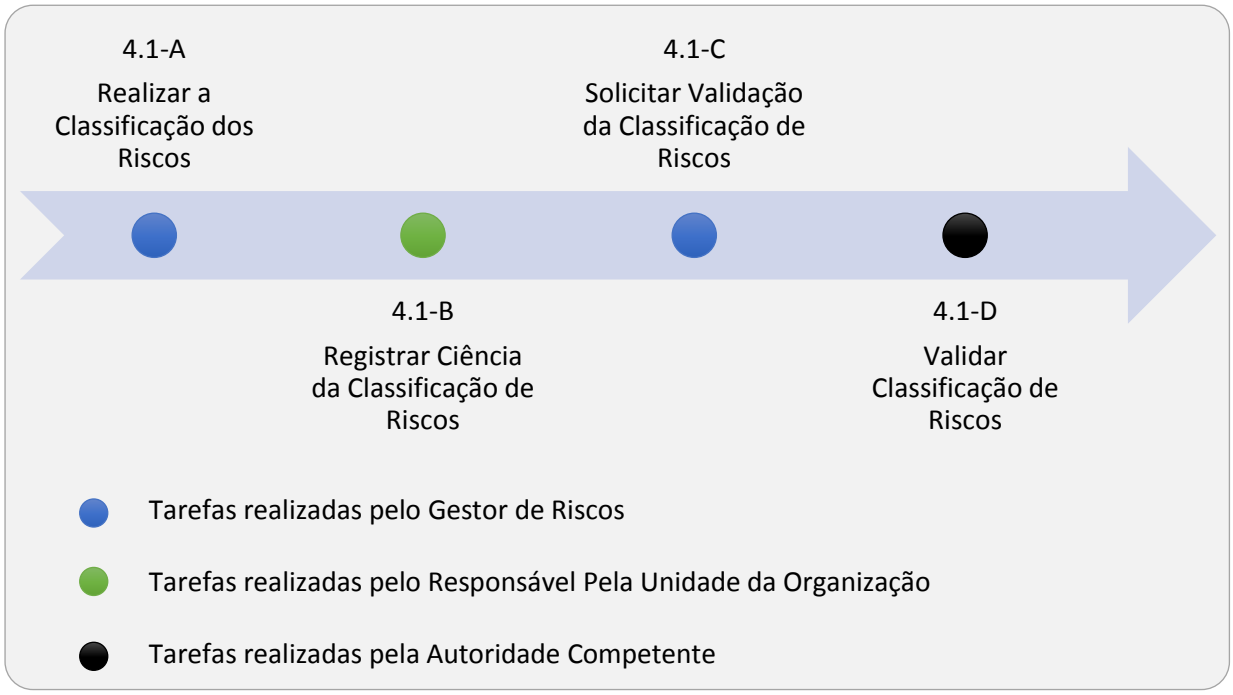

Figura 32: Fluxo de tarefas da Atividade 4.1 – Classificar os Riscos

TAREFAS DA ATIVIDADE 4.1 – Classificar os Riscos

Tarefa 4.1-A: Realizar a Classificação dos Riscos.

O Gestor de Riscos deve classificar os riscos no Mapa de Riscos. Posteriormente, o Gestor de Riscos deve notificar os Responsáveis Pelas Unidades da Organização para realização da Tarefa 4.1-B: Registrar Ciência da Classificação de Riscos e informar o prazo para realização da tarefa.

Responsável: Gestor de Riscos.

Tarefa 4.1-B: Registrar Ciência da Classificação de Riscos.

O Responsável Pela Unidade da Organização deve registrar a ciência da classificação de riscos no Mapa de Riscos. Posteriormente, o Responsável Pela Unidade da Organização deve notificar o Gestor de Riscos para realização da Tarefa 4.1-C: Solicitar Validação da Classificação de Riscos.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 4.1-C: Solicitar Validação da Classificação de Riscos.

O Gestor de Riscos notifica a Autoridade Competente para realização da Tarefa 4.1-D: Validar Classificação de Riscos.

Responsável: Gestor de Riscos.

Tarefa 4.1-D: Validar Classificação de Riscos.

A Autoridade competente com apoio do Gestor de Riscos e também dos Responsáveis Pelas Unidades da Organização deve decidir sobre a necessidade ou não de se levantar mais informações antes de iniciar o tratamento de riscos. Caso seja necessário, é possível a realização de quaisquer dos processos anteriores (Processos – 1, 2, 3 ou 4). Caso contrário, a Autoridade Competente deve registrar a aprovação e encerra-se, dessa forma, o Processo 4 – Avaliar Riscos.

Responsável: Autoridade Competente com apoio do Gestor de Riscos e dos Responsáveis Pelas Unidades da Organização.

Condição para início:

- atividades do Processo 3 – Estimar Riscos realizadas;
- impactos e probabilidades identificadas, descritas e estimadas.

Informações necessárias:

- Mapa de Riscos atualizado onde cada item do mapa define: ativo, ameaça ao ativo, estimativa de impacto, justificativa para a estimativa de impacto, estimativa de probabilidade, e nível de risco.

Condição para ser finalizada:

- riscos classificados e ordenados por nível de risco.

Informações produzidas:

- estimativas do nível de cada risco associados aos itens do Mapa de Riscos. Cada item do mapa define: ativo, ameaça ao ativo, estimativa de impacto, justificativa para a estimativa de impacto, estimativa de probabilidade, nível de risco, e classe de nível de risco (MB: Muito Baixo; B: Baixo; M: Moderado; A: Alto; MA: Muito Alto).

***Template* e exemplo da Atividade 4.1 – Classificar os Riscos.**

O *template* e o exemplo são semelhantes aos das **Figuras 41 e 42**. A única distinção é que o Mapa de Riscos refere-se a todas as unidades da organização no escopo do **Projeto de GRSIC** de forma conjunta.

6.7 – Processo 5 – Tratar Riscos

6.7.1 – Descrição do Processo

Neste processo todas as análises realizadas e informações obtidas são utilizadas na tomada de decisão sobre como a organização irá agir em relação aos riscos.

O tratamento de riscos envolve a tomada de decisão sobre uma ou mais opções de tratamento. Estas opções são descritas a seguir.

- **Redução de riscos.** O nível de risco deve ser reduzido pela seleção e implementação de controles de modo que o risco residual possa ser reavaliado como sendo aceitável. Em geral, controles devem fornecer uma ou mais dos seguintes tipos de proteção:
  - Correção;
  - Eliminação;
  - Prevenção;
  - Minimização de impacto;
  - Dissuasão;
  - Detecção;
  - Recuperação;
  - Monitoramento; ou
  - Conscientização.

- **Retenção (aceitação) de riscos.** Trata-se da decisão de reter o risco sem maiores ações. Se o nível dos riscos satisfaz o critério de aceitação, não existe necessidade de implementar controles adicionais e o risco pode ser retido. A decisão deve ser registrada formalmente e justificada.
- **Transferência de riscos.** Trata-se de transferir o risco para outra parte externa, que pode ser feita pela contratação de um seguro, que irá apoiar em relação às consequências do risco, ou por subcontratação de serviços.
- **Evitar riscos.** Quando riscos identificados e são considerados muito altos, ou se os custos de implementação de outro tratamento de risco excedem os benefícios, a decisão deve ser feita para evitar risco por completo, pela retirada de forma planejada de atividades existentes.

Algumas diretrizes para o tratamento de riscos:

- Quando uma redução significativa de riscos pode ser obtida com custos relativamente baixos, esta opção deve ser implementada;
- As consequências e a probabilidade dos riscos devem ser minimizadas tanto quanto possível, considerando níveis tratáveis de custo;
- Deve-se considerar de forma especial eventos raros, cujas consequências tenham impacto muito grave;
- As quatro opções para o tratamento de risco não são mutuamente exclusivas. Em alguns casos, a organização pode combinar mais de uma opção;
- Alguns tratamentos de riscos podem atingir mais que um risco.
- A escolha do tratamento de riscos deve levar em conta os resultados da estimativa de impacto, analisando de forma separada cada atributo de segurança (confidencialidade, integridade, disponibilidade). Deve ser priorizado a implantação de controles que tratam o atributo definido como mais crítico.

Também é importante levar em consideração o esforço e as restrições que podem envolver o tratamento do risco. Para tanto, este processo foi dividido em três atividades.

A **Figura 33** mostra o fluxo de atividades do processo.

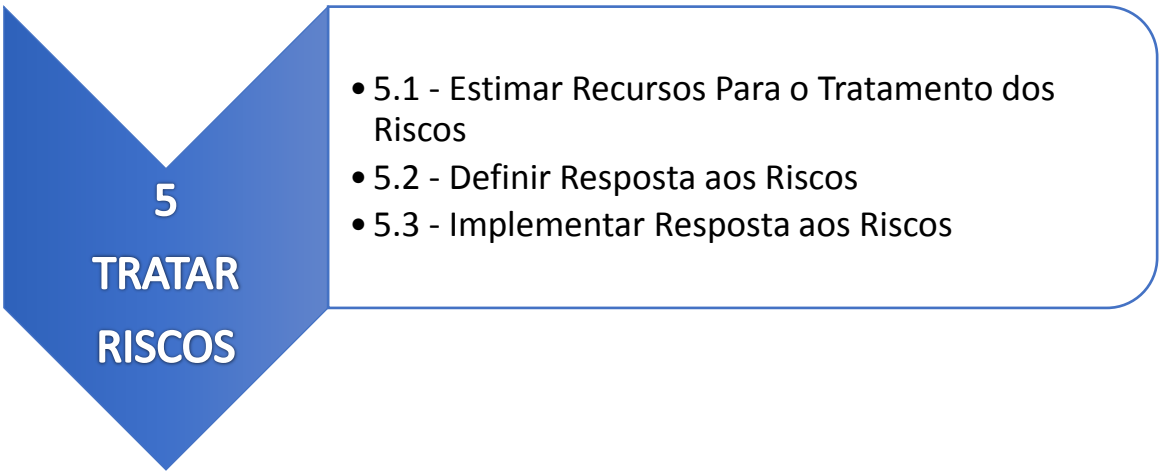

Figura 33: Processo 5 – Tratar Riscos

6.7.2 – Atividade 5.1 - Estimar Recursos Para o Tratamento dos Riscos

Depois de estabelecido o Mapa de Riscos, assim como definidas as classes risco (Muito Baixo; Baixo; Moderado; Alto; Muito Alto), podem ser consideradas restrições que potencialmente afetam as decisões sobre o tratamento de riscos (custos, prazos, etc.).

Nesse sentido, os riscos podem passar por uma análise preliminar a fim de estimar a ordem de grandeza de custos, esforço e prazo e se existem restrições para o tratamento do risco.

Caso as restrições de custo, esforço e prazo não sejam significativas para a tomada de decisão, esta atividade pode ser suprimida.

Para cada risco do Mapa de Riscos, deve ser recuperada as informações levantadas nas atividades anteriores como:

- Os controles aplicáveis para o risco;
- Para cada controle, a situação da implementação do controle:

a) Não implementado;
b) Implementado;
c) Não se aplica ou desnecessário.

Deve ser feita uma estimativa do custo, esforço e de prazo para implementar os controles identificado nas situações “Não implementado”. Esses controles, se implementados, podem reduzir a exposição do ativo ao risco.

Importante notar que a análise descrita acima (identificar controles ainda não implementados) abrange diferentes alternativas de tratamento, associadas aos diferentes controles. Tipicamente controles agem **Reduzindo Riscos** ou **Transferindo Riscos**. É importante registrar o custo, esforço e prazo estimados para cada alternativa de controle que possa ser utilizada para um risco específico, seja ele para reduzir o risco ou para transferir o risco.

O resultado desta atividade é a associação de **uma Estimativa de Custo, Estimativa de Esforço, Estimativa de Prazo e de Restrições** para cada risco presente no Mapa de

Riscos e para cada alternativa de controle.

Desse modo, a saída desta atividade é o Mapa de Riscos, no qual cada linha apresenta as informações:

- Ativo.
- Ameaça ao ativo.
- Estimativa de impacto.
- Justificativa para a estimativa de impacto.
- Estimativa de probabilidade.
- Nível de risco.

Para cada alternativa de controle:

- Estimativa de custo para tratamento.
- Estimativa de esforço.
- Estimativa de prazo para tratamento.

Caso sejam estimados recursos para as alternativas: Transferir o Risco ou Evitar o Risco, essa informação também e fornecida como saída desta atividade.

A **Figura 34** mostra o fluxo de tarefas da atividade.

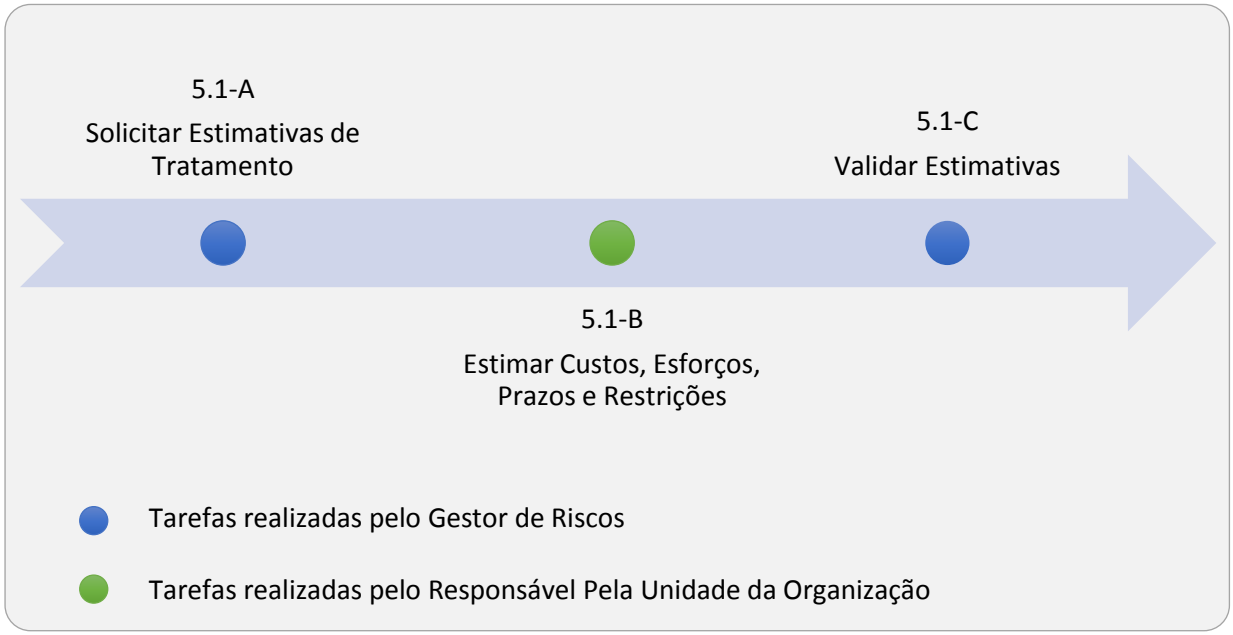

Figura 34: Fluxo de tarefas da Atividade 5.1 – Estimar Recursos Para o Tratamento dos Riscos

TAREFAS DA ATIVIDADE 5.1 – Estimar Recursos Para o Tratamento dos Riscos

Tarefa 5.1-A: Solicitar Estimativas de Tratamento.

O Gestor de Riscos notifica os Responsáveis Pelas Unidades da Organização para realização da Tarefa 5.1-B: Estimar Custos, Esforços, Prazos e Restrições e informa o prazo para realização da tarefa.

Responsável: Gestor de Riscos.

Tarefa 5.1-B: Estimar Custos, Esforços, Prazos e Restrições.

O Responsável Pela Unidade da Organização deve, com apoio dos Responsáveis Por Ativos e do próprio Gestor de Riscos, estimar, no Mapa de Riscos, os custos de implementação dos controles para tratar cada risco, o quanto de esforço é necessário para implementar cada controle definido anteriormente, bem como identificar se existe alguma restrição que impacte na escolha do tratamento do risco. Em especial, deve ser avaliada a disponibilidade de recursos humanos para realizar os tratamentos de riscos analisados. Posteriormente, o Responsável pela Unidade da Organização deve notificar o Gestor de Riscos das informações disponíveis para realização da Tarefa 5.1-C: Validar Estimativas.

Responsável: Responsável pela Unidade da Organização. Os Responsáveis Por Ativos e o Gestor de Riscos devem apoiar.

Tarefa 5.1-C: Validar Estimativas.

O Gestor de Riscos deve avaliar as estimativas levantadas pelos Responsáveis Pelas Unidades da Organização no Mapa de Riscos. Caso estejam de acordo, o Gestor de Riscos deve registrar a aprovação e encerra-se, dessa forma, a Atividade 5.1 – Estimar Recursos Para o Tratamento dos Riscos. Caso contrário, o Gestor de Riscos deve notificar o Responsável pela Unidade da Organização da necessidade de reexecutar a Tarefa 5.1-B: Estimar Custos, Esforços, Prazos e Restrições e informar o prazo para conclusão da tarefa, bem como as orientações para aprimoramento das informações. Pode ser realizada novamente a Tarefa 5.1-B até que o Gestor de Riscos aprove as estimativas e registre o fato.

Responsável: Gestor de Riscos.

Condição para início:

- é necessário o Mapa de Riscos atualizados com os controles que podem ser implementados.

Informações necessárias:

- informações históricas sobre custo, esforço e tempo para implementação de controles;
- avaliações de especialistas ou de representantes de setores / proprietários de ativos.

Condição para ser finalizada:

- estimativas relacionadas a todos os controles estabelecidas e restrições identificadas.

Informações produzidas:

- Mapa de Riscos atualizado com as estimativas para cada controle, restrições identificadas.

***Template* e exemplo da Atividade 5.1 – Estimar Recursos.**

A **Figura 35** mostra o Mapa de Riscos com as informações relativas aos ativos, às respectivas ameaças e aos riscos ordenados e classificados. Para cada risco são apresentados os controles aplicáveis. Cada controle é descrito e é fornecida a sua situação de implementação (não implementado, implementado ou não se aplica). A cada controle são associadas estimativas para a implementação (custo, esforço, prazo) e são apresentadas as restrições.

A **Figura 36** apresenta um exemplo.

MAPA DE RISCOS											
Ativos		**Ameaças**		**Riscos Ordenados e Classificados**		**Controles**		**Estimativas / Restrições**			
ID	**Descrição**	**Tipo**	**Descrição**	**Nível Risco -Rsco**	**Classe - CLRsc (MB,B,M,A,MA)**	**Descrição**	**Situação / Justificativa**	**Custo (Cst)**	**Esforço (Esf)**	**Prazo (Prz)**	**Restrições (Rst)**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	Rsc 1	CL Rsc 1	Descrição Controle 1	Situação / Justificativa Controle 1	Cst 1	Esf 1	Prz 1	Rst 1

						Descrição Controle 2	Situação / Justificativa Controle 2	Cst 2	Esf 2	Prz 2	Rst 2
						...	...	...	...	...	...
						Descrição Controle 1	Situação / Justificativa Controle 1	Cst 1	Esf 1	Prz 1	Rst 1
		Tipo Ameaça 2	Descrição Ameaça 2	Rsc 2	CL Rsc 2	Descrição Controle 2	Situação / Justificativa Controle 2	Cst 2	Esf 2	Prz 2	Rst 2
						...	...	...	...	...	...
...	...	...	...	...	...	...	...			...	

Figura 35: *Template* do Mapa de Riscos – ativos, ameaças, riscos ordenados, controles estimativas para tratamento

MAPA DE RISCOS											
Ativos		**Ameaças**		**Riscos Ordenados e Classificados**		**Controles**		**Estimativas / Restrições**			
ID	**Descrição**	**Tipo**	**Descrição**	**Nível Risco**	**Classe (MB, B, M, A, MA)**	**Descrição**	**Situação / Justificativa**	**Custo (Cst)**	**Esforço (Esf) – Baixo Médio. Alto.**	**Prazo (Prz)**	**Restrições (Rst)**
A01	Processo avaliação RDA	Compro-metimento da informa-ção	Extravio do documen-to sigiloso RDA-YZ.doc	8	MA	Conscienti-zação "mesa limpa"	Não Implementado	10.000 R$	Médio	120 Dias	x
						Fechadura mecânica	Totalmente Implementa	x	x	x	x

					do				
				Câmara monitora-mento.	Parcialmen-te Implemen-tado – câmera VGA, pouco nítida img.	1.000 R$	Baixo	20 Dias	x
Falhas técnicas	Sistema de apoio RDA-AB pouco confiável	7	A	Realizar teste de software	Parcialmen-te Implementa do – teste não sistemático.	15.000 R$	Alto	150 Dias	Equipe interna
				Realizar teste de segurança	Totalmente Implementa do	x	x	x	x
Ações não autoriza-das	Acesso de não autoriza-dos no ambiente físico RdaR	4	B	Política e procedi-mentos de controle acesso	Parcialmen-te Implementa do – procedimen-tos informais	3.000 R$	Médio	45 Dias	x
				Fechadura mecânica	Totalmente Implemen-tado	x	x	x	x
				Câmara monitora-mento.	Totalmente Implemen-tado	x	x	x	x

Figura 36: Exemplo de Mapa de Riscos – ativos, ameaças, riscos ordenados, controles e estimativas para tratamento

6.7.3 – Atividade 5.2 – Definir Resposta aos Riscos

Nesta atividade cada risco do Mapa de Riscos é analisado para determinar a resposta adequada (resposta ao risco – RR). Como já destacado, devem ser tratados prioritariamente os riscos maiores segundo o estabelecido nos critérios de avaliação de riscos e de aceitação de riscos estipulado anteriormente.

Esta atividade trata de avaliar cada risco relevante do Mapa de Riscos e decidir sobre o tratamento.

Depois de finalizada a **Atividade 5.1 – Estimar Recursos Para o Tratamento dos Riscos**, devem ser realizadas decisões sobre como tratá-los. Essa decisão deve considerar os riscos priorizados por níveis (Muito Baixo; Baixo; Moderado; Alto; Muito Alto) as opções de tratamento (Reduzir os Riscos; Reter os Riscos; Transferir os Riscos; ou Evitar os Riscos) e as estimativas feitas para a implementação dos controles (custo, esforço, tempo e restrições).

A **Figura 37** mostra o fluxo de tarefas da atividades.

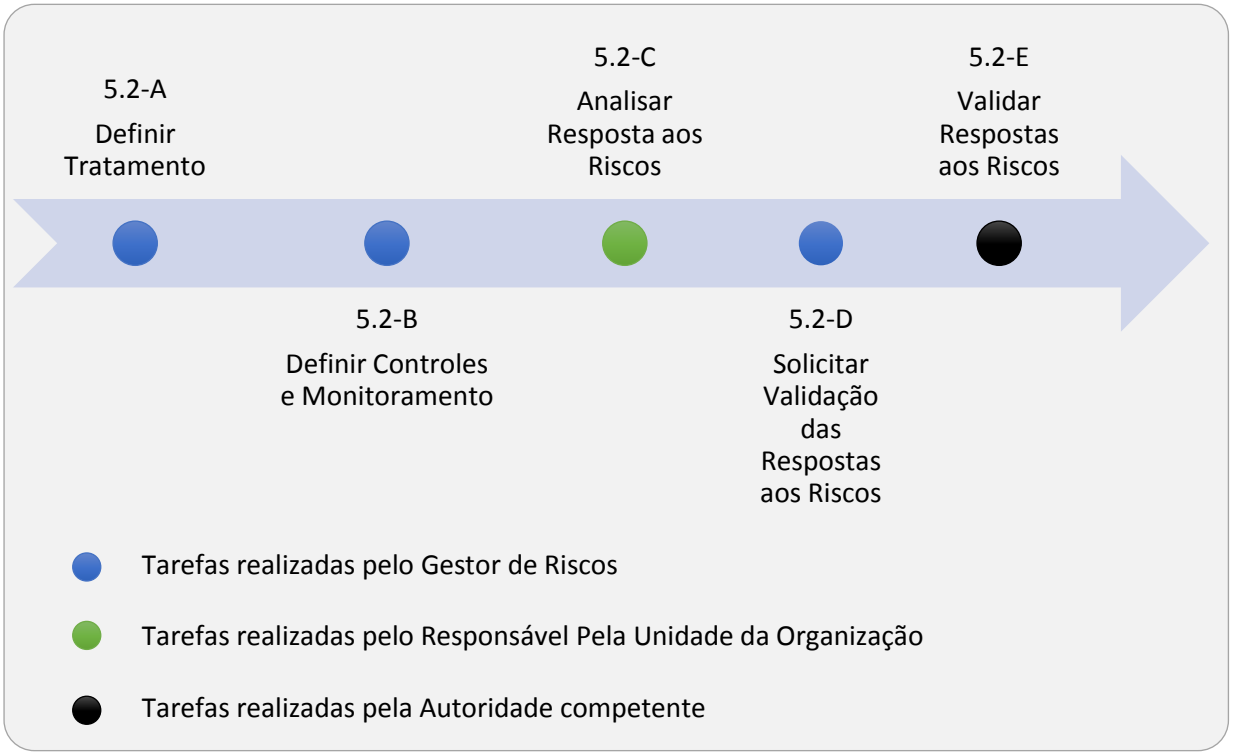

Figura 37: Fluxo de tarefas da Atividade 5.2 – Definir Resposta aos Riscos

TAREFAS DA ATIVIDADE 5.2 – Definir Resposta aos Riscos

Tarefa 5.2-A: Definir Tratamento.

O Gestor de Riscos deve analisar cada risco no Mapa de Riscos e identificar o nível do risco e o tratamento recomendado para este nível, que foi cadastrado no Processo 1 – Estabelecer Contexto. Uma opção de tratamento (Reduzir os Riscos; Reter os Riscos; Transferir os Riscos; ou

Evitar os Riscos) deve ser selecionada e uma justificativa deve ser fornecida. A opção por Reduzir os Riscos é vista como a solução mais comum a ser adotada na maior parte das situações.

Responsável: Gestor de Riscos.

Tarefa 5.2-B: Definir Controles e Monitoramento.

Esta tarefa é realizada apenas quando for definido na Tarefa 5.1–A o tipo Reduzir Riscos.

O Gestor de Riscos, baseado nas informações produzidas na Atividade 5.1 – Estimar Recursos para Tratamento de Riscos, deve analisar o estado de implementação dos controles (Não implementado; Implementado; Não se aplica), bem como as estimativas para a implementação dos controles (custo, esforço, tempo e restrições). Ele também deve definir, para cada risco, um ou mais controles a serem implementados no Mapa de Riscos, bem como sua respectiva periodicidade de monitoramento. Posteriormente, o Gestor de Riscos deve notificar os Responsáveis Pelas Unidades da Organização das informações disponíveis no Mapa de Riscos para realização da Tarefa 5.2-C: Analisar Resposta aos Riscos.

Responsável: Gestor de Riscos.

Tarefa 5.2-C: Analisar Resposta aos Riscos.

Os Responsáveis Pelas Unidades da Organização, com apoio dos Responsáveis Por Ativos, devem analisar, no Mapa de Riscos, as respostas aos riscos definidas no escopo da unidade. Caso estejam de acordo, os Responsáveis Pelas Unidades da Organização devem notificar o Gestor de Riscos para realização da Tarefa 5.2-D: Solicitar Validação das Respostas aos Riscos. Caso contrário, os Responsáveis Pelas Unidades da Organização devem notificar o Gestor de Riscos para realizar novamente as Tarefas 5.2-A e 5.2-B e fornecer uma descrição das questões identificadas e sugestões de melhorias.

Responsável: Responsável pela Unidade da Organização. Os Responsáveis Por Ativos podem apoiar.

Tarefa 5.2-D: Solicitar Validação das Respostas aos Riscos.

O Gestor de Riscos deve notificar a Autoridade Competente das informações disponíveis para realização da Tarefa 5.2-G: Validar Respostas aos Riscos no Mapa de Riscos.

Responsável: Gestor de Riscos.

Tarefa 5.2-E: Validar Respostas aos Riscos.

A Autoridade Competente, com respaldo da análise técnica feita pelo Gestor de Riscos, é a

responsável por decidir sobre a adequação das opções definidas para tratar os riscos.

Caso alguma opção de tratamento não esteja de acordo com a visão estratégica da organização, pode ser necessário revisar ou refinar decisões anteriores.

Nesses casos, o Gestor de Riscos deve ser informado da necessidade de revisar decisões e devem ser fornecidas descrições das questões estratégicas identificadas pela organização para que as Tarefas 5.2-A a 5.2-E sejam realizadas novamente. Caso estejam de acordo, a Autoridade Competente deve registrar a aprovação das Respostas aos Riscos no Mapa de Riscos e encerra-se, dessa forma, a Atividade 5.2 – Definir Resposta aos Riscos.

Responsável: Autoridade Competente.

Condição para início:

- níveis de risco e respectivos tratamentos recomendáveis estabelecidos no **Processo 1 – Estabelecer Contexto**;
- recursos para tratamento de riscos estimados na Atividade 5.1 – Estimar Recursos.

Informações necessárias:

- quais são as prioridades, custo e o tempo para a implementação de cada alternativa do tratamento de risco;
- objetivos da GRSIC na organização.

Condição para ser finalizada:

- para que esta tarefa seja finalizada, é importante que todos os riscos tenham sua opção de tratamento selecionada, bem como elaborada a justificativa da escolha.

Informações produzidas:

- Mapa de Riscos atualizado com o tratamento selecionado e a justificativa da escolha e o responsável pelo tratamento;
- também é gerada uma lista com os riscos aceitos e suas justificativas.

Template e exemplo da Atividade 5.2 – Definir Resposta aos Riscos.

A **Figura 38** mostra o Mapa de Riscos com as informações relativas aos ativos, às respectivas ameaças e aos riscos ordenados e classificados. Para cada risco, são apresentados os controles aplicáveis. Cada controle é descrito e é fornecida a sua situação de implementação. Para os tratamentos a serem realizadas são associados Planos de Tratamento de Riscos (PTRs). A **Figura 39** apresenta um exemplo.

MAPA DE RISCOS									
Ativos		**Ameaças**		**Riscos Ordenados e Classificados**		**Controles**		**Tratamento de Riscos**	
ID	**Descrição**	**Tipo**	**Descrição**	**Risco -Rsc (Cnq X Prob)**	**Classe - CLRsc (MB, B, M, A, MA)**	**Descrição**	**Situação / Justificativa**	**Opção de tratamento**	**Plano de Tratamento (PTR)**
A01	Descrição A01	Tipo Ameaça 1	Descrição Ameaça 1	Rsc 1	CL Rsc 1	Descrição Controle 1	Situação / Justificativa Controle 1	Op 1	PTR 1
						Descrição Controle 2	Situação / Justificativa Controle 2	Op 2	PTR 2
						...	...	...	...
		Tipo Ameaça 2	Descrição Ameaça 2	Rsc 2	CL Rsc 2	Descrição Controle 1	Situação / Justificativa Controle 1	Op 1	PTR 3
						Descrição Controle 2	Situação / Justificativa Controle 2	Op 2	PTR 4
						...	...	...	...
		...	...	...	...	...	...	...	
...	...	...	...	...	...	...	...	...	

Figura 38: *Template* do Mapa de Riscos – ativos, ameaças, riscos, controles e informações de tratamento

MAPA DE RISCOS									
Ativos		**Ameaças**		**Riscos Ordenados e Classificados**		**Controles**		**Tratamento de Riscos**	
ID	**Descrição**	**Tipo**	**Descrição**	**Risco -Rsc (Cnq X Prob)**	**Classe-CLRsc (MB, B, M, A, MA)**	**Descrição**	**Situação / Justificativa**	**Opção de tratamento**	**Plano de Tratamento de Risco (PTR)**
A01	Processo avaliação RDA	Compro metime-nto da informa-ção	Extravio do documen-to sigiloso RDA-YZ.doc	8	MA	Conscienti-zação "mesa limpa"	Não Implementa do	1 - Obs: mais eficaz	PTR-RDA-1
						Fechadura mecânica	Implemen-tado	x	x
						Câmara monitora-mento.	Não Implementa do – câmera VGA, pouco nítida img.	2 – Obs: pouco efetiva	x
		Falhas técnicas	Sistema de apoio RDA-AB pouco confiável	7	A	Realizar teste de software	Não Implementa do – teste não sistemático.	1	PTR-RDA-1
						Realizar teste de segurança	Implemen-tado	x	x
		Ações não autori-zadas	Acesso de não autoriza-dos no ambiente físico RdaR	4	B	Política e procedime ntos de controle acesso	Não Implemen-tado – procedimen-tos informais	1	PTR-RDA-1
						Fechadura mecânica	Implemen-tado	x	x

Figura 39: Exemplo de Mapa de Riscos – ativos, ameaças, riscos, controles e informações de tratamento

6.7.4 – Atividade 5.3. Implementar Reposta aos Riscos

Nesta atividade, o Gestor de Riscos deve criar condições para que os riscos sejam tratados e os Planos de Tratamento de Riscos (PTRs) devem ser criados.

Um Plano de Tratamento de Riscos deve reunir ações voltadas ao tratamento de riscos comuns.

Um PTR pode agrupar, por exemplo, um conjunto de ações de melhoria de segurança a serem implementadas em uma unidade específica da organização.

Para cada PTR deve ser definido: escopo; unidade da organização; controles a serem implementados; descrição de ações necessárias; responsável pela execução; data de início; e data prevista para término.

O Gestor de Riscos deve alocar a execução dos PTRs aos responsáveis e acompanhar a execução (parte do **Processo 7 – Monitorar Riscos**). A **Figura 40** mostra o fluxo de tarefas da atividade.

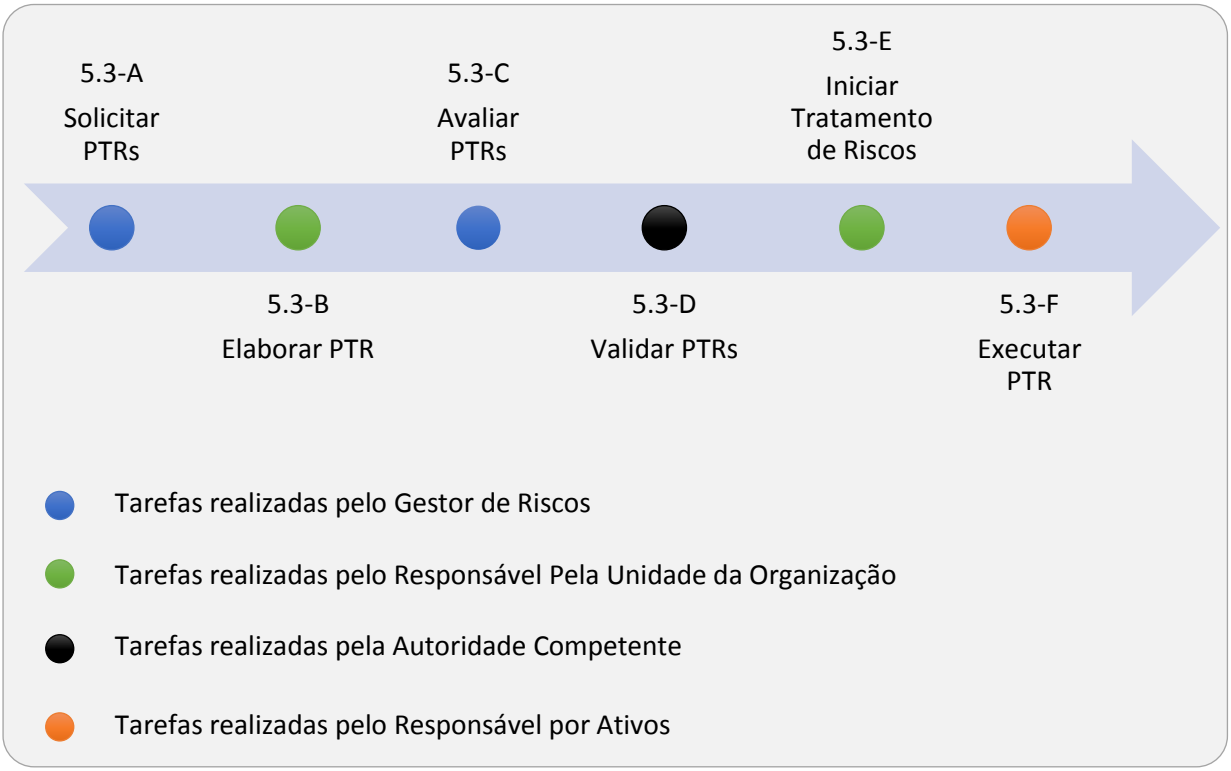

Figura 40: Fluxo de tarefas da Atividade 5.3 – Implementar Respostas aos Riscos

TAREFAS DA ATIVIDADE 5.3 – Implementar Resposta aos Riscos

Tarefa 5.3-A: Solicitar Planos de Tratamento de Riscos.

O Gestor de Riscos deve, para cada risco a ser tratado, associar um Plano de Tratamento de Riscos (PTR) que aborde o risco. Um PTR tipicamente aborda mais de um risco.

Deve ser definido e comunicado um responsável pela elaboração de cada PTR. Tipicamente, o responsável pelo PTR deve ser um Responsável Pela Unidade da Organização. Posteriormente, o Gestor de Riscos deve notificar o responsável pela elaboração de cada PTR (Responsável Pela Unidade da Organização) para realização da Tarefa 5.3-B: Elaborar Plano de Tratamento de Riscos e informar também o prazo para realização da tarefa.

Responsável: Gestor de Riscos.

Tarefa 5.3-B: Elaborar Plano de Tratamento de Riscos.

O Responsável Pela Unidade da Organização, designado para elaborar um Plano de Tratamento de Risco, deve levantar informações sobre o risco a ser tratado (ativos, ameaças, opções de tratamento, controles a serem implementados, estimativas e restrições) e detalhar as ações a serem tomadas, com suas respectivas estimativas no Plano de Tratamento de Riscos. O Responsável Pela Unidade da Organização deve também, no Plano de Tratamento de Riscos, alocar e comunicar os responsáveis por executar cada o tratamento, que são os Responsáveis por Ativos. Uma vez finalizada a tarefa, o Responsável Pela Unidade da Organização deve notificar o Gestor de Riscos das informações disponíveis para realização da Tarefa 5.3-C: Avaliar Planos de Tratamento de Riscos.

Responsável: Responsável pela Unidade da Organização. O Responsável Por Ativos pode apoiar.

Tarefa 5.3-C: Avaliar Planos de Tratamento de Riscos.

O Gestor de Riscos deve avaliar as informações constantes dos Planos de Tratamento de Riscos. Caso estejam de acordo, o Gestor de Riscos deve notificar a Autoridade Competente para realização da Tarefa 5.3-D: Validar Planos de Tratamento de Riscos. Caso contrário, o Gestor de Riscos deve notificar o Responsável Pela Unidade da Organização para realização da Tarefa 5.3-B: Elaborar Plano de Tratamento de Riscos e fornecer as informações e estabelecer o respectivo prazo para realização da tarefa.

Responsável: Gestor de Riscos.

Tarefa 5.3-D: Validar Planos de Tratamento de Riscos.

A Autoridade Competente, com respaldo da análise técnica feita pelo Gestor de Riscos, deve avaliar se os Planos de Tratamento de Riscos são adequados às necessidades da organização.

Caso estejam de acordo, a Autoridade Competente deve notificar os Responsáveis Pelas Unidades da Organização para realização da Tarefa 5.3-D: Iniciar Tratamento de Riscos.

Caso contrário, a Autoridade Competente deve notificar o Gestor de Riscos para realizar novamente a Tarefa 5.3-A: Solicitar Planos de Tratamento de Riscos e fornecer as informações necessárias para as devidas correções nos Planos de Tratamento de Riscos, bem como o prazo para realização da tarefa.

Responsável: Autoridade Competente. O Gestor de Riscos deve apoiar.

Tarefa 5.3-E: Iniciar Tratamento de Riscos.

O Responsável Pela Unidade da Organização deve notificar os Responsáveis por Ativos para realização da Tarefa 5.3-F: Executar Plano de Tratamento de Riscos.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 5.3-F: Executar Plano de Tratamento de Riscos.

Os Responsáveis por Ativos designados devem executar as ações previstas no Plano de Tratamento de Riscos e informar os Responsáveis Pelas Unidades da Organização responsáveis pelo Plano de Tratamento de Riscos do andamento e dos resultados das ações, conforme previsto no Plano de Comunicação de Riscos.

Responsável: Responsável por Ativos.

Condição para início:

- Mapa de Riscos atualizado da atividade anterior.

Informações necessárias:

- escopo;
- descrição de ações necessárias e controles a serem implementados;
- conhecimento técnico específico sobre a implementação de controles;
- responsável pela execução;
- estimativas para o tratamento de riscos.

Condição para ser finalizada:

- é necessário que a Autoridade Competente valide os Planos de Tratamento de Riscos.

Informações produzidas:

- Mapa de Riscos atualizado com os Planos de Tratamento de Riscos que serão entregues aos responsáveis, contendo as justificativas e o tempo para que o tratamento de risco seja concretizado;
- os **Processos 6 – Comunicar Riscos e 7 – Monitorar Riscos** também recebem informações inerentes a esta atividade.

***Template* e exemplo da Atividade 5.3 – Implementar Resposta aos Riscos.**

A **Figura 41** mostra um modelo de PTR – Plano de Tratamento de Riscos. Cada PTR possui um identificador e refere-se a uma unidade da organização dentro do escopo do **Projeto de GRSIC**. São identificados os responsáveis pela execução e pela elaboração do PTR**. São listados os riscos a serem tratados no escopo do PTR, identificando ativos, ameaças, controle a ser implementado, estimativas, situação e evidências.** São fornecidas datas para acompanhamento do PTR. A **Figura 42** apresenta um exemplo.

PTR – PLANO DE TRATAMENTO DE RISCOS							
Identificador:			**Unidade:**				
Responsáveis							
Responsável pela execução do PTR			**Responsável pela definição do PTR**				
Nome: Telefone: e-mail:			Nome: Telefone: e-mail:				
Riscos a Serem Tratados							
Ativo	**Ameaça**	**Controle a ser implementado**	**Estimativas/Restrições**				**Evidência (situação)**
			Cst	**Esf**	**Prz**	**Rst**	
...	...	...	...	...	...	...	...
...	...	...	...	...	...	....	...
Datas							
Data de Início:		**Data Prevista para a Finalização:**			**Data de Finalização:**		

Figura 41: *Template* do PTR - Plano de Tratamento de Riscos

PTR – PLANO DE TRATAMENTO DE RISCOS							
Identificador: PTR RDA-1			**Unidade: DMPS**				
Responsáveis							
Responsável pela execução do PTR			**Responsável pela definição do PTR**				
Nome: Carlos Henrique	Telefone: 2345678	e-mail: Carlos@apf.gov	Nome: Marco Antônio	Telefone: 8765432	e-mail: marcos@apf.gov		
Riscos a serem tratados							
Ativo	**Ameaça**	**Controle a ser Implementado**	**Estimativas/Restrições**				**Evidência (situação)**
			Cst	Esf	Prz	Rst	
Processo avaliação RDA	Extravio do documento sigiloso RDA-YZ.doc	Conscientização "mesa limpa"	10.000 R$	Médio	120 Dias	X	• Pauta do Treinamento (disponível) • Relatório de Ocorrências (disponível)
Processo avaliação RDA	Sistema de apoio RDA-AB pouco confiável	Realizar teste sistemático de software	15.000 R$	Alto	150 Dias	Equipe interna	• Relatório de teste (não executado) • OS de correções (não aberta)
Processo avaliação RDA	Acesso de não autorizados no ambiente físico RdaR	Implementar Política e procedimentos de controle acesso	3.000 R$	Médio	45 Dias	x	• Política de controle de acesso institucionalizada (publicada) • Relatório de Ocorrências (disponível)
Datas							
Data de Início: 05/06/2015		**Data Prevista para a Finalização: 19/06/2015**			**Data de Finalização: 19/06/2015**		

Figura 42: Exemplo de PTR - Plano de Tratamento de Riscos

6.8 – Processo 6 – Comunicar Riscos

6.8.1 – Descrição do Processo

Este processo trata da comunicação dos riscos entre os envolvidos no processo de GRSIC. Tem por objetivo comunicar o desenvolvimento das atividades e os resultados alcançados em todas as fases da gestão de riscos. Este processo deve ser iniciado em paralelo com o **Processo 1 – Estabelecer Contexto**.

A comunicação do risco é importante, uma vez que o tomador de decisão baseia-se nessas entradas de informações para um bom entendimento dos riscos e para decidir quais são as ações a serem tomadas.

As atividades relacionadas a este processo visam tornar a comunicação um procedimento eficaz. **Este processo se desenvolve simultaneamente com os demais processos e as atividades são executadas durante todo o processo de gestão de riscos.** A comunicação de riscos deve atender aos seguintes requisitos:

- Fornecer garantia do resultado da gestão de risco da organização.
- Coletar informações sobre o risco.
- Compartilhar os resultados da análise e avaliação de riscos e apresentar os planos de tratamento de riscos.
- Dar suporte ao processo decisório.
- Dar aos tomadores de decisão e as partes interessadas um senso de responsabilidade sobre os riscos.

A **Figura 43** mostra o fluxo de atividades do processo.

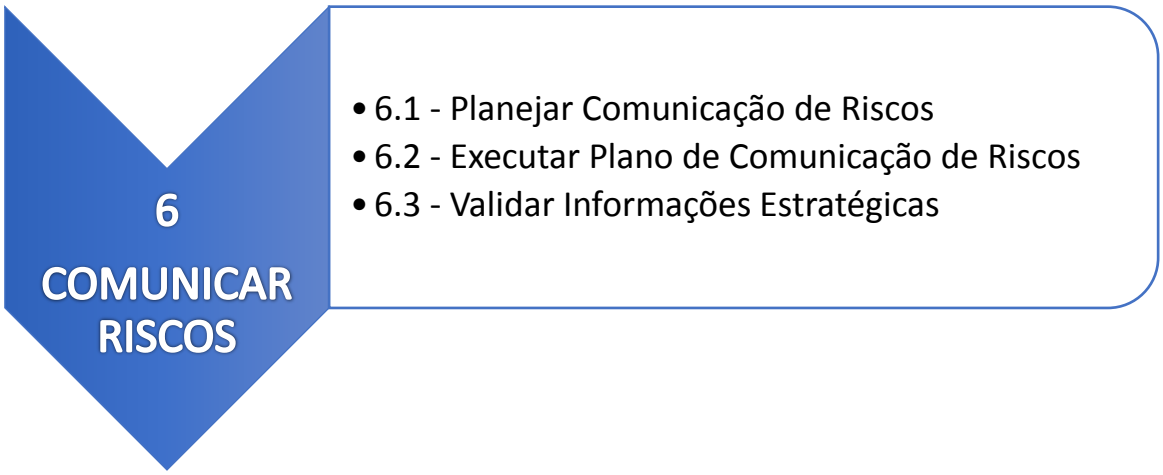

Figura 43: Fluxo de Atividades do Processo 6 – Comunicar Riscos

6.8.2 – Atividade 6.1 – Planejar Comunicação de Riscos

Nesta atividade o Gestor de Riscos deve elaborar o Plano de Comunicação da GRSIC e obter aprovação da Autoridade Competente. A **Figura 44** mostra o fluxo de tarefas da atividade.

Um Plano de Comunicação de Riscos traz o mapeamento de todos os envolvidos na análise de riscos, estabelece quais as responsabilidades de cada um e define pontos relacionados à comunicação.

Figura 44: Fluxo de tarefas da Atividade 6.1 – Planejar Comunicação de Riscos

TAREFAS DA ATIVIDADE 6.1 – Planejar Comunicação de Riscos

Tarefa 6.1-A: Elaborar Plano de Comunicação de Riscos.

O Gestor de Riscos deve elaborar o Plano de Comunicação de Riscos, definir o públicos-alvo, o que será comunicado, especificar o tempo apropriado de entrega para cada informação, os resultados desejados, a forma como a informação será entregue (veículo), quem entregará e quem receberá cada informação. Em seguida, o Gestor de Riscos deve notificar a Autoridade Competente das informações disponíveis para realização da Tarefa 6.1-B: Validar Plano de Comunicação de Riscos.

Responsável: Gestor de Riscos.

Tarefa 6.1-B: Validar Plano de Comunicação de Riscos.

A Autoridade Competente deve avaliar o Plano de Comunicação de Riscos para verificar se as informações atendem as necessidades da organização. Caso estejam de acordo, a Autoridade Competente deve registrar a aprovação do Plano de Comunicação de Riscos e encerra-se, dessa forma, a Atividade 6.1 – Planejar Comunicação de Riscos. Caso contrário, a Autoridade competente deve notificar o Gestor de Riscos da necessidade de realizar novamente a Tarefa 6.1-A e fornecer descrições das questões identificadas como necessárias a serem modificadas que foram incluídas ou excluídas do Plano de Comunicação de Riscos.

Responsável: Autoridade competente.

Condição para início:

- Início do Processo 1 – Estabelecer Contexto.

Informações necessárias:

- objetivos, premissas e restrições, e escopo do Projeto de GRSIC;
- papéis para gestão de riscos e respectivos profissionais;
- políticas da organização;
- procedimentos da organização;
- conhecimento de profissionais da organização; e
- conhecimento dos responsáveis pelos setores e responsáveis por ativos na unidade.

Condição para ser finalizada:

- Plano de Comunicação de Riscos aprovado pela Autoridade competente.

Informações produzidas:

- Plano de Comunicação de Riscos com o público-alvo, as informações a serem comunicadas, a periodicidade de comunicação das informações, os resultados desejados, a forma de comunicação (veículo), emissor e receptor de cada informação a ser comunicada definidos.

***Template* e exemplo da Atividade 6.1 – Planejar Comunicação de Riscos.**

A **Figura 45** mostra um modelo de Plano de Comunicação de Riscos. A **Figura 46** apresenta um exemplo.

PLANO DE COMUNICAÇÃO DE RISCOS						
Organização:				**Projeto de GRSIC:**		
Público Alvo:						
ID	**Evento**	**Informação**	**Periodici-dade**	**Forma de Comunicação**	**Responsável**	**Parte Interessada**
...	...	...	...	...	...	...
Aprovação						
Autoridade competente **Local** **Data**						

Figura 45: *Template* do Plano de Comunicação de Riscos

PLANO DE COMUNICAÇÃO DE RISCOS						
Organização: Ministério do Interior				**Projeto de GRSIC: Projeto de Gestão de Riscos de Segurança da Informação e Comunicações da Secretaria de Relações Institucionais**		
Público Alvo: Gestor de Riscos, Secretário de Relações Institucionais, Coordenadores e Técnicos da Secretaria.						
ID	**Evento**	**Informação**	**Periodici-dade**	**Forma de Comunicação**	**Responsá-vel**	**Parte Interessada**
E01	Aprovação dos PTRs	Planos de Tratamento de Riscos	Após realização da Tarefa	Via ferramenta de apoio à MGR-	Autor de PTR	- Autoridade competente - Gestor de

			5.3-B	SISP		Riscos
E02	...	...	...	...	...	...
Aprovação						
João Carlos da Silva **31/02/2016**						

Figura 46: Exemplo do Plano de Comunicação de Riscos

6.8.3 – Atividade 6.2 – Executar Plano de Comunicação de Riscos

Esta atividade é realizada pelo Gestor de Riscos em grande parte dos **Processos 1 a 5**. Ela tem por objetivo coletar informações de todas as atividades dentro de um Processo e reporta-las às partes interessadas, conforme definido no **Plano de Comunicação de Riscos**.

O fluxo de tarefas desta Atividade deve estar definido nos próprios Planos de Comunicação de Riscos.

Dessa forma, de forma resumida, a **Figura 47** mostra fluxo de tarefas da atividade.

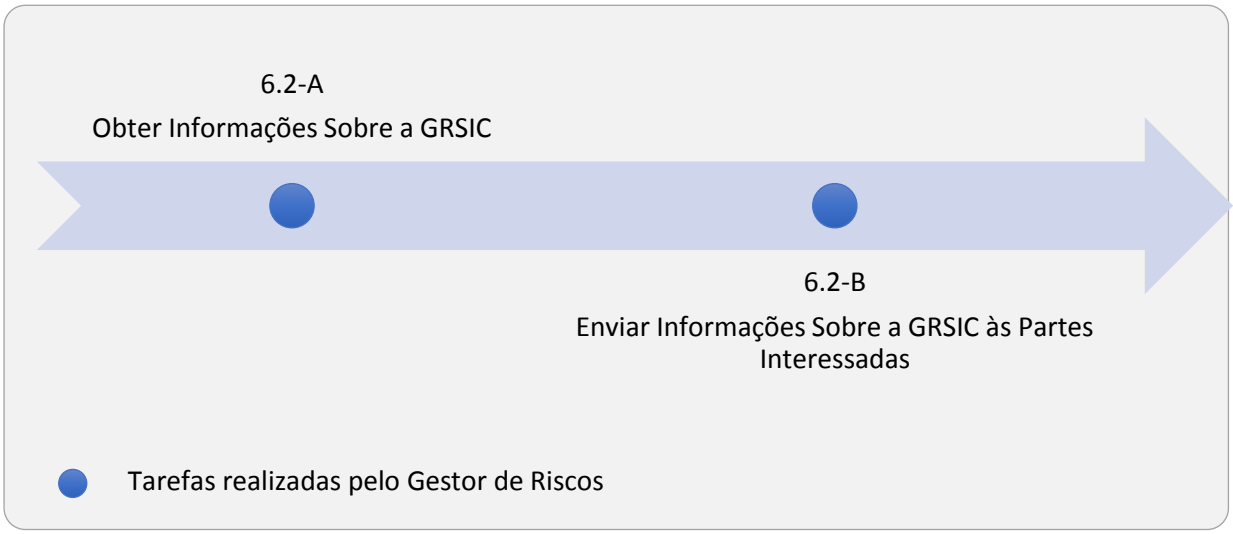

Figura 47: Fluxo de tarefas da Atividade 6.2 – Executar Plano de Comunicação de Riscos

TAREFAS DA ATIVIDADE 6.2 – Executar Plano de Comunicação de Riscos

Tarefa 6.2-A: Obter Informações Sobre a GRSIC.

O Gestor de Riscos deve obter as informações constantes do Plano de Comunicação de Riscos durante a realização dos Processos 1 a 5.

Responsável: Gestor de Riscos.

Tarefa 6.2-B: Enviar Informações Sobre a GRSIC às Partes Interessadas.

O Gestor de Riscos deve enviar as informações obtidas na Tarefa 6.2-A para as partes interessadas conforme Plano de Comunicação de Riscos.

Responsável: Gestor de Riscos.

Condição para início:

- Plano de Comunicação de Riscos aprovado pela Autoridade competente.

Informações necessárias:

- Aquelas constantes do Plano de Comunicação de Riscos

Condição para ser finalizada:

- Projeto de GRSIC encerrado.

Informações produzidas: Não há. Existe apenas tráfego de informações conforme Plano de GRSIC.

Não há *template* para a realização desta atividade.

6.8.4 – Atividade 6.3 – Validar Informações Estratégicas

Esta atividade tem como objetivo avaliar e validar informações estratégicas para organização, relacionadas ao processo de GRSIC. Algumas atividades requerem que a **Autoridade Competente** avalie e valide as informações que foram produzidas de forma que, caso seja necessário, a atividade seja reexecutada. A **Figura 48** mostra fluxo de tarefas da atividade.

As atividades em que ocorre este tipo de comunicação são as descritas abaixo.

- **Atividade – 1.1 – Iniciar Projeto de GRSIC**
- **Atividade – 1.2 - Realizar Pré-Análise do Escopo do Projeto de GRSIC**

- **Atividade – 4.1 - Classificar os Riscos**
- **Atividade – 5.2 - Definir Resposta aos Riscos**
- **Atividade – 5.3 - Implementar Resposta aos Riscos**

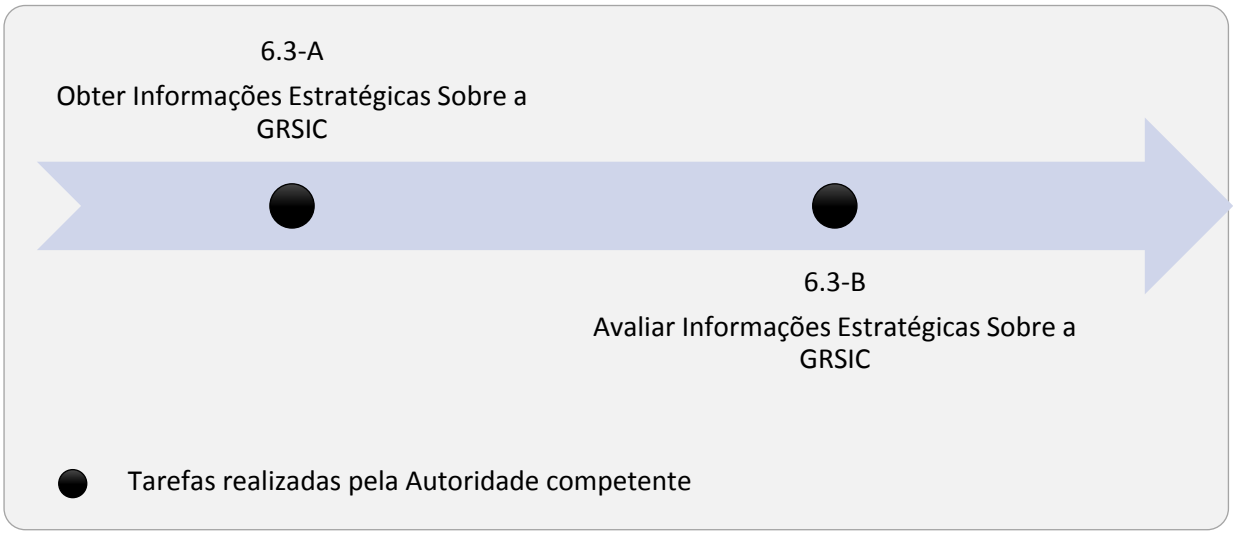

Figura 48: Fluxo de tarefas da Atividade 6.3 – Validar Informações Estratégicas

TAREFAS DA ATIVIDADE 6.3 – Validar Informações Estratégicas da GRSIC

Tarefa 6.3-A: Obter Informações Estratégicas Sobre a GRSIC.

A Autoridade Competente deve obter as informações constantes do Plano de Comunicação de Riscos durante a realização dos Processos 1 a 5.

Responsável: Autoridade Competente.

Tarefa 6.3-B: Avaliar Informações Estratégicas Sobre a GRSIC.

A Autoridade Competente deve avaliar se as informações obtidas na Tarefa 6.3-A atendem as necessidades e expectativas da organização. Caso estejam de acordo, a Autoridade Competente deve registrar a aprovação das Informações Estratégicas da GRSIC e encerra-se, dessa forma, a Atividade 6.3 – Validar Informações Estratégicas. Caso contrário, a Autoridade Competente deve notificar o Gestor de Riscos da necessidade de realizar novamente a Tarefa, Atividade e/ou Processo de origem da informação e fornecer descrições das questões identificadas como necessárias a serem modificadas, incluídas, excluídas ou realizadas.

Responsável: Autoridade Competente.

Condição para início:

- Plano de Comunicação de Riscos em execução.

Informações necessárias:

- aquelas constantes do Plano de Comunicação de Riscos

Condição para ser finalizada:

- Informações Estratégicas da GRSIC validadas.

Informações produzidas (para os casos de não validação das informações estratégicas da GRSIC):

- descrições das questões identificadas como necessárias a serem modificadas, incluídas, excluídas ou realizadas;
- Tarefas, Atividades e/ou Processos a serem realizados novamente.

Não há *template* para a realização desta atividade.

6.9 – Processo 7 – Monitorar Riscos

6.9.1 – Descrição do Processo

Este processo tem por objetivo monitorar os resultados do **Processo de GRSIC**. Novas ameaças, novas vulnerabilidades e novos ativos podem alterar ou ampliar os riscos anteriormente avaliados, tornando necessário o monitoramento.

Também faz parte desse processo o acompanhamento do tratamento dos riscos, para assegurar que as medidas de resposta aos riscos planejadas sejam adequadamente implementadas.

Como no processo anterior, este processo desenvolve-se simultaneamente com os demais processos (iniciando no **Processo 1 – Estabelecer Contexto**) e as atividades são executadas durante todo o processo de gestão de riscos. A **Figura 49** mostra o fluxo de atividades do processo.

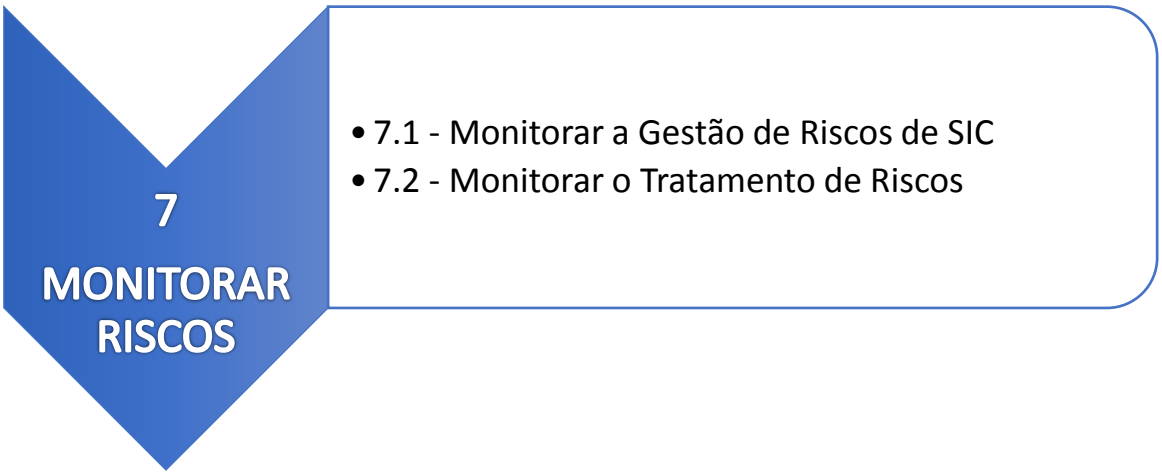

Figura 49: Fluxo de atividades do Processo 7 – Monitorar Riscos

6.9.2 – Atividade 7.1 – Monitorar a Gestão de Riscos de SIC

Nesta atividade, todos os papéis envolvidos na GRSIC devem monitorar alterações que impactam no resultado da GRSIC.

Monitorar procedimentos e novas informações que possam impactar ou alterar os resultados do **Projeto de GRSIC** de modo geral. A atividade abrange todas as informações que possam alterar o contexto geral da avaliação dos riscos. Isso inclui:

- Novos ativos, substituídos ou descartados.
- Restrições ou escopo que foram modificados.
- Alterações na valoração dos ativos.
- Novas ameaças e vulnerabilidades.
- Incidentes de segurança que podem ocorrer após a análise de risco.

Essas informações precisam ser repassadas ao Gestor de Riscos por todos os envolvidos no processo de Gestão de Riscos de Segurança da Informação e Comunicações da Organização. Neste caso, deve-se observar o Plano de Comunicação de Riscos elaborado no Processo 6 – Comunicar Riscos. O Gestor de Riscos deve ser sempre comunicado no momento oportuno das informações ou fatos que possam impactar ou alterar os resultados do **Projeto de GRSIC.** Recomenda-se que a Política de Segurança da Informação e Comunicações da Organização contenha diretrizes sobre o assunto.

A **Figura 50** mostra fluxo de tarefas da atividade.

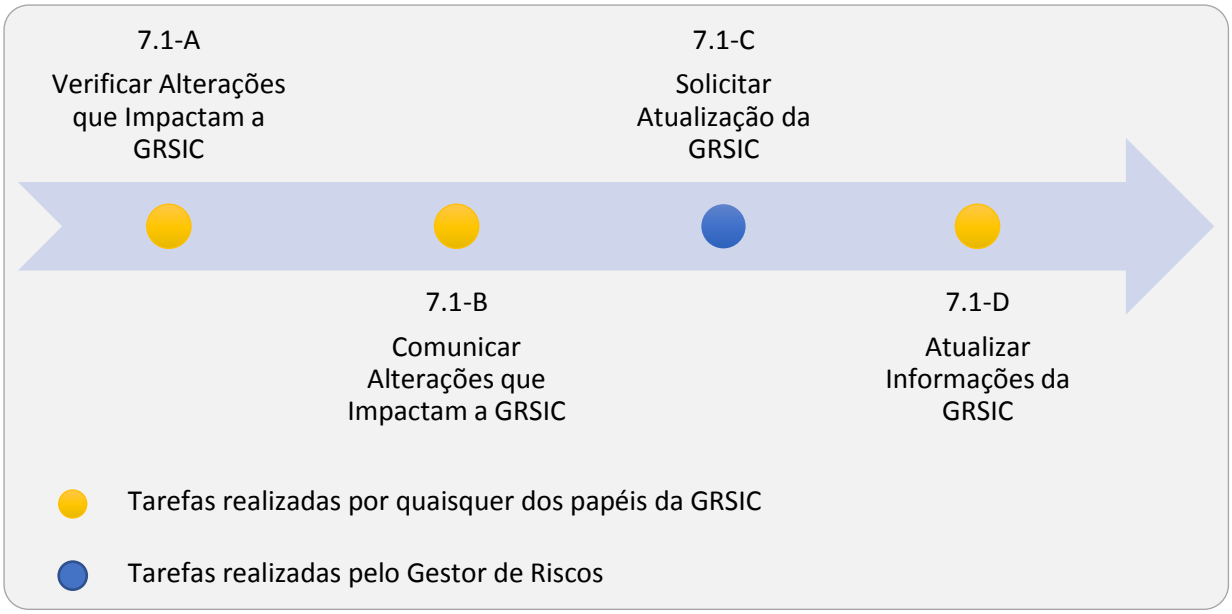

Figura 50: Fluxo de tarefas da Atividade 7.1 – Monitorar Gestão de Riscos de SIC

TAREFAS DA ATIVIDADE 7.1 – Monitorar Gestão de Riscos de SIC

Tarefa 7.1-A: Verificar Alterações que Impactam a GRSIC.

Os Responsáveis Por Ativos, os Responsáveis Pelas Unidades da Organização, o Gestor de Riscos e a Autoridade Competente devem verificar, a qualquer momento do processo de GRSIC, se existem procedimentos ou novas informações que possam impactar ou alterar os resultados da Análise Riscos de modo geral, tais como:

- novos ativos, substituídos ou descartados;
- restrições ou escopo que foram modificados;
- alterações na valoração dos ativos;
- novas ameaças e vulnerabilidades
- incidentes de segurança que podem ocorrer após a análise de riscos.

Caso existam, realiza-se a Tarefa 7.1-B: Informar Alterações que Impactam a GRSIC.

Responsável: Responsável Por Ativos, Responsável Pela Unidade da Organização, Gestor de Riscos e Autoridade Competente.

Tarefa 7.1-B: Comunicar Alterações que Impactam a GRSIC.

Esta tarefa é realizada somente se a Tarefa 7.1-A for concluída.

Os Responsáveis Por Ativos, os Responsáveis Pelas Unidades da Organização e a Autoridade Competente devem notificar o Gestor de Riscos para realizar a Tarefa 7.1-C: Solicitar Atualização

da GRSIC e informar o prazo e as informações necessárias para que se procedam as atualizações, observado o Plano de Comunicação de Riscos.

Responsável: Responsável Por Ativos, Responsável Pela Unidade da Organização, Gestor de Riscos e Autoridade Competente.

Tarefa 7.1-C: Solicitar Atualização da GRSIC.

O Gestor de Riscos deve notificar os responsáveis pela realização de processos, atividades e/ou tarefas, fornecendo descrições das questões identificadas como necessárias a serem modificadas, incluídas, excluídas ou realizadas. Neste ponto, pode ser necessária a realização de quaisquer Processos da MGR-SISP.

Responsável: Gestor de Riscos.

Tarefa 7.1-D: Atualizar Informações da GRSIC.

Os Responsáveis Por Ativos, os Responsáveis Pelas Unidades da Organização, o Gestor de Riscos e/ou a Autoridade Competente devem realizar de processos, atividades e/ou tarefas indicadas pelo Gestor de Riscos, utilizando as descrições das questões identificadas como necessárias a serem modificadas, incluídas, excluídas ou realizadas.

Responsável: Gestor de Riscos.

Condição para início:

- Processo 1 – Estabelecer Contexto iniciado.

Informações necessárias:

- Quaisquer procedimentos e/ou novas informações que possam impactar ou alterar os resultados do Projeto de GRSIC de modo geral.

Condição para ser finalizada: Projeto de GRSIC encerrado.

Informações produzidas: Informações geradas nos processos, tarefas e/ou atividades que foram reexecutadas.

6.9.3 – Atividade 7.2 – Monitorar o Tratamento de Riscos

Nesta atividade o Gestor de Riscos deve monitorar os riscos que estão em processo de tratamento, ou seja, se o PTR está sendo seguido. Isso inclui:se o PTR está dentro do

prazo estabelecido para a implementação; se o PTR foi finalizado, verificar se a realização de testes de efetividade dos controles.

O fluxo de tarefas desta atividade pode ser definido em cada PTR elaborado. De forma resumida, a **Figura 51** mostra fluxo de tarefas da atividade.

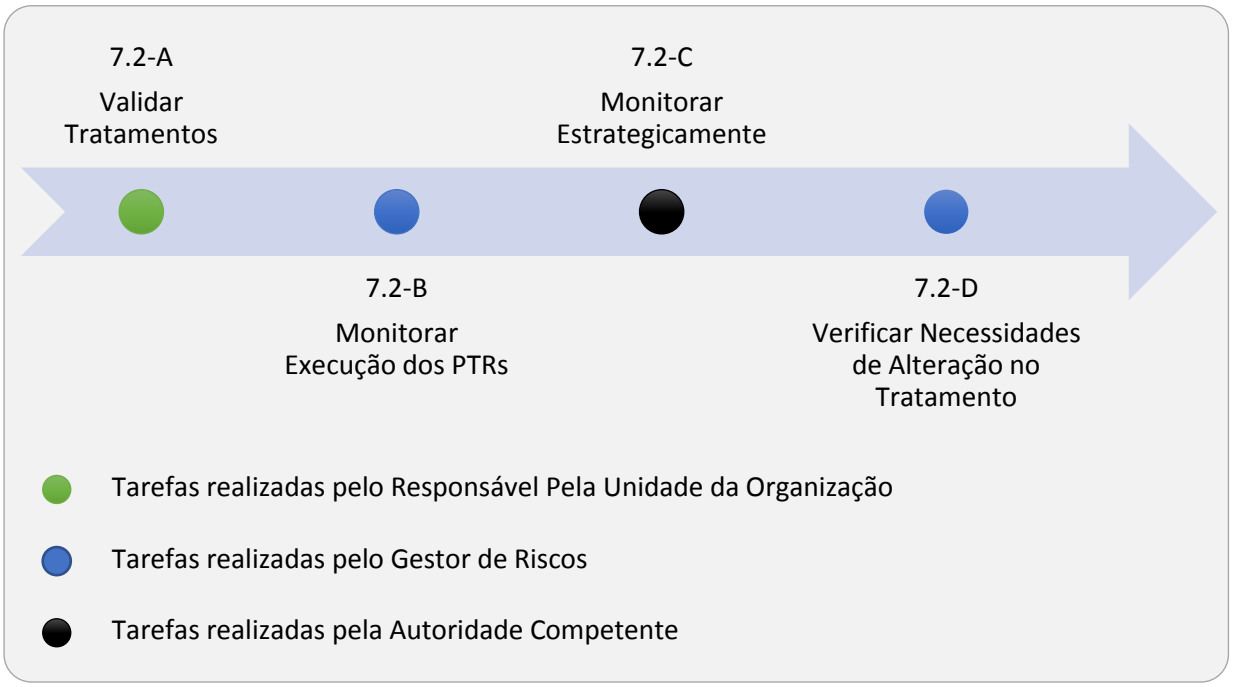

Figura 51: Fluxo de tarefas da Atividade 7.1 – Monitorar Tratamento de Riscos

TAREFAS DA ATIVIDADE 7.2 – Monitorar o Tratamento de Riscos

Tarefa 7.2-A: Avaliar Tratamentos.

Esta tarefa deve ser executada em paralelo com a Tarefa 5.3-F: Executar Plano de Tratamento de Riscos.

Cada Responsável Pela Unidade da Organização responsável por um Plano de Tratamento de Riscos deve avaliar periodicamente a execução do tratamento e registrar o progresso da implementação (em percentual realizado).

Ao final da implementação do Plano de Tratamento de Riscos, o responsável deve avaliar a correção dos controles estabelecidos por meio de verificações e testes e deve fornecer uma descrição sobre as ações realizadas. Além disso, o responsável deve anexar uma evidência da correta implementação dos controles previstos no Plano de Tratamento de Riscos e comunicar ao Gestor de Riscos o final da implementação do Plano de Tratamento de Riscos para realização da Tarefa 7.1-B: Monitorar Execução dos Planos de Tratamento de Riscos.

Responsável: Responsável Pela Unidade da Organização.

Tarefa 7.2-B: Monitorar Execução dos Planos de Tratamento de Riscos.

Esta tarefa deve ser executada em paralelo com a Tarefa 7.1-A: Avaliar Tratamentos.

O Gestor de Riscos deve obter as informações constantes de cada Plano de Tratamento de Riscos, para verificar o *status* de cada atividade, do ponto de vista do cumprimento dos prazos, dos testes e da efetividade dos controles implementados.

Ao ser comunicado do final da implementação de um Plano de Tratamento de Riscos, o Gestor de Riscos deve avaliar as evidências fornecidas pelo responsável pelo Plano de Tratamento de Riscos e atualizar o estado de implementação dos controles tratados nos Planos de Tratamento de Riscos.

Caso o Gestor de Riscos não aprove o tratamento dos riscos e as evidências fornecidas, o Responsável pela Unidade da Organização designado como responsável pelo Plano de Tratamento de Riscos deve ser notificado da necessidade de realizar ações adicionais, fornecendo descrições das questões identificadas como necessárias a serem modificadas, incluídas, excluídas ou realizadas. Isto ocorre até que o tratamento e as evidências sejam satisfatórias. Pode ser necessário realizar novamente as Tarefas 5.3-D e 7.1-A.

Aprovado o tratamento, Gestor de Riscos deve comunicar à Autoridade Competente dos resultados do tratamento de riscos para realização da Tarefa 7.1-C: Monitorar Estrategicamente.

Responsável: Gestor de Riscos.

Tarefa 7.2-C: Monitorar Estrategicamente.

A Autoridade Competente, com respaldo da análise técnica feita pelo Gestor de Riscos, deve decidir se o tratamento de riscos realizado é suficiente ou se outras ações são necessárias.

Neste ponto de decisão, atividades de processos anteriores podem ser reexecutadas se o julgamento indicar a necessidade de realizar outras ações para tratar os riscos.

Nesses casos, o Gestor de Riscos deve ser informado da necessidade de revisar decisões e devem ser fornecidas descrições das questões identificadas pela organização.

Responsável: Autoridade Competente.

Tarefa 7.2-D: Verificar Necessidades de Alteração no Tratamento dos Riscos.

Esta tarefa deve ser executada em paralelo com a Tarefa 5.3-F: Executar Plano de Tratamento de Riscos.

O Gestor de Riscos deve obter as informações sobre os riscos de modo geral, ou seja, todos os riscos que compõem o Mapa de Riscos precisam ser monitorados. Isso inclui, no caso de riscos

aceitos (retidos), avaliar periodicamente se há alterações relevantes que justifiquem a definição de outro tratamento. Caso necessário, podem ser realizados novamente os Processos 4 – Avaliar Riscos e 5 – Tratar Riscos.

Responsável: Gestor de Riscos.

Condição para início:

- Plano de Tratamento de Riscos em execução.

Informações necessárias:

- Mapa de Riscos.
- Plano de Tratamento de Riscos.

Condição para ser finalizada:

- Projeto de GRSIC encerrado.

Informações produzidas:

- Para os casos de não validação dos testes de efetividade dos controles: descrições das questões identificadas como necessárias a serem modificadas, incluídas, excluídas ou realizadas; Tarefas, Atividades e/ou Processos a serem realizados novamente.
- Para os casos de alteração do tratamento dos riscos: novo PTR ou PTRs alterados.

Não há *template* para a realização desta atividade.

7 – REFERÊNCIAS

ABNT ISO GUIA 73: 2009, “Gestão de riscos – Vocabulário”.

(Canongia e outros, 2010): Claudia Canogia, Admilson Gonçalves Júnior, Raphael Mandarino Junior (organizadores) "Guia de referência para a Segurança das Infraestruturas Críticas da Informação. Versão 01 – Nov./2010." Presidência da República. Disponível em: http://dsic.planalto.gov.br. Consultado em Maio, 2015.

ABNT NBR ISO/IEC 27001, “Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da SIC —”, ISO/IEC 2013.

ISO/IEC 27002, “Information technology – Security techniques – Code of pratice for information security management”, ISO/IEC 2013.

ABNT NBR ISO/IEC 27005, “Tecnologia da informação — Técnicas de segurança — Gestão de riscos de SIC”, ISO/IEC 2011.

ISO 31000, “Risk management – Principles and guidelines”, ISO 2009.

ISO 31010, “Risk management – Risk assessment guidelines”, ISO 2009.

“IT-Grundschutz Methodology, BSI Standard 100-2”, Version 2.0, Maio 2008, www.bsi.bund.de

National Institute of Standards and Technology – NIST (EUA). NIST 800-39 – “Managing Information Security Risk.” Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>. Consultado em Maio, 2015.

(NIST 800-30, 2011). National Institute of Standards and Technology – NIST (EUA). “NIST 800-30 – Guide for Conducting Risk Assessment”, Setembro, 2011. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-30-final.pdf>. Consultado em Maio, 2015.

(Yoo e outros, 2007) Dong-Young Yoo, Jong-Whoi Shin, Gang Shin Lee, and Jae-I Lee. “Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)”, International Scholarly and Scientific Research & Innovation 1(12), 2007, World Academy of Science, Engineering and Technology.

ANEXO A

CONSIDERAÇÕES SOBRE O TRATAMENTO DE ATIVOS DE INFORMAÇÃO NA NC 10 IN01/DSIC/GSI/PR E NA MGR-SISP

Este anexo descreve a relação entre o tratamento de ativos de informação definido na Norma Complementar nº 10/IN01/DSIC/GSIPR e o estipulando na Metodologia de Gestão de Riscos MGR-SISP. Esta NC estabelece as diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta, tendo sido publicado em 2012.

A MGR-SISP contempla boa parte das considerações, conceitos, diretrizes e procedimentos desta NC. No entanto, para deixar a metodologia mais compreensível, voltada a organizações que ainda não estão aderentes à NC, optou-se por adotar uma terminologia mais genérica, como a adotada nas Normas ABNT NBR ISO/IEC 27001, e ABNT NBR ISO/IEC 27005.

Para propiciar o alinhamento da MGR-SISP com os princípios e diretrizes da NC 10 IN01/DSIC/GSI/PR a **Tabela 8** descreve o mapeamento de etapas do processo inventário de ativos, descritas na NC 10 IN01/DSIC/GSI/PR, para os respectivos elementos da MGR-SISP.

PROCESSO DE INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO (NC 10 IN01/DSIC/GSI/PR)	TRATAMENTO ESTABELECIDO NA MGR-SISP
Etapa coleta de informações gerais dos ativos de informação	As definições do escopo e de estratégia são feitas no processo **1 – Estabelecer Contexto.**
Etapa Detalhamento dos ativos de informação	O nível de detalhe para cadastro de ativos é definido no processo Estabelecer Contexto. A organização pode identificar a necessidade de cadastrar apenas ativos primários (processos de negócio e informações), ou todos os tipos de ativo. As informações sobre o ativo são definidos nos processos **2 – Identificar Riscos e 3 – Estimar Riscos**.
Etapa Identificação dos responsáveis de cada ativo de informação	Nas etapas de Identificação de Riscos e Estimativa de Riscos os Proprietários de Ativos e os Responsáveis por Unidades são identificados. A MGR-SISP não estabelece o papel de

	"custodiante de ativos", no entanto o papel "responsável por unidade" pode atuar como custodiante, na medida em que este é o responsável formal pelos ativos alocados em cada unidade da organização. O papel "Responsável Por Ativos" é previsto na MGR-SISP tendo significado semelhante ao encontrado na NC 10 IN01/DSIC/GSI/PR.
Etapa caracterização dos containers dos ativos de informação.	Este conceito (container: "local onde vive o ativo de informação") não existe explicitamente na MGR-SISP. Entretanto a metodologia permite caracterizar ativos como: "sala", "rede de transmissão", "notebook", etc., que por natureza, podem conter outros ativos. A possibilidade de correlacionar os ativos permite, portanto modelar o conceito de "container" da NC 10 IN01/DSIC/GSI/PR.
Definição dos requisitos de SIC e comunicações e Estabelecimento do valor dos ativos de informação.	Os Processos Estimar Riscos e Avaliar Riscos abordam a definição dos requisitos de segurança e o estabelecimento de valor dos ativos por meio da análise sistemática de Ameaças, Controles existentes, Vulnerabilidades, Probabilidades de incidentes e Consequências de Incidentes.

Tabela 8: Mapeamento entre etapas do processo inventário de ativos e elementos da metodologia de gestão de riscos