sid.inpe.br/mtc-m21c/2021/05.04.21.23-TDI

UM ESTUDO SOBRE A GESTÃO DE RISCOS E A GARANTIA DA SEGURANÇA EM PROJETOS DE SATÉLITES

Bruna Franco Campos Barroso

Dissertação de Mestrado do Curso de Pós-Graduação em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelos Drs. Leonel Fernando Perondi, e Andreia Fatima Sorice Genaro, aprovada em 29 de abril de 2021.

URL do documento original:
<http://urlib.net/8JMKD3MGP3W34R/44KL2Q5>

INPE
São José dos Campos
2021

PUBLICADO POR:

Instituto Nacional de Pesquisas Espaciais - INPE
Coordenação de Ensino, Pesquisa e Extensão (COEPE)
Divisão de Biblioteca (DIBIB)
CEP 12.227-010
São José dos Campos - SP - Brasil
Tel.:(012) 3208-6923/7348
E-mail: pubtc@inpe.br

sid.inpe.br/mtc-m21c/2021/05.04.21.23-TDI

UM ESTUDO SOBRE A GESTÃO DE RISCOS E A GARANTIA DA SEGURANÇA EM PROJETOS DE SATÉLITES

Bruna Franco Campos Barroso

Dissertação de Mestrado do Curso de Pós-Graduação em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais, orientada pelos Drs. Leonel Fernando Perondi, e Andreia Fatima Sorice Genaro, aprovada em 29 de abril de 2021.

URL do documento original:
<http://urlib.net/8JMKD3MGP3W34R/44KL2Q5>

INPE
São José dos Campos
2021

Dados Internacionais de Catalogação na Publicação (CIP)

Barroso, Bruna Franco Campos.

B278e Um estudo sobre a gestão de riscos e a garantia da segurança em projetos de satélites / Bruna Franco Campos Barroso. – São José dos Campos : INPE, 2021.

xxiii + 167 p. ; (sid.inpe.br/mtc-m21c/2021/05.04.21.23-TDI)

Dissertação (Mestrado em Engenharia e Tecnologia Espaciais/Engenharia e Gerenciamento de Sistemas Espaciais) – Instituto Nacional de Pesquisas Espaciais, São José dos Campos, 2021.

Orientadores : Drs. Leonel Fernando Perondi, e Andreia Fatima Sorice Genaro.

1. Segurança de sistemas. 2. Satélite. 3. Gerenciamento de projeto espacial. 4. Gestão de riscos. 5. Processos. I.Título.

CDU 629.78:005.53

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

Serviço de Pós-Graduação - SEPGR

DEFESA FINAL DE DISSERTAÇÃO DE BRUNA FRANCO CAMPOS BARROSO
BANCA Nº 076/2021, REG 141569/2018

No dia 29 de abril de 2021, às10h00min, por Conferência Online, o(a) aluno(a) mencionado(a) acima defendeu seu trabalho final (apresentação oral seguida de arguição) perante uma Banca Examinadora, cujos membros estão listados abaixo. O(A) aluno(a) foi APROVADO(A) pela Banca Examinadora por unanimidade, em cumprimento ao requisito exigido para obtenção do Título de Mestra em Engenharia e Tecnologia Espaciais / Engenharia e Gerenciamento de Sistemas Espaciais. O trabalho precisa da incorporação das correções sugeridas pela Banca Examinadora e revisão final pelo(s) orientador(es).

Título: "UM ESTUDO SOBRE A GESTÃO DE RISCOS E A GARANTIA DA SEGURANÇA EM PROJETOS DE SATÉLITES"

Observações da banca: Seguir as sugestões da banca.

Eu, Milton de Freitas Chagas Junior, Presidente da Banca Examinadora, assino esta ATA, em nome de todos os membros, com o consentimento dos mesmos.

Membros da Banca

Dr. Milton de Freitas Chagas Junior - Presidente – INPE
Dr. Leonel Fernando Perondi – Orientador - INPE
Dra. Andreia de Fátima Sorise Genaro - Orientadora - INPE
Dr. Mauricio Gonçalves Vieira Ferreira - Membro Interno - INPE
Dr. Carlos Henrique Netto Lahoz – Membro Externo – ITA/UNIVAP/UNIP

Documento assinado eletronicamente por **Milton de Freitas Chagas Junior**, **Chefe do Serviço de Relações Institucionais**, em 03/05/2021, às 08:24 (horário oficial de Brasília), com fundamento no art. 6º do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **7038419** e o código CRC **E7E0AB18**.

Referência: Processo nº 01340.002556/2021-85 SEI nº 7038419

“Mesmo quando tudo parece desabar, cabe a mim decidir entre rir ou chorar, ir ou ficar, desistir ou lutar; porque descobri, no caminho incerto da vida que o mais importante é o decidir”.

Cora Coralina

Dedico este trabalho a meu pai Robério (*in memoriam*) que sempre sonhou junto comigo e foi meu maior incentivador, mas que infelizmente não pode ver esse nosso sonho se realizar.

A minha mãe Nicimar que é minha maior inspiração por sua dedicação e apoio.

A meu irmão Vinícius pela cumplicidade e palavras de motivação.

A meu marido Mário pelo amor, incentivo e parceria que tornaram possível a conclusão desse trabalho.

AGRADECIMENTOS

Primeiramente quero agradecer a minha mãe que nunca mediu esforços para me dar a melhor educação possível, a meu irmão pelo constante apoio emocional e meu marido por compreender minha dedicação ao meu curso de mestrado.

Deixo um agradecimento especial aos meus orientadores Dra. Andreia Sorice Genaro e Dr. Leonel Fernando Perondi por acreditarem em mim e na minha proposta de trabalho e pelo incansável suporte e valiosas contribuições dadas ao longo do processo.

Agradeço a todos os professores do curso de Engenharia e Gerenciamento de Sistemas Espaciais (CSE) do INPE – Instituto Nacional de Pesquisas Espaciais pelo conhecimento compartilhado que possibilitou o desenvolvimento da pesquisa. Agradeço também ao Dr. Leandro Toss Hoffmann, Dr. Adenilson Roberto Da Silva, Dr. Antonio Carlos De Oliveira Pereira Junior e Dr. Nelson Jorge Schuch por se disponibilizarem a responder questionários que foram de extrema relevância para a conclusão deste trabalho.

Gostaria de agradecer a minha amiga Fernanda Lopes pelas caronas para as aulas de manhã cedo, aos meus amigos Larissa Martins e Philipe Bringhenti que foram meus procuradores para questões relacionadas ao INPE e me deram todo suporte enquanto estive fora do país. Também gostaria de agradecer aos meus amigos de curso Bruno Junqueira, Isomar Lima e Yuri Matheus pelo companheirismo e amizade que tornaram meus dias mais leves e divertidos.

Por último, quero agradecer também ao Instituto Nacional de Pesquisas Espaciais e todos seus colaboradores por fornecer toda infraestrutura necessária e pela qualidade e excelência do ensino que me foi oferecido.

RESUMO

O ambiente espacial apresenta riscos de diversas naturezas que, aliados à complexidade de execução de projetos de sistemas espaciais, justificam o exercício de técnicas e metodologias de gestão especiais no sentido de garantir o sucesso de missões. A disciplina de gestão de riscos, de forma sintética, tem por objetivo identificar os riscos que afetam o sucesso de missões e desenvolver estratégias para a sua mitigação, enquanto a de garantia da segurança busca, de forma geral, garantir a integridade da vida humana, dos recursos físicos gerais envolvidos nos projetos e do meio ambiente. As disciplinas de gestão de risco e garantia de segurança apresentam similaridades de objetivos e técnicas, pois buscam identificar e monitorar riscos a fim de evitá-los ou minimizar seu impacto. Pesquisa na literatura acerca das disciplinas de gestão de riscos e de garantia da segurança demonstrou haver um hiato de estudos versando sobre como uma disciplina se relaciona à outra, em suas aplicações no desenvolvimento de projetos espaciais. O presente trabalho visa abordar esta relação, com foco no tratamento dispensado por ambas as disciplinas a riscos comuns entre si, como os que ameaçam a segurança do sistema, com repercussões sobre domínios do projeto como custo, cronograma e outros. Este trabalho também apresentará uma lista de requisitos mínimos de segurança e gestão de risco para missões de grande, médio, pequeno e nano portes, considerando a relação entre a gestão de risco e de garantia da segurança.

Palavras-chave: Segurança de sistemas, Satélite, Gerenciamento de projeto espacial, Gestão de riscos, Processos.

A STUDY OF RISK MANAGEMENT AND SAFETY ASSURANCE IN SATELLITE PROJECTS

ABSTRACT

The space environment presents risks of different natures which associated to the complexity of space system projects justifies the exercise of the special management techniques and methodologies to ensure mission success. The discipline of risk management, in essence, aims to identify the risks that affect the success of missions and to develop strategies for their mitigation, while the discipline of safety assurance seeks, in general, to ensure the integrity of human life, physical resources involved in the projects, and of the environment. The disciplines of risk management and safety assurance present similarities in their objectives and techniques since they seek to identify and monitor risks to avoid them or minimize their impact. A literature search on the disciplines of risk management and safety assurance demonstrated that there is a gap in the studies dealing with how one discipline is related to the other, in their application to the development of space projects. The present work aims to address this relationship, focusing on how both disciplines deal with risks that are common to each other, such as those that deals with system safety, which are directly related to project domains such as cost, schedule, and others. This dissertation will also present a list of minimum safety and risk management requirements for large, medium, small, and nano-sized orbital satellite missions, taking into consideration the relationship between risk management and safety.

Keywords: Systems safety, Satellite, Space project management, Risk management, Processes.

LISTA DE FIGURAS

LISTA DE TABELAS

Pág.

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
AEB	Agência Espacial Brasileira
ANSI	American National Standards Institute
AR	Acceptance Review
AS	Aerospace Standard
ASARP	As Safe as Reasonably Practicable
CBERS	China–Brazil Earth Resources Satellite Program
CCB	Configuration Control Board
CDR	Critical Design Review
CGETE	Coordenação de Engenharia e Tecnologia Espacial
CRM	Continuous Risk Management
CRR	Commissioning Result Review
DOD	Department of Defense
DRD	Document requirements description
EADS	European Aeronautic Defense and Space Company
ECSS	European Cooperation for Space Standardization
ELR	End of Life Review
EQUARS	Equatorial Atmosphere Research Satellite
ESA	European Space Agency
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effect and Criticality Analysis
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
GEO	Geostationary Orbit
GOCNAE	Grupo de Organização da Comissão Nacional de Atividades Espaciais
GSE	Ground Support Equipment
GTO	Transfer Orbits and Geostationary Transfer Orbit
INCOSE	International Council on Systems Engineering
INPE	Instituto Nacional de Pesquisas Espaciais
ISA	Integrated Safety Analysis
ISO	International Organization for Standardization
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
LEO	Low Earth Orbit
LRR	Launch Readiness Review
MCR	Mission Close-out Review
MDR	Mission Definition Review
MEO	Medium Earth Orbit
MIL-STD	Military Standard
NASA	National Aeronautics and Space Administration
NBR	Norma Brasileira Regulamentadora

NESC	NASA Engineering and Safety Center
NR	Normas Regulamentadoras
NRBs	Nonconformance Review Boards
ORR	Operational Readiness Review
PDR	Preliminary Design Review
PMBOK	Project Management Body of Knowledge
PRA	Probabilistic Risk Assessment
PRR	Preliminary Requirements Review
QR	Qualification Review
RIDM	Risk-Informed Decision Making
RM	Risk Management
SEH	Systems Engineering Handbook
SMA	Safety Mission Assurance
SMEs	Subject Matter Experts
SRR	System Requirements Review
SSO	Sun-synchronous Orbit
SSTL	Surrey Satellite Technology
SSTP	Small Spacecraft Technology Program
TRB	Test Review Board

SUMÁRIO

1 INTRODUÇÃO

1.1 Contexto

O conceito de segurança de sistema foi introduzido após a Segunda Guerra Mundial, na indústria nuclear evoluindo para a aviação civil e indústria química. (LEVENSON, 2008). A disciplina de gestão da segurança pode ser definida como a aplicação de conhecimento interdisciplinar para otimizar a segurança de um sistema sem comprometer a eficácia operacional do sistema e as restrições de tempo e custo ao longo das fases do ciclo de vida do sistema, incluindo projeto e operação (INCOSE, 2015). Na área espacial, tal conceito surge com a guerra fria, onde o foco eram voos tripulados e o desenvolvimento de foguetes, atendendo a requisitos de alto nível no sentido de se assegurar inexistência de danos em relação à vida humana, durante a execução de projetos e missões espaciais (GENARO, 2018). O ano de 1957 marca o início da era espacial da humanidade, com o lançamento do satélite Sputnik-1 da União Soviética desencadeando a corrida espacial dos anos 1960 (SWEETING, 2018). No contexto histórico compreendido entre o final da década de 1950 e o início da década de 1960, nasce a disciplina de segurança de sistemas espaciais (MUSGRAVE; LARSEN; SGOBBA, 2009).

O gerenciamento de riscos do projeto é definido como uma disciplina direcionada a reduzir as incertezas sobre os objetivos de um projeto e restringir ou mitigar o impacto de eventos deletérios sobre tais objetivos. A disciplina é organizada como um conjunto de processos que tratam, inicialmente, da identificação, avaliação e priorização dos riscos e, posteriormente, do monitoramento e controle desses riscos e da implementação das ações planejadas para minimizar o impacto de eventos que venham a ocorrer.

Em organizações que desenvolvem projetos grandes e complexos, como missões espaciais, o gerenciamento de segurança e o gerenciamento de riscos do projeto são geralmente considerados disciplinas pouco relacionadas, com os processos correspondentes realizados de forma independente. Enquanto os processos de gestão de segurança estão principalmente preocupados em identificar, monitorar e agir sobre os perigos associados às instalações e

operações, como em atividades de integração e teste, os processos de gestão de risco do projeto estão principalmente preocupados em identificar, monitorar e agir sobre os riscos que podem impactar os objetivos do projeto.

No entanto, embora exibam objetivos aparentemente diferentes, não é difícil argumentar que ambas as disciplinas compartilham uma grande parte do escopo de seus processos. Por exemplo, ambos estão preocupados em identificar e monitorar riscos e implementar estratégias que minimizem o impacto dos riscos identificados quando eles ocorrem. Além disso, as equipes que desenvolvem atividades nas disciplinas de gerenciamento de risco de projeto e segurança exibem muitos pontos em comum em suas capacidades profissionais, como experiência em identificação de risco e avaliação de exposição a risco.

Em 1958, a *National Aeronautics and Space Administration (NASA)* iniciou o primeiro programa, para enviar o homem ao espaço exterior, por meio do projeto Mercury. Este projeto tinha como um de seus objetivos verificar a capacidade do homem em sobreviver no espaço (MUSGRAVE; LARSEN; SGOBBA, 2009). Em seguida, teve início o programa Gemini e todos os esforços para voos espaciais tripulados se estenderam até a missão Apollo, que culminou com a chegada do homem à Lua, no ano de 1969 (MUSGRAVE; LARSEN; SGOBBA, 2009). A NASA gerenciou programas de sucesso, mas muitos falharam, levando a acidentes com a perda de vidas humanas, como os da Apollo 1 e dos ônibus espaciais Challenger e Columbia (MUSGRAVE; LARSEN; SGOBBA, 2009). As investigações de tais acidentes ajudaram a NASA a aprimorar técnicas para a melhoria de projetos e programas de *safety* (segurança), construindo uma cultura de *safety* que hoje permeia a organização, sendo tratada como referência em projetos espaciais de outros países (MUSGRAVE; LARSEN; SGOBBA, 2009).

Em 2003, logo após o acidente com o ônibus espacial Columbia, a NASA criou o NESC – NASA *Engineering and Safety Center*, com o objetivo de garantir a segurança dos projetos, provendo avaliações independentes dos problemas mais difíceis enfrentados pela NASA (NESC, 2018).

O modelo de funcionamento do NESC foi inovador para a época, e demonstrou ser eficaz, validando o conceito de um centro com autonomia, em

que avaliações e análises são realizadas de forma independente da liderança técnica da NASA. Tal modelo mostrou-se necessário, pois é comum haver divergências de avaliação entre as equipes de *safety* e programa/projeto. A eficácia de resultados consolidou a visão de que equipes de *safety* tenham autonomia e independência para desempenhar seu papel em uma organização (NESC, 2018).

No Brasil, as atividades espaciais tiveram impulso com a criação de uma comissão, no governo do presidente Jânio Quadros, para "*estudar e sugerir a política e o programa de investigação espacial brasileira, além de propor medidas para implementação das pesquisas nesse campo*" (OLIVEIRA, 1991). À publicação desse decreto, seguiu-se a criação do Grupo de Organização da Comissão Nacional de Atividades Espaciais (GOCNAE) com os objetivos de formar pessoal especializado e desenvolver atividades nas áreas de radioastronomia, astronomia, rastreio ótico de satélites e comunicações por meio de satélites (OLIVEIRA, 1991). Em 3 de agosto de 1961, é publicado o decreto de criação do GOCNAE que mais tarde deu origem do INPE (OLIVEIRA, 1991).

A Agência Espacial Brasileira (AEB), estabelecida em 1994, é responsável por definir e implantar regulamentação da segurança para controlar os riscos envolvidos nas atividades espaciais no Brasil, com o objetivo de proteção de pessoas, de propriedades e do meio ambiente. Para tal, instituiu um conjunto de regulamentos que estabelecem regras gerais e requisitos aplicáveis a segurança ambiental, lançamento e voo, carga útil, complexo de lançamento e veículo lançador (AEB, 2020). Conforme estes regulamentos, a análise de riscos aborda os riscos de segurança provenientes dos sistemas, das instalações, dos equipamentos de apoio no solo, dos procedimentos, do ambiente e dos erros humanos (AEB, 2020). Referentemente à gestão de riscos, há somente uma iniciativa de âmbito interno à Agência, a com a publicação da portaria de Nº 62, DE 9 DE MAIO DE 2017, que define a política de gestão de riscos e controles internos da gestão da agência. Tal portaria tem por finalidade estabelecer os princípios, diretrizes e responsabilidades a serem observados e seguidos para a gestão de integridade, de riscos e de controles internos dos planos estratégicos, programas, projetos e processos da Agência Espacial Brasileira (BRASIL, 2021).

1.2 Objetivo

O objetivo deste trabalho é estudar a relação entre as disciplinas de gestão de risco de projetos e a de garantia de segurança de sistemas espaciais. Para isso, pretende-se analisar normas e manuais em três vertentes que compõem um projeto espacial: Engenharia de Sistemas, Gestão da Qualidade e Gerenciamento de Projetos, além de documentos específicos sobre a temática de gestão de riscos e de garantia de segurança, dentro de organizações. Também, pretende-se detalhar o processo de garantia de segurança de sistemas espaciais à luz de diversas normas aplicáveis à área espacial.

Este trabalho também apresentará uma lista de requisitos mínimos de segurança e gestão de risco para missões de grande, médio, pequeno e nano portes, considerando a relação entre a gestão de risco e de garantia da segurança.

1.3 Motivação

Gerar uma referência acadêmica sobre o tema de gestão de risco e de garantia da segurança, e suas relações, em projetos da área espacial. Esta referência, entre outras aplicações, poderá vir a subsidiar o Grupo de Garantia da Segurança de Sistemas Espaciais da CGETE do INPE no desenvolvimento de uma metodologia de Gestão de Riscos de Garantia da Segurança em projetos espaciais adaptada aos tipos de projetos desenvolvidos pelo INPE.

1.4 Materiais e métodos

A pesquisa tem um caráter exploratório e, em linhas gerais, visa aprofundar o conhecimento de uma temática, com o objetivo de torná-la mais compreensível. É realizada através de levantamento bibliográfico e da análise de documentos de organizações espaciais (GIL, 2002).

A aplicação da metodologia pode ser dividida nas etapas que se seguem.

1.4.1 Materiais e métodos para introduzir *conceitos* e definições

Os conceitos e definições que proveem o arcabouço teórico para o desenvolvimento do trabalho foram compilados a partir de um trabalho de revisão bibliográfica, consultando livros, artigos científicos, diversas fontes da área espacial e outras fontes relacionadas.

1.4.2 Materiais e métodos para o estudo da gestão de risco e garantia da segurança em padrões e organizações da área espacial

Em um primeiro exercício, analisou-se como a garantia de segurança e a gestão de riscos são abordadas em padrões e manuais, em três disciplinas necessárias ao desenvolvimento de um projeto no âmbito espacial: a Engenharia de Sistemas, a Gestão da Qualidade e o Gerenciamento de Projetos. Para tal, foram estudados os temas de gestão de riscos e de garantia da segurança nas seguintes referências: Project Management Book of Knowledge (PMBOK) 6ª edição (PMBOK, 2017), *Systems Engineering Handbook 4ª edição do International Council on Systems Engineering* (INCOSE) (INCOSE, 2015) *e a Aerospace Standard 9100 (AS9100) REV D* (SAE, 2016).

A seguir, verificou-se como as organizações da área espacial tratam o assunto em termos de processos, requisitos e definições. Para cumprir essa etapa, foram analisados documentos da NASA, da *European Cooperation For Space Standardization* (ECSS) e do INPE. Com relação à ECSS (ESA), foram analisadas as normas ECSS-M-ST-80C *Space Project Management- Risk Management* (ECSS, 2008a)*, ECSS-Q-ST-40C Space Product Assurance – Safety* (ECSS, 2017a)*.* Referente a NASA foram analisados *System Safety Handbook - volumes 1* (NASA, 2011a) *e volume 2* (NASA, 2014), NASA *Risk Management Handbook* (NASA, 2011b). No âmbito do INPE, foram elaborados questionários usando o *Google forms* com perguntas referentes ao assunto e após avaliação foram escolhidos 4 projetos de satélites com diferentes perfis dentro do INPE, a saber: o CBERS-4A, AMAZONIA-1, EQUARS e NANOSATC-BR1. Os questionários foram enviados a cada gerente de programa por meio do

Google forms e os dados foram compilados fazendo uso desta mesma ferramenta.

1.4.3 Materiais e métodos para o estudo da relação entre garantia de segurança e gerenciamento de riscos

Foi efetuado um primeiro estudo sobre como a garantia de segurança e a gestão de riscos se interrelacionam, em nível de disciplinas, na área espacial. Para tal, analisaram-se normas e manuais, nas três vertentes anteriormente citadas. Nesse primeiro exercício, foram estudados os capítulos referentes ao processo de gestão de riscos e de garantia da segurança, nas seguintes referências: PMBOK 6ª edição (PMBOK, 2017), *Systems Engineering Handbook 4ª edição do INCOSE* (INCOSE, 2015) *e a AS9100 REV D* (SAE, 2016).

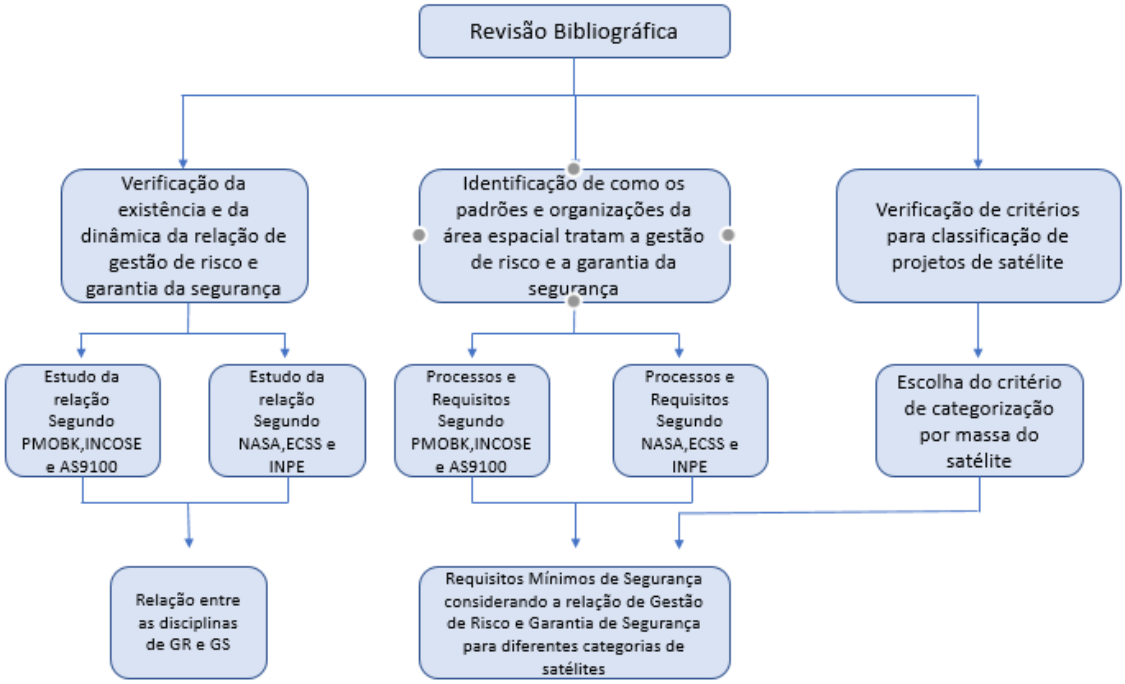
Em um segundo momento, analisou-se como a garantia de segurança e a gestão de riscos se relacionam no âmbito de organizações da área espacial, tomando a ESA, NASA e o INPE como exemplos paradigmáticos. Foram analisados documentos destas organizações, nas três vertentes anteriormente citadas, além de outras normas e documentos específicos sobre a temática de gestão de riscos e garantia de segurança. No que se refere à ESA, foram analisadas as normas ECSS-M-ST-80C *Space Project Management- Risk Management* (ECSS, 2008a)*, ECSS-Q-ST-40C Space Product Assurance – Safety* (ECSS, 2017a)*,* ECSS-E-ST-*10C Space engineering- System engineering general requirements* (ECSS, 2017b)*,* ECSS-M-ST-10C *Space project management- Project planning and implementation* (ECSS, 2009). Referentemente à NASA, foram analisados os seguintes documentos: *NASA Space Flight Program and Project Management Handbook*, *NASA Systems Engineering Handbook* (NASA, 2016), NASA *System Safety Handbook - volume 1* (NASA, 2001a) *e volume 2* (NASA, 2014), NASA *Risk Management Handbook* (NASA, 2011b). No que se refere ao INPE, foram analisadas informações provenientes dos questionários anteriormente citados e documentos do projeto EQUARS, para entender como ocorre essa interação entre gestão de riscos e garantia da segurança em projetos do INPE.

1.4.4 Materiais e métodos para propor requisitos de segurança mínimos para diferentes tipos de projeto de satélite

Para propor os requisitos mínimos de segurança, adequados a diferentes tipos de projeto, buscou-se na literatura a definição de critérios para a classificação de projetos em categorias. Com base neste estudo, adotou-se um esquema de classificação conforme a massa do satélite.

Para realizar o levantamento dos requisitos, optou-se por adaptar o trabalho de Genaro (2019), no qual a autora apresenta um conjunto de requisitos de segurança para projetos de satélite do INPE. No entanto, o levantamento não aborda a relação da gestão de riscos e garantia da segurança, durante o desenvolvimento de projetos, ao tratar de riscos comuns, assim como não separa os requisitos descritos por tipo/classificação de satélite. Para propor os requisitos finais, foram analisados os requisitos de gestão de riscos conforme o padrão ECSS-M-ST-80C *Space Project Management- Risk Management* (ECSS, 2008a*)* e para classificar os satélites foi feita uma adaptação de Konecny (2004). A figura a seguir ilustra a metodologia adotada.

Figura 1.1: Fluxograma da metodologia empregada na pesquisa.



Fonte: Produção da autora.

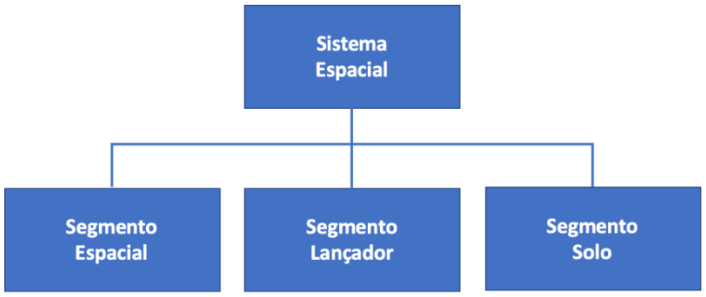
2 REVISÃO DA BIBLIOGRAFIA

2.1 Sistema espacial

O padrão ECSS define a composição de um sistema espacial como segmento espacial, segmento solo e segmento lançador (ECSS, 2012), conforme ilustrado na Figura 2.1. Os elementos são formalmente definidos conforme segue abaixo.

O segmento solo é a parte de um sistema espacial que monitora e controla os elementos do segmento espacial em órbita. Segmento espacial é a parte de um sistema espacial colocada no espaço para cumprir os objetivos da missão. Segmento lançador é a parte de um sistema espacial que é usada para transportar elementos para o espaço (ECSS,2012).

Figura 2.1: Hierarquia de um sistema espacial.



Fonte: Adaptado de ECSS (2012).

2.2 Projetos de sistemas espaciais

Segundo Loureiro (1999), Projetos de sistemas espaciais são empreendimentos específicos, considerando que cada missão é única e com uma estrutura de requisitos extensa e complexa. Os riscos inerentes ao ambiente espacial, somados à complexidade das missões espaciais, mostram a importância e a necessidade de haver um esforço no sentido de assegurar o sucesso de uma missão espacial. Loureiro (1999) afirma a importância da incorporação de tais requisitos no produto espacial, considerando que não existe a possibilidade de consertar o sistema uma vez que ele esteja em órbita: qualquer desvio no projeto pode resultar em perdas para a missão.

De acordo com Yassuda e Perondi (2009), os projetos da área espacial, em contraste com projetos que contemplam aplicações não críticas, requerem atenção especial à qualidade, pois têm como produto sistemas de alta confiabilidade, que exibem perigos tais como: perda de vidas humanas, altos custos causados pela perda de equipamentos, além de prejuízo à imagem de organizações e nações envolvidas com o empreendimento.

Para Yassuda e Perondi (2009), em programas espaciais, as lições aprendidas e o conhecimento gerado têm sido integrados e consolidados em padrões de ampla aplicação. No INPE, as diretrizes para o desenvolvimento de projetos espaciais têm sido, na maioria das aplicações, baseadas no padrão ECSS.

Segundo o padrão ECCS, um projeto na área espacial engloba todos os processos associados ao planejamento e à execução do projeto, do seu início até sua conclusão, envolvendo cooperação próxima entre os diversos domínios do projeto (ECSS, 2009).

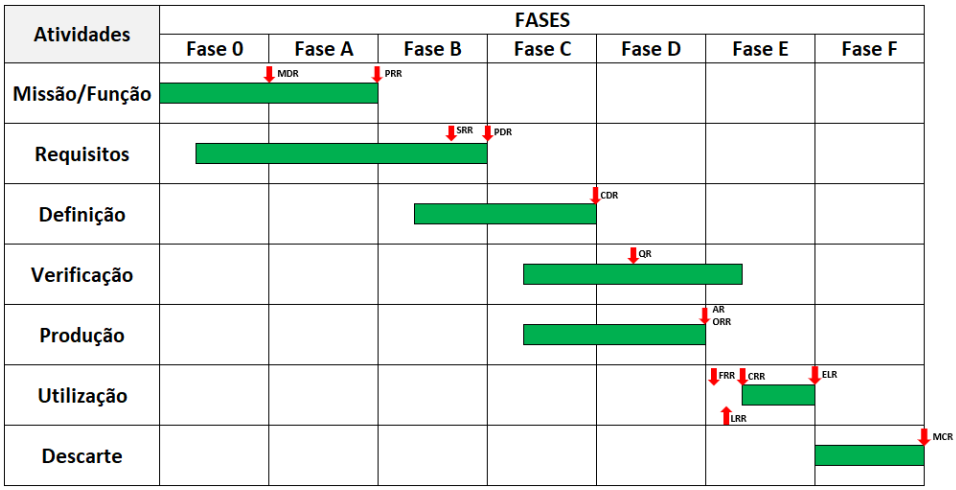
2.3 Ciclo de vida de projeto espacial

O ciclo de vida de projetos espaciais, proposto pela ECSS, apresentado na

Figura 2.2, é tipicamente dividido em sete fases, que compreendem desde a fase de identificação de necessidades, até o descarte do sistema. As fases são nominadas como segue:

- Fase 0 - Análise da missão / identificação de necessidades;
- Fase A - Viabilidade do Projeto;
- Fase B - Definição Preliminar;
- Fase C - Definição Detalhada;
- Fase D - Qualificação e Produção;
- Fase E - Operações;
- Fase F - Descarte.

Figura 2.2: Ciclo de vida de um projeto/ produto espacial.



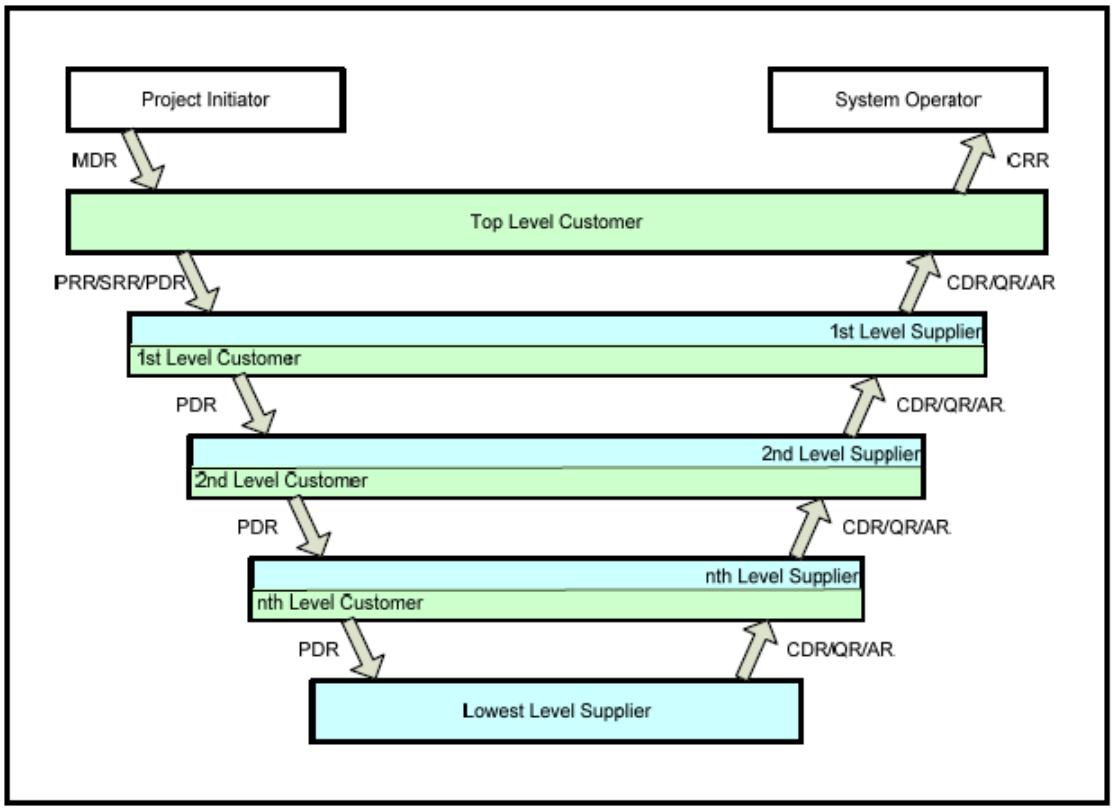
Fonte: Adaptado de ECSS (2009).

O padrão ECSS preconiza que as Fases 0, A e B foquem em: definição de requisitos funcionais e técnicos do sistema; elaboração de possíveis conceitos de sistema para cumprir a missão, tendo em conta as restrições técnicas e programáticas identificadas; identificação de atividades e recursos necessários ao desenvolvimento dos segmentos espacial, solo e lançador; avaliações iniciais de risco técnico e programático; e início de atividades de projeto preliminar (ECSS, 2009). As Fases C e D compreendem as atividades de projeto detalhado e aquelas para desenvolver, qualificar, fabricar e integrar todos os produtos dos segmentos espacial, solo e lançador. A Fase E compreende as atividades para lançar, comissionar, utilizar e manter os elementos orbitais do segmento espacial, além de utilizar e manter o segmento solo associado. A Fase F compreende as atividades para o descarte dos produtos lançados no espaço, bem como para a liberação da infraestrutura do segmento solo. (ECSS, 2009).

2.4 Revisões de projeto segundo ECSS

Ao final de cada fase do ciclo de vida do projeto, são efetuadas revisões que avaliam se o projeto pode seguir para a próxima fase. A Figura 2.3 ilustra o *review life cycle*, segundo a ECSS (ECSS, 2009).

Figura 2.3: Review Life Cycle.



Fonte: (ECSS,2009).

A mission definition review (MDR) ocorre no fim da fase 0. É divulgada a declaração de missão e identificados os requisitos de missão. Como resultado, é emitida aprovação para seguir para a fase A (ECSS, 2009).

Já a *preliminary requirements* review (PRR) ocorre no fim da fase A, com os seguintes objetivos: disponibilizar o plano preliminar de gerenciamento, assim como os planos de engenharia e de garantia do produto; disponibilizar requisitos técnicos; confirmar a viabilidade técnica e programática de conceitos de sistema (ECSS, 2009).

A fase B apresenta duas revisões principais: *a system requirements review* (SRR) e a *preliminary design review* (PDR). A SRR avalia a arquitetura (conceito) selecionada para o sistema e estabelece o programa de verificação preliminar, além de disponibilizar especificações técnicas de sistema . A PDR é realizada no final da fase B, tendo como meta verificar o projeto preliminar do conceito do sistema selecionado, liberar os planos finais de gerenciamento, bem como, a

árvore do produto e o plano de verificação incluindo a filosofia de modelos (ECSS, 2009).

A *critical design review* (CDR) ocorre no final da fase C e tem como principais objetivos avaliar o status de qualificação e validação de processos críticos; confirmar a compatibilidade com interface externas; disponibilizar o planejamento da montagem, integração e testes e o design final do sistema; liberar a fabricação, montagem e testes de software/hardware de voo; lançar o manual de usuário (ECSS, 2009).

A fase D apresenta três revisões associadas: *qualification review* (QR), *acceptance review* (AR) e *operational readiness review* (ORR). Na QR, busca-se confirmar que o processo de verificação tenha demonstrado que o design atende aos requisitos; é conferida a completude do registro de verificação e avaliada a aceitação de desvios; é emitido o dossiê “as-designed” do sistema. Na AR, os principais objetivos são: confirmar que o produto está livre de erros de fabricação; confirmar se o registro de verificação de aceitação está completo; estabelecer se os produtos estão prontos para a entrega; conferir o dossiê “as-built” do produto; verificar a aceitabilidade de desvios; autorizar a entrega do produto; e liberar seu certificado de aceitação. Já a ORR ocorre no final da fase D e tem por objetivos: verificar a prontidão para procedimentos operacionais e sua compatibilidade com o sistema de voo; apurar a prontidão das equipes de operações; e aceitar e liberar o segmento solo para operação (ECSS, 2009).

Durante a fase E, ocorrem quatro revisões: *Flight readiness review* (FRR), *Launch readiness review* (LRR), *Commissioning result review* (CRR) e *End of life review* (ELR). A FRR ocorre antes do lançamento, para verificar se os segmentos estão prontos para o lançamento. Já a LRR é realizada imediatamente antes do lançamento, com o objetivo de declarar a disponibilidade do veículo de lançamento, dos segmentos e sistemas de apoio, fornecendo, assim, a autorização para o lançamento. A CRR é realizada no final do comissionamento, após a conclusão de testes em órbita, que objetivam verificar se todos os elementos do sistema estão funcionando, e pode ser declarada a prontidão para operações e utilização. A ELR tem por objetivo verificar se a missão concluiu sua

operação e garantir que os elementos em órbita estejam configurados para o descarte seguro (ECSS, 2009).

A *mission close-out review* (MCR) é realizada ao final da fase F, a fim de garantir que todas as atividades de descarte do produto sejam concluídas adequadamente (ECSS, 2009).

2.5 Gestão de riscos e garantia da segurança de acordo com diferentes padrões.

Os processos e objetivos correspondentes a cada disciplina podem variar dentro da indústria espacial, o que justifica a disponibilidade de diferentes padrões. Esta seção apresenta uma visão geral sobre como são abordadas as disciplinas de gestão de risco e garantia da segurança em padrões e guias que cobrem a maioria das práticas da indústria.

2.5.1 PMBOK

O guia PMBOK provê orientações de gestão e define conceitos associados, descrevendo o ciclo de vida de projetos em termos de processos e atividades necessários ao gerenciamento de um projeto (PMBOK, 2017). As informações do guia estão organizadas em processos, os quais, por sua vez, encontram-se classificados em áreas de conhecimento. São quarenta e nove processos, classificados em dez áreas de conhecimento. As informações fornecidas também incluem ferramentas e técnicas para melhorar a organização e execução de projetos. A gestão de riscos é considerada como uma área de conhecimento do projeto, no contexto do guia. O guia apresenta um capítulo dedicado ao detalhamento dos processos envolvidos no gerenciamento de riscos. De acordo com o PMBOK, a gestão de riscos objetiva aumentar a probabilidade de ocorrência de eventos positivos e diminuir a probabilidade de ocorrência de eventos negativos (PMBOK, 2017).

Segundo o guia PMBOK, o risco do projeto é um evento estocástico, que, caso ocorra, apresenta um efeito positivo ou negativo em um ou mais objetivos

do projeto, como escopo, cronograma, custo e qualidade (PMBOK, 2017). A gestão de riscos, conforme o guia PMBOK, é composta dos seguintes processos:

1. planejar o gerenciamento de riscos;
2. identificar os riscos;
3. realizar análise qualitativa de risco;
4. realizar análise quantitativa de risco;
5. planejar resposta ao risco;
6. implementar resposta ao risco;
7. monitorar os riscos.

O plano de gerenciamento de riscos define e documenta as atividades de gerenciamento de riscos a serem conduzidas ao longo do ciclo de vida do projeto. Além de detalhar as atividades de gerenciamento de riscos, este processo visa garantir que os esforços do gerenciamento de riscos do projeto sejam proporcionais tanto às perdas potenciais quanto à relevância do projeto para as partes interessadas. A Figura 2.4 ilustra o processo.

Figura 2.4: Fluxograma do plano de gestão de risco.

Fonte: Adaptado de PMBOK (2017).

O processo de identificação de riscos busca identificar eventos que possam afetar o projeto e documenta suas características. Todas as partes integrantes do projeto devem ser incentivadas a identificar riscos individuais incluindo os riscos relacionados à segurança. A identificação dos riscos é

iterativa porque novos riscos podem aparecer com o avanço do projeto. A Figura 2.5 ilustra o processo

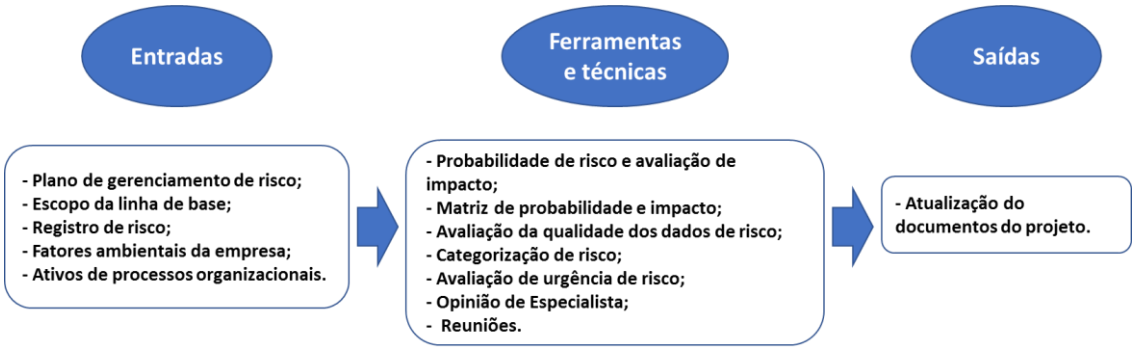
Figura 2.5: Fluxograma de identificação de riscos.

Fonte: Adaptado de PMBOK (2017).

O processo de análise qualitativa de riscos objetiva priorizar os riscos para análises ou ações adicionais, com base em estimativas da probabilidade de ocorrência de cada evento e do impacto de cada risco sobre o projeto. A Figura 2.6 ilustra o processo.

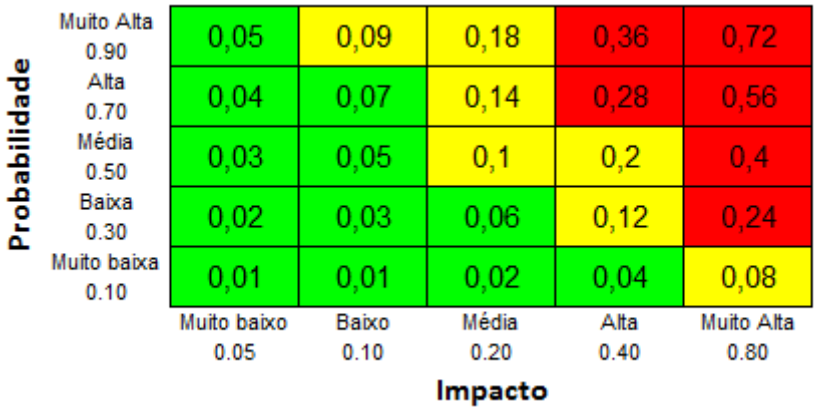
Os riscos identificados têm sua probabilidade de ocorrência e impacto nos objetivos do projeto estimados. A avaliação da probabilidade analisa a probabilidade de ocorrência de um risco específico e a avaliação do impacto analisa a extensão do efeito sobre os objetivos do projeto. Tais riscos podem ser avaliados através de entrevistas ou reuniões com membros que possuem familiaridade com os tipos de riscos abordados. Para representar os dados de tal análise, a matriz de probabilidade e impacto é usada. Ela especifica as combinações entre probabilidade e impacto e permite a hierarquização dos riscos em grupos prioritários (PMBOK,2017). Os riscos que exibem classificações predefinidas de alto nível de gravidade são inseridos no processo planejar respostas aos riscos, que visa detalhar as ações apropriadas que podem aumentar o sucesso do projeto. Os riscos ligados a segurança são riscos de alto impacto no projeto, pois são riscos associados a perda de vida humana, dano a propriedade e instalações, e danos ao meio-ambiente. A Figura 2.7 apresenta um exemplo de matriz de impacto e probabilidade.

Figura 2.6: Fluxograma da Análise Qualitativa de Riscos.



Fonte: Adaptado de PMBOK (2017).

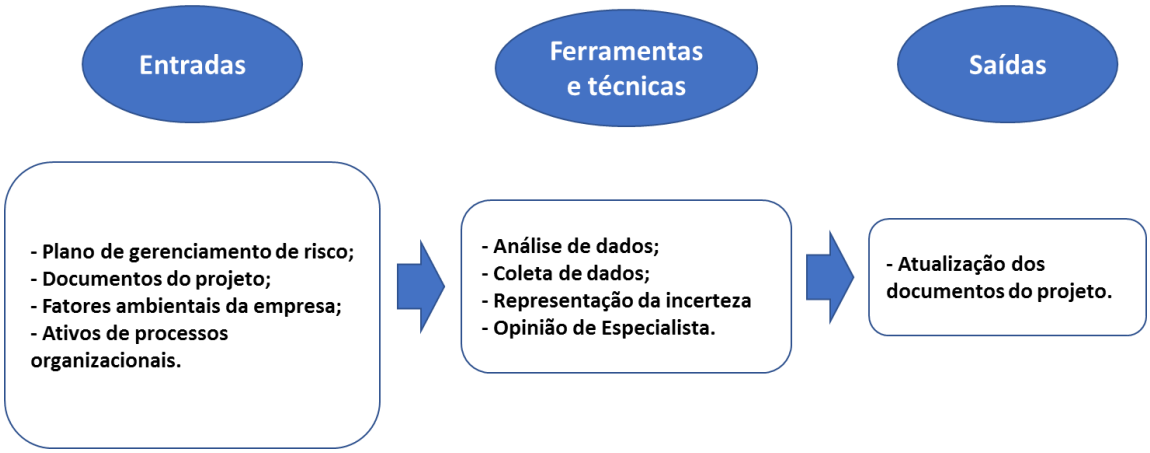
Figura 2.7: Exemplo de Matriz de Probabilidade e Impacto.



Fonte: Adaptado de PMBOK (2017).

O processo de realizar a análise quantitativa utiliza como entrada as informações geradas pela análise qualitativa. Na análise quantitativa de risco é realizada a análise numérica dos efeitos dos riscos que comprometem os objetivos do projeto para produzir as informações quantitativas de risco que ajudarão a reduzir incertezas no projeto. Durante o processo, pode-se determinar os riscos que tem o maior impacto sobre os resultados do projeto através da análise de sensibilidade e tem como principais saídas a lista priorizada de riscos individuais que representa os riscos em ordem de criticidade e a recomendação de respostas aos riscos (PMBOK,2017). A
Figura *2.8* ilustra o processo.

Figura 2.8: Fluxograma da Análise Quantitativa de Riscos.

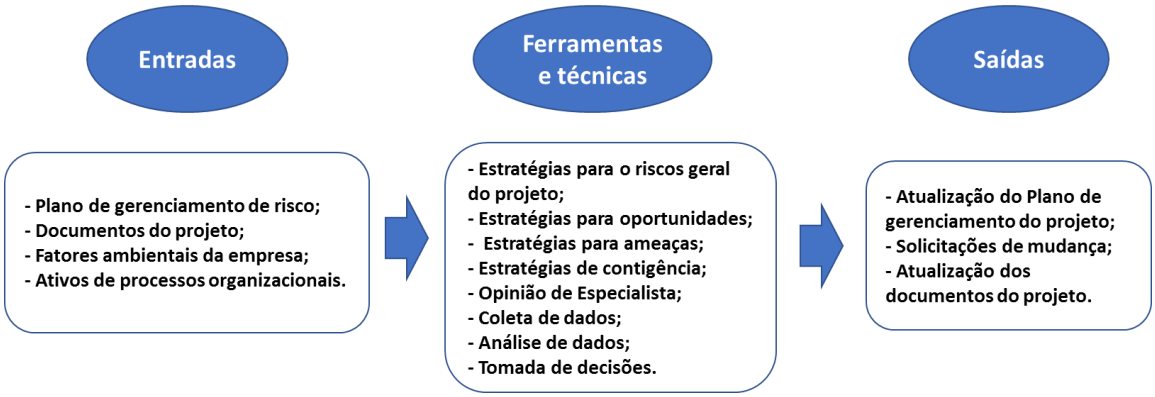


Fonte: Adaptado de PMBOK (2017).

O processo de planejamento de respostas a riscos define a estratégia e a forma de tratamento de cada risco e consequentemente como lidar com os riscos em ordem de prioridade alocando recursos conforme necessário (PMBOK, 2017). A

Figura 2.9 ilustra o processo. Após os riscos serem identificados, analisados e classificados em ordem de prioridade, deve ser planejada a resposta a cada risco individual e selecionada a estratégia de maior eficácia. Para lidar com as ameaças são consideradas cinco estratégias, escalar, prevenir, transferir, mitigar e aceitar.

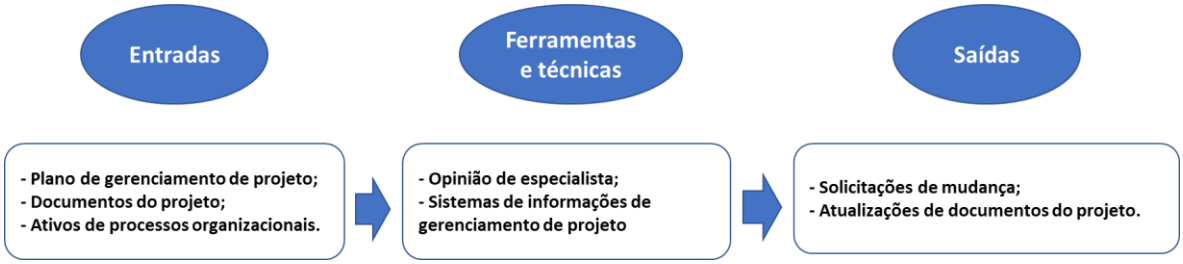
Figura 2.9: Fluxograma do Planejamento de Resposta ao Risco.



Fonte: Adaptado de PMBOK (2017).

A implementação de resposta ao risco busca garantir a execução do que foi planejado para responder adequadamente ao risco, com o objetivo de minimizar ameaças individuais e maximizar oportunidades (PMBOK, 2017). Figura 2.10 .

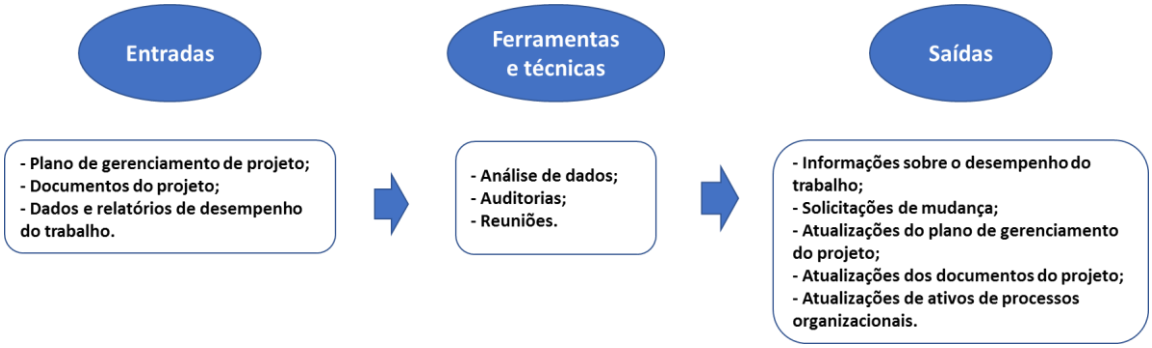
Figura 2.10: Fluxograma de Implementação de Resposta ao Risco.



Fonte: Adaptado de PMBOK (2017)

O monitoramento de risco visa monitorar a execução dos planos de resposta a riscos, através do acompanhamento de riscos já identificados e da identificação e análise de novos riscos. Tal abordagem permite que decisões do projeto sejam tomadas, tendo como base informações sempre atualizadas (PMBOK, 2017). Figura 2.11.

Figura 2.11: Fluxograma de Monitoramento do Risco.



Fonte: Adaptado de PMBOK (2017).

Em relação à garantia da segurança, o padrão PMBOK, de um lado, não aborda a certificação, testes e inspeções de produtos, projetos ou instalações, principalmente no que concerne à saúde e segurança de equipes e instalações.

Tais temas, em geral, são considerados como de responsabilidade da organização provedora de tais recursos. Por outro lado, porém, reconhece que as necessidades de um projeto podem exigir uma ou mais áreas do conhecimento adicionais, em que tanto a segurança quanto a saúde poderiam ser uma delas (PMBOK, 2017).

Assim, conclui-se que as organizações do setor espacial que adotam o guia PMBOK como referência, para o gerenciamento de projetos, devem agregar os processos de gestão da segurança ao arcabouço provido pela guia.

De acordo com o padrão PMBOK, a estrutura organizacional pode afetar a disponibilidade de recursos e a forma como os projetos são conduzidos. A Figura 2.12 ilustra as principais características das estruturas organizacionais em que são desenvolvidos os projetos em uma organização.

Figura 2.12: Influência das estruturas organizacionais em projetos.

Tipos de estrutura organizacional	Características do projeto					
	Grupos de trabalho organizados por	Autoridade do gerente do projeto	Papel do gerente do projeto	Disponibilidade de recursos	Quem gerencia o orçamento do projeto?	Pessoal administrativo de gerenciamento de projetos
Orgânico ou simples	Flexível; pessoas trabalhando lado a lado	Pouca ou nenhuma	Em tempo parcial; pode ou não ser um papel designado, como coordenador	Pouca ou nenhuma	Proprietário ou operador	Pouco ou nenhum
Funcional (centralizado)	Trabalho realizado (ex.: engenharia, fabricação)	Pouca ou nenhuma	Em tempo parcial; pode ou não ser um papel designado, como coordenador	Pouca ou nenhuma	Gerente funcional	Em tempo parcial
Multidivisional (pode replicar funções para cada divisão com pouca centralização)	Um de: produto; processos de produção; portfólio; programa; região geográfica; tipo de cliente	Pouca ou nenhuma	Em tempo parcial; pode ou não ser um papel designado, como coordenador	Pouca ou nenhuma	Gerente funcional	Em tempo parcial
Matriz – forte	Por função, com gerente do projeto como uma função	Moderada a alta	Função designada em tempo integral	Moderada a alta	Gerente do projeto	Full-time
Matrix – fraca	Função	Baixa	Em tempo parcial; feito como parte de outro trabalho e não uma função designada, como coordenador	Baixa	Gerente funcional	Em tempo parcial
Matriz – equilibrada	Função	Baixa a moderada	Em tempo parcial; incorporado nas funções como uma habilidade e pode não ser um papel designado, como coordenador	Baixa a moderada	Misto	Em tempo parcial
Orientado a projetos (composto, híbrido)	Projeto	Alta a quase total	Função designada em tempo integral	Alta a quase total	Gerente do projeto	Em tempo integral
Virtual	Estrutura de rede com nós nos pontos de contato com outras pessoas	Baixa a moderada	Em tempo integral ou parcial	Baixa a moderada	Misto	Poderia ser em tempo integral ou parcial
Híbrido	Mix de outros tipos	Mista	Misto	Mista	Misto	Misto
EGP*	Mix de outros tipos	Alta a quase total	Função designada em tempo integral	Alta a quase total	Gerente do projeto	Em tempo integral

Fonte: PMBOK (2017).

A organização funcional, ou organização por departamentos funcionais, é uma hierarquia em que cada funcionário tem um superior e cada departamento realiza seu trabalho de forma independente dos outros departamentos. Cada departamento constitui-se em uma unidade funcional especializada, tanto em áreas de conhecimento técnicas, tais como engenharia, mecânica, e elétrica, ou administrativas, tais como finanças, vendas, marketing e outras. Já as organizações matriciais são classificadas como fracas, equilibradas ou fortes, dependendo, tal classificação, do nível de relacionamento existente entre gerentes funcionais e gerentes de projeto. Em uma organização matricial fraca o

trabalho é organizado por função e o gerente do projeto tem baixa autoridade, enquanto em que uma organização matricial forte, o gerente possui uma autoridade considerável e trabalha em tempo integral no projeto. Na organização matricial equilibrada a autoridade do gerente é de baixa a moderada. Na organização projetizada, inexistem estruturas funcionais, há somente as estruturas hierárquicas de projetos, de modo que a totalidade dos recursos encontra-se alocada aos projetos (PMBOK, 2017).

Ativos de processos organizacionais são definidos, segundo o padrão PMBOK, como planos, processos, políticas, procedimentos e bases de conhecimento usados pela organização. Podem ser agrupados em duas categorias: (1) processos e procedimentos e (2) bases de conhecimento corporativas. Dentro de processos e procedimentos, destacam-se os padrões organizacionais específicos, como as políticas de segurança e saúde e os requisitos de segurança. O guia PMBOK, assim, sugere que enquanto uma parte dos requisitos de segurança são determinados pela organização, na forma de planos e políticas de segurança, outra parte é determinada pelo projeto em questão (PMBOK, 2013).

2.5.2 AS9100

A norma AS9100 padroniza requisitos do sistema de gestão da qualidade para organizações que projetam, desenvolvem ou fornecem produtos e serviços no ramo de aviação, espaço e defesa (SAE, 2016).

Dentre os potenciais benefícios para as organizações que implementam um sistema de qualidade baseado na norma AS9100 está o de buscar fornecer produtos com performance superior em termos de qualidade, custo e prazo, através tanto da eliminação de requisitos únicos a uma dada organização, quanto pela adoção de melhores práticas em sua estrutura geral de produção (SAE, 2016 p. 49).

Ao contrário do guia PMBOK, a norma AS9100 não está estruturada em termos de áreas de conhecimento e processos, mas em termos de requisitos para o sistema de qualidade de uma organização. Cabe à organização definir os

processos do sistema de gestão da qualidade e sua operacionalização, atendendo os requisitos do padrão.

Os requisitos constantes da norma AS9100 focam, primariamente, o sistema de gestão da qualidade da organização como um todo e não aqueles de organizações temporárias, relativas, por exemplo, a projetos desenvolvidos no âmbito da organização-mãe. Observa-se que a norma enfatiza, também, que o arcabouço geral de qualidade proposto "… *se presta à padronização, mais extensa possível, de requisitos de sistemas de gestão da qualidade e pode ser utilizado por organizações em todos os níveis da cadeia cliente-fornecedor* …"[1], incluindo, portanto, projetos (SAE, 2106 p. 49). Entende-se esta afirmação da seguinte forma. A norma propõe uma abordagem por processos. Desta forma, projetos ou operações desenvolvidos no âmbito da organização são vistos, de forma geral, como um conjunto de processos. Conclui-se, assim, que as disposições previstas na norma aplicam-se, também, ao conjunto de processos que constituem os projetos e operações. Porém, de modo a deixar claro que o escopo geral da norma é a organização, o texto estabelece, ainda, que "... *os requisitos especificados neste padrão são complementares (não alternativos) àqueles do cliente e aos de carácter legal e regulatório.* …"[2], enquanto se observa que requisitos referentes ao produto ou a operações são fixados pelo usuário (SAE, 2016 p. 10).

A norma especifica requisitos para processos que são organizados em cinco grupos: liderança, planejamento, apoio e operação, avaliação de desempenho e melhoria contínua. A revisão da norma publicada em 2016 incorpora as atualizações introduzidas na última revisão da norma ISO 9001, publicada em 2015, que incluem novas áreas de conhecimento, entre estas o relacionamento com stakeholders (partes interessadas), a gestão do conhecimento, a gestão de riscos e a gestão da segurança (SIMÃO et al, 2019).

[1] Tradução livre do autor. Texto original: "… *standardizes quality management system requirements to the greatest extent possible and can be used at all levels of the supply chain by organizations …".*

[2] Tradução livre do autor. Grifo nosso. Texto original: "... *the requirements specified in this standard are complementary (not alternative) to customer and applicable statutory and regulatory requirements …".*

Os tratamentos dados à gestão de riscos e à gestão de segurança, porém, são muito diferenciados. A norma não inclui requisitos específicos a outros sistemas de gerenciamento, tais como gerenciamento ambiental, saúde ocupacional e, em particular, gestão da segurança (SAE, 2016 p. 9).

Referências à gestão de segurança, contrariamente ao caso da gestão de riscos, não são explícitas na definição de requisitos e apresentam-se com caráter informativo, com a exceção de que no *projeto, desenvolvimento e uso do produto* há o requisito de que seja planejada a segurança do produto, atendendo requisitos do gerenciamento de segurança da organização, bem como aqueles advindos de demandas legais e regulatórias. Especificamente, a norma requer que *"… A organização deverá planejar, implementar e controlar os processos necessários à garantia da segurança do produto durante o ciclo de vida completo do produto, atendendo requisitos da organização e do próprio produto* …"[3] (SAE, 2016 p. 23). Cita os seguintes processos como exemplos associados à garantia da segurança:

- a avaliação de perigos e gerenciamento dos riscos associados;
- a gestão de itens críticos de segurança;
- a análise e relatórios informativos acerca de eventos ocorridos que afetam a segurança;
- a comunicação destes eventos e treinamento de pessoas.

Projetos desenvolvidos no âmbito da organização são tratados como um conjunto de processos, planejados e desenvolvidos com o fim específico de prover um dado produto ou serviço (SAE, 2016 p. 15). Conforme a norma, no planejamento de tais processos, uma das primeiras tarefas consiste na determinação dos requisitos do produto e objetivos da qualidade, que inclui considerações, entre outras, acerca da segurança do produto e de equipes (SAE, 2016 p. 15).

A última versão da norma introduz o conceito de "*risk-based thinking*" (pensamento ou avaliação baseados em risco). Para um sistema de gestão da

[3] Tradução livre do autor. Texto original: "*The organization shall plan, implement, and control the processes needed to assure product safety during the entire product life cycle, as appropriate to the organization and the product "*.

qualidade eficaz é essencial o pensamento baseado em risco, pois permite que a organização acompanhe os fatores que podem causar desvios do resultado planejado. No planejamento do sistema de gestão da qualidade a organização deve levar em consideração os riscos e oportunidades, onde as opções para lidar com os riscos podem incluir: evitar riscos; assumir riscos a fim de buscar uma oportunidade; eliminar a fonte de risco; alterar a probabilidade ou consequências; compartilhar o risco ou reter o risco por decisão informada. (SAE, 2016)

Em relação à gestão de riscos fica claro que a organização deve planejar, implementar um processo de gerenciamento de riscos, mas limita essa abordagem aos riscos associados a processos operacionais. Para tal, a organização deve atribuir responsabilidades pela gestão do risco operacional; definir critérios de avaliação de risco (por exemplo, probabilidade, consequências, aceitação de risco); identificar, avaliar e comunicar os riscos em todas as operações; implementar ações para mitigar riscos que excedem o critério de aceitação definido e aceitar os riscos remanescentes após a implementação de ações de mitigação (SAE,2016). Durante o planejamento e o controle operacional a organização deve considerar a segurança de pessoas e do produto.

Os riscos que afetam um projeto em uma organização podem ser classificados quanto à sua natureza, em sentido amplo, conforme apresentado na Tabela *2.1*. A primeira coluna apresenta a instância em que o risco é tratado, enquanto a segunda coluna apresenta uma breve caracterização do risco. Enquanto o processo de gestão de riscos realizado na instância de projeto deve lidar com os riscos técnicos do sistema e os riscos de gestão de projetos, aquele realizado na instância da organização deve lidar com os riscos dos processos da organização.

Tabela 2.1: Riscos típicos que afetam um projeto em uma organização.

Instância	Caracterização do Risco
Projeto do sistema	riscos que afetam o sistema desenvolvido durante seu ciclo de vida (riscos técnicos, riscos de operações do sistema)
Gestão de projeto	riscos que afetam os aspectos gerenciais do projeto (custo, cronograma, *stakeholders*, fornecedores)
Organização	riscos que afetam a operação da organização (processos organizacionais, uso de instalações, normas gerais aplicáveis à riscos institucionais)

Fonte: Produção da Autora

Na Tabela *2.2* e Tabela *2.3* encontram-se listados os requisitos referentes à gestão de riscos e garantia de segurança abordados na norma, assim como sua caracterização de acordo com a Tabela *2.1*.

.

Tabela 2.2: Requisitos de Gestão de Risco segundo AS9100.

Requisito Relativos à Gestão de Riscos	Instância
5 Liderança	
5.1 Liderança e Compromisso	
5.1.2 Foco no Cliente	
A alta administração deve demonstrar liderança e compromisso com relação ao foco no cliente, garantindo que: b) os riscos e oportunidades que podem afetar a conformidade de produtos e serviços e a capacidade de melhorar o cliente a satisfação é determinada e tratada;	**Projeto do sistema** **Gerenciamento de Projetos** **Organização**
6 Planejamento	
6.1 Ações para lidar com riscos e oportunidades	
6.1.1 Ao planejar o sistema de gestão da qualidade, a organização deve considerar as questões referidas em 4.1 e determinar os riscos e oportunidades que precisam ser abordados para: a) Dar garantia de que o sistema de gestão da qualidade pode atingir os resultados pretendidos; b) Aumentar os efeitos desejáveis; c) Prevenir ou reduzir os efeitos indesejáveis; d) Alcançar a melhoria.	**Organização**
6.1.2 A organização deve planejar: a) Ações para lidar com esses riscos e oportunidades; b) Como: 1. integrar e implementar as ações em seus processos de sistema de gestão da qualidade (ver 4.4); 2. avaliar a eficácia dessas ações. c) As ações tomadas para enfrentar os riscos e oportunidades devem ser proporcionais ao potencial impacto sobre a conformidade dos produtos e serviços.	**Organização**
8. Operação	
8.1 Planejamento e Controle Operacional	
a) Conforme apropriado para a organização, requisitos do cliente e produtos e serviços, a organização deve planejar e gerenciar o fornecimento de produtos e serviços de forma estruturada e controlada, incluindo eventos programados realizados em uma sequência planejada para atender aos requisitos com risco aceitável, dentro dos recursos e cronograma restrições.	**Gerenciamento de Projetos** **Organização**
b) A organização deve estabelecer, implementar e manter um processo para planejar e controlar a transferência temporária ou permanente de trabalho, para garantir a supervisão contínua do trabalho com os requisitos. O processo deve garantir que os riscos e riscos da transferência de trabalho sejam gerenciados.	**Gerenciamento de Projetos (Fornecedores)**

continua

Tabela 2.2 – Continuação.

Requisito Relativos à Gestão de Riscos	Instância
8.1.1 Gestão de Risco Operacional	
A organização deve planejar, implementar e controlar um processo de gestão de riscos operacionais para o cumprimento dos requisitos aplicáveis, que incluem, os seguintes produtos e serviços: a) Atribuição de responsabilidades pela gestão do risco operacional b) Definição de critérios de avaliação de risco (por exemplo, probabilidade, consequências, aceitação de risco); c) Identificação, avaliação e comunicação de riscos em todas as operações; d) Identificação, implementação e gestão de ações para mitigar riscos que excedem os critérios de aceitação definidos; e) Aceitação dos riscos remanescentes após a implementação das ações mitigadoras.	**Gerenciamento de Projetos** **Organização**
8.2 Requisitos para produtos e serviços	
8.2.2 Determinando os Requisitos para Produtos e Serviços	
Ao determinar os requisitos para os produtos e serviços a serem oferecidos aos clientes, a organização deve garantir que: a. os requisitos para os produtos e serviços são definidos, incluindo: 1. quaisquer requisitos estatutários e regulamentares aplicáveis; 2. aqueles considerados necessários pela organização;	**Projeto do sistema** **Gerenciamento de Projetos** **Organização**
b. a organização pode atender às demandas dos produtos e serviços que oferece;	**Projeto do sistema** **Gerenciamento de Projetos** **Organização**
c. requisitos especiais dos produtos e serviços são determinados;	**Projeto do sistema** **Gerenciamento de Projetos** **Organização**
d. riscos operacionais (por exemplo, nova tecnologia, capacidade e capacidade de fornecer, prazo de entrega curto) foram identificados.	**Projeto do sistema** **Gerenciamento de Projetos** **Organização**
8.4 Controle de processos, produtos e serviços fornecidos externamente	
8.4.1 Geral	
A organização deve assegurar que os processos, produtos e serviços fornecidos externamente estejam em conformidade com os requisitos.	**Gerenciamento de Projetos (Fornecedores)**
A organização deve identificar e gerenciar os riscos associados ao fornecimento externo de processos, produtos e serviços, bem como a seleção e uso de fornecedores externos.	**Gerenciamento de Projetos (Fornecedores)**

continua

Tabela 2.2 – Continuação.

Requisito Relativos à Gestão de Riscos	Instância
8.4.2 Tipo e extensão de Controle	
A organização deve assegurar que os processos, produtos e serviços fornecidos externamente não afetem adversamente a capacidade da organização de entregar consistentemente produtos e serviços em conformidade aos seus clientes.	**Gerenciamento de Projetos (Fornecedores)**
As atividades de verificação de processos, produtos e serviços fornecidos externamente devem ser realizadas de acordo com os riscos identificados pela organização. Isso deve incluir inspeção ou testes periódicos, conforme aplicável, quando houver alto risco de não-conformidades, incluindo peças falsificadas.	**Gerenciamento de Projetos (Fornecedores)**
Quando relatórios de teste de fornecedores externos são utilizados para verificar produtos fornecidos externamente, a organização deve implementar um processo para avaliar os dados nos relatórios de teste para confirmar se o produto atende aos requisitos. Quando um cliente ou organização identificou a matéria-prima como um risco operacional significativo (por exemplo, itens críticos), a organização deve implementar um processo para validar a precisão dos relatórios de teste.	**Gerenciamento de Projetos (Fornecedores)**
8.5 Produção e Prestação de Serviços	
8.5.1 Controle de Produção e Prestação de Serviços	
A organização deve implementar a produção e o fornecimento de serviços sob condições controladas.	**Gerenciamento de Projetos (Fornecedores)**
8.5.1.3 Verificação do Processo de Produção	
A organização deve implementar atividades de verificação do processo de produção para garantir que o processo de produção seja capaz de produzir produtos que atendam aos requisitos. Essas atividades podem incluir avaliações de risco dentre outras.	**Projeto do sistema Gerenciamento de Projetos**
9 Gestão de Risco Operacional	
9.1 Monitoramento, Medição, Análise e Avaliação	
9.1.3 Análise e Avaliação	
A organização deve analisar e avaliar os dados e informações apropriados oriundos do monitoramento e da medição. Um sucesso das ações recuperadas para lidar com riscos e oportunidades. Os resultados da análise devem ser usados para avaliar: e) A eficácia das ações tomadas para lidar com riscos e oportunidades;	**Projeto do sistema Gerenciamento de Projetos Organização**

Continua

Tabela 2-2 – Conclusão.

Requisito Relativos à Gestão de Riscos	Instância
9.3 Revisão de Gerenciamento	
9.3.2 *Inputs* da Revisão de Gerenciamento	
A análise crítica da gestão deve ser planejada e realizada levando em consideração: e) A eficácia das ações tomadas para lidar com riscos e oportunidades (ver 6.1);	**Projeto do sistema Gerenciamento de Projetos Organização**
93.3 Resultados da Revisão de Gerenciamento	
As saídas da análise crítica da gestão devem incluir decisões e ações relacionadas a: d) Riscos identificados.	**Projeto do sistema Gerenciamento de Projetos Organização**
10 Melhoria	
10.2 Não Conformidade e Ação Corretiva	
10.2.1 Quando ocorrer uma não conformidade, incluindo qualquer decorrente de reclamações, a organização deve: e) Atualizar riscos e oportunidades determinados durante o planejamento, se necessário;	**Projeto do sistema Gerenciamento de Projetos Organização**

Fonte: Produção da autora.

Tabela 2.3: Requisitos referentes a Garantia da Segurança segundo AS9100.

Requisito Relativos à Garantia da Segurança	Instância
7 *Support*	
7.3 *Awareness*	
A organização deve garantir que as pessoas que realizam trabalhos sob o controle da organização estejam cientes de: g) Sua contribuição para a segurança do produto;	**Gerenciamento de Projetos** **Organização**
8 Operação	
8.1 Planejamento e Controle Operacional	
A organização deve planejar, implementar e controlar os processos necessários para o fornecimento de produtos e serviços, a determinação dos requisitos para os produtos e serviços deve incluir: a) Segurança pessoal e do produto	**Gerenciamento de Projetos** **Organização**
8.1.3 Segurança do Produto	
A organização deve planejar, implementar e controlar os processos necessários para garantir a segurança do produto durante o ciclo de vida completo do produto, conforme apropriado para a organização e o produto. Esses processos incluem: a) Avaliação dos perigos e gestão dos riscos associados (ver gestão de risco operacional) b) Gerenciamento de itens críticos de segurança c) Análise e relatório de eventos ocorridos que afetam a segurança d) Comunicação desses eventos e treinamento de pessoas.	**Projeto do sistema** **Gerenciamento de Projetos** **Organização**
8.3.3 *Inputs* de projeto e desenvolvimento	
A organização deve determinar os requisitos essenciais para os tipos específicos de produtos e serviços a serem projetados e desenvolvidos. A organização deve considerar: e) Consequências potenciais de falha devido à natureza dos produtos e serviços	**Projeto do sistema** **Gerenciamento de Projetos**
8.5 Produção e prestação de serviços	
8.5.4 Preservação	
A organização deve preservar os resultados durante a produção e a prestação de serviços, a preservação pode incluir: a) Identificação, manuseio, controle de contaminação, embalagem, armazenamento, transmissão ou transporte e proteção. A preservação dos resultados também deve incluir, quando aplicável de acordo com as especificações e aplicáveis requisitos estatutários e regulamentares, disposições para: a) limpeza; b) Prevenção, detecção e remoção de objetos estranhos; c) Manuseio e armazenamento especiais para produtos sensíveis; d) Marcação e rotulagem, incluindo avisos e precauções de segurança; e) Controle de vida útil e rotação de estoque; f) Manuseio especial e armazenamento de materiais perigosos.	**Organização**

continua

Tabela 2.3: Conclusão.

Requisito Relativos à Garantia da Segurança	Instância
7 *Support*	
7.3 *Awareness*	
A organização deve garantir que as pessoas que realizam trabalhos sob o controle da organização estejam cientes de: g) Sua contribuição para a segurança do produto;	**Gerenciamento de Projetos** **Organização**
8 Operação	
8.1 Planejamento e Controle Operacional	
A organização deve planejar, implementar e controlar os processos necessários para o fornecimento de produtos e serviços, a determinação dos requisitos para os produtos e serviços deve incluir: a) Segurança pessoal e do produto	**Gerenciamento de Projetos** **Organização**
8.1.3 Segurança do Produto	
A organização deve planejar, implementar e controlar os processos necessários para garantir a segurança do produto durante o ciclo de vida completo do produto, conforme apropriado para a organização e o produto. Esses processos incluem: a) Avaliação dos perigos e gestão dos riscos associados (ver gestão de risco operacional) b) Gerenciamento de itens críticos de segurança c) Análise e relatório de eventos ocorridos que afetam a segurança d) Comunicação desses eventos e treinamento de pessoas.	**Projeto do sistema** **Gerenciamento de Projetos** **Organização**
8.3.3 *Inputs* de projeto e desenvolvimento	
A organização deve determinar os requisitos essenciais para os tipos específicos de produtos e serviços a serem projetados e desenvolvidos. A organização deve considerar: e) Consequências potenciais de falha devido à natureza dos produtos e serviços	**Projeto do sistema** **Gerenciamento de Projetos**
8.5 Produção e prestação de serviços	
8.5.4 Preservação	
A organização deve preservar os resultados durante a produção e a prestação de serviços, a preservação pode incluir: a) Identificação, manuseio, controle de contaminação, embalagem, armazenamento, transmissão ou transporte e proteção. A preservação dos resultados também deve incluir, quando aplicável de acordo com as especificações e aplicáveis requisitos estatutários e regulamentares, disposições para: a) limpeza; b) Prevenção, detecção e remoção de objetos estranhos; c) Manuseio e armazenamento especiais para produtos sensíveis; d) Marcação e rotulagem, incluindo avisos e precauções de segurança; e) Controle de vida útil e rotação de estoque; f) Manuseio especial e armazenamento de materiais perigosos.	**Organização**

Fonte: Produção da autora.

2.5.3 INCOSE

O INCOSE possui um manual de engenharia de sistemas, em que define a disciplina e a prática de engenharia de sistemas. O objetivo do *Systems Engineering Handbook* (SEH) é descrever as principais atividades e processos de engenharia de sistema no contexto de projeto, provendo uma referência para entender a disciplina em termos de conteúdo e prática (INCOSE, 2015).

O manual SEH propõe um conjunto de trinta processos de engenharia de sistemas, organizados em quatro áreas de conhecimento: Processos Técnicos, Processos de Gestão Técnica, Processos de Acordo e Processos de Habilitação de Projetos Organizacionais. O guia fornece diretrizes e requisitos gerais para cada um dos trinta processos de engenharia de sistema propostos. Enquanto o processo de Gestão de Riscos é tratado como um dos trinta processos, acima referidos, classificado sob a área de conhecimento de Processos de Gestão Técnica, o processo de gestão da segurança não é tratado explicitamente no manual. As diretrizes gerais relacionadas ao gerenciamento de segurança são fornecidas em uma seção especial intitulada Atividades de Engenharia Especializada, sob o título Engenharia de Segurança do Sistema.

O manual adota *a* definição de risco da norma ISO 73:2009 que define risco como sendo o efeito da incerteza sobre os objetivos do projeto. Cita, ainda, que os objetivos podem ter diferentes naturezas como custo, saúde, segurança e ambiental. O risco é expresso através de uma combinação das consequências de um evento e sua probabilidade de ocorrência (INCOSE, 2015, p 114).

Segundo o manual, gestão de risco é uma abordagem disciplinada e estruturada para lidar com as incertezas que incidem sobre os objetivos gerais de um projeto, que podem ter naturezas distintas, tais como custo, prazo, saúde, segurança e meio ambiente, e podem se aplicar a diferentes níveis, como projeto, produto e processos. Tal abordagem deve ser executada durante todo o ciclo de vida do sistema. A proposta de considerar oportunidades e resultados positivos como escopo adicional do processo de gerenciamento de riscos de projetos tem ganho popularidade entre alguns círculos de profissionais, recentemente (INCOSE, 2015, p. 114; PMBOK, 2017). A edição atual do SEH incorpora essa visão.

Os processos de gestão de risco, segundo o manual do INCOSE, incluem uma priorização de riscos, onde riscos com maior impacto e maior probabilidade de ocorrência recebem prioridade de tratamento. (INCOSE, 2015) A Figura 2.13 Ilustra o processo segundo o INCOSE.

Figura 2.13: Processo de gestão de riscos segundo INCOSE.

Fonte: Adaptado de INCOSE (2015)

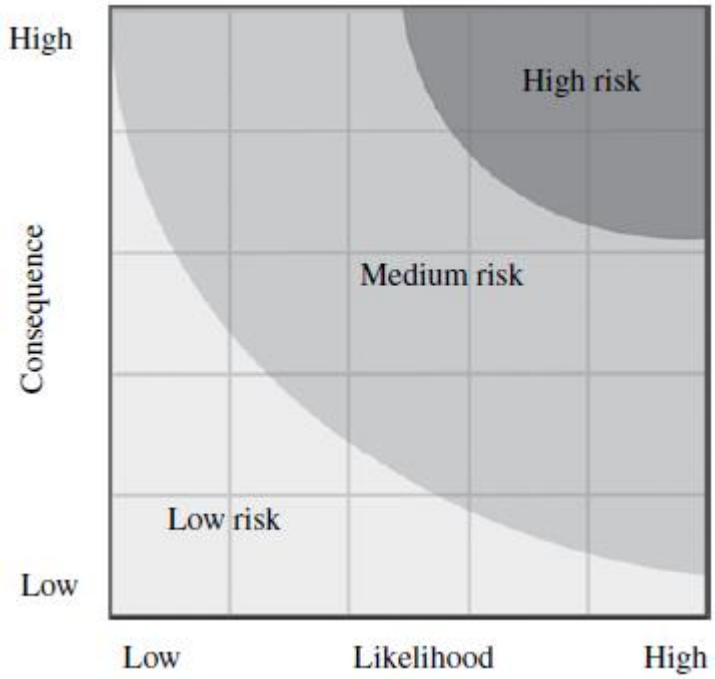
Em linhas gerais, a primeira atividade, plano de gerenciamento de riscos, trata da definição e documentação da estratégia geral de risco, enquanto a segunda, gerenciar o perfil de riscos, trata da definição de elementos de avaliação e classificação, como perfis de risco, limites para riscos aceitáveis e inaceitáveis e estratégias de resposta. Durante a terceira atividade, analisar os riscos, os riscos são identificados, classificados e priorizados, conforme sua magnitude, a partir de estimativas de impacto sobre o projeto e de probabilidade de ocorrência. Essa avaliação pode ser realizada através de métodos de análise qualitativa e quantitativa. A criticidade do risco é medida pela probabilidade de ocorrência e consequência do evento associado (INCOSE, 2015). A Figura 2.14 mostra um exemplo de escala para a categorização da criticidade de riscos.

Em geral, para os riscos que se enquadram nas classificações "Alto Risco" e "Médio Risco" são definidos planos e estratégias para o seu tratamento. Normalmente, os riscos classificados como "Baixo risco" não são considerados críticos e, portanto, não recebem nenhuma ação adicional. Durante a etapa de "tratar riscos", para cada risco que se enquadra em um nível de classificação relevante, é definindo um responsável pelo seu monitoramento e pela

implementação das ações associadas. As estratégias propostas pelo manual para o tratamento de riscos são como segue (INCOSE, 2015, p. 120): (i) evitar o risco por meio da mudança de requisitos ou do redesenho, (ii) aceitar o risco e fazer não mais, (iii) controlar o risco para reduzir a probabilidade e consequência, e (iv) transferir o risco por acordo com outra parte. Por fim, na última etapa, “monitorar risco”, o plano de risco é operacionalizado, tendo sua execução documentada e controlada.

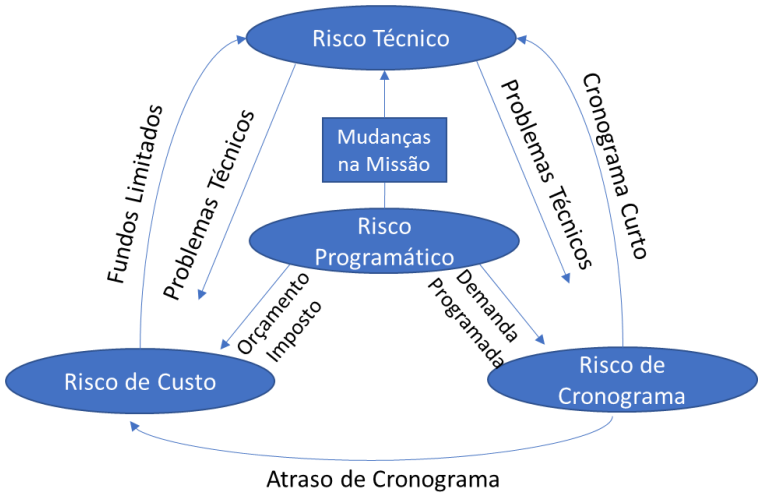
O manual aborda quatro categorias de riscos: programático, cronograma, custo e técnico. O mesmo risco pode ser classificado em mais de uma categoria. Por exemplo, os riscos na categoria de custo podem estar associados a recursos para suprir outros domínios do projeto, como por exemplo, quando o projeto possui cronogramas atrasados e se faz necessário o investimento de recursos que não estavam previstos para compensar atrasos. (INCOSE, 2015) Essa interação entre as quatro categorias de risco está ilustrada na Figura 2.15.

Figura 2.14: Definição do nível de risco.



Fonte: INCOSE (2015).

Figura 2.15: Relação típica entre as categorias de risco.



Fonte: Adaptado de INCOSE (2015).

O manual SEH define risco de segurança como qualquer circunstância que conduza a condições indesejáveis do sistema, resultando em danos ao sistema, a humanos envolvidos nas operações e suporte do sistema ou ao meio ambiente (INCOSE, 2015, p 231).

No que se refere à engenharia de segurança do sistema, o manual considera que o cerne da engenharia de segurança de sistemas concentra-se na análise de requisitos técnicos do sistema, abrangendo cada elemento, e cada comportamento macro a micro, no contexto do sistema, a fim de identificar, eliminar ou controlar riscos de segurança (INCOSE, 2015, p 231).

No que tange ao papel da engenharia de sistemas na segurança do sistema, o manual SEH preconiza pré-ações na organização do projeto de forma a garantir que as metas de segurança de sistema sejam incluídas no planejamento, assim como, incorporar o esforço de engenharia de segurança do sistema em processos de engenharia desde o início do projeto, para que a segurança possa ser projetada no sistema (INCOSE, 2015, p 232).

O papel da equipe de segurança é identificar os requisitos e fornecê-los à equipe de projeto (*design*). Ou seja, é função tanto da engenharia de sistemas quanto da engenharia de segurança de sistemas garantir que os requisitos e diretrizes de segurança sejam implementados no sistema (INCOSE, 2015, p 232).

As atividades de gerenciamento de segurança começam com a definição de um plano de gerenciamento de segurança. Os perigos são identificados no início da definição do conceito do sistema, normalmente no início da Fase A, e sua identificação continua ao longo de todo o ciclo de vida. A partir desse levantamento, uma análise de perigos é iniciada e atualizada ao longo do ciclo de vida de projeto. Cada perigo é analisado a fim de determinar sua gravidade e probabilidade de ocorrência, que irão determinar sua categorização, realizada através de uma matriz de avaliação de riscos. A categorização prioriza os esforços para mitigação, dando foco para os perigos considerados mais severos. O manual apresenta, como exemplo, uma matriz de avaliação de risco da MIL-STD-882E, Figura 2.16, em que os riscos são classificados como Alto, Sério, Médio, Baixo e Eliminado, de acordo com s combinação entre a severidade do evento e a probabilidade de ocorrência deste.

Figura 2.16: Matriz de avaliação de riscos.

Matriz de Avaliação de Risco				
Severidade / Probabilidade	Catastrófico (1)	Crítico (2)	Marginal (3)	Insignificante (4)
Frequente (A)	Alto	Alto	Crítico	Médio
Provável (B)	Alto	Alto	Crítico	Médio
Ocasional (C)	Alto	Crítico	Médio	Baixo
Remoto (D)	Crítico	Médio	Médio	Baixo
Improvável (E)	Médio	Médio	Médio	Baixo
Eliminado (F)	Eliminado			

Fonte: Adaptado de DOD (2012).

Uma vez que os perigos foram identificados e analisados, um sistema de rastreamento de perigos é configurado e usado para seguir o plano de ação

relativo a cada perigo, verificando o cumprimento de marcos e metas, como a implementação de requisitos de segurança, verificações e avaliação de riscos residuais. Os resultados do sistema de rastreamento de perigo são atualizados ao longo do ciclo de vida do projeto do sistema (INCOSE, 2015).

Em conclusão, o objetivo geral da gestão da segurança, conforme o manual SEH, é implantar, operar e manter um sistema que apresente um risco de segurança aceitável.

2.6 Gestão de riscos e garantia da segurança segundo ECSS, NASA e INPE

2.6.1 NASA

Para a Agência NASA, as atividades de gestão de risco são desenvolvidas tanto no âmbito da sede da Agência, quanto no de suas organizações, programas e projetos. As atividades de gestão de riscos devem ser realizadas horizontal e verticalmente, dentro de programas, projetos e organizações, para garantir uma gestão equilibrada de riscos (NASA, 2017a).

O documento NASA - *Risk Management Handbook* orienta a realização da gestão de riscos no contexto dos programas da NASA, durante o ciclo de vida do projeto. Preconiza práticas de engenharia de sistemas e orienta o usuário a efetuar a customização de métodos, conforme as características específicas do projeto (NASA, 2011b, p 1).

Para a NASA, risco é caracterizado como o potencial de um déficit de desempenho e está relacionado ao cumprimento de requisitos de desempenho estabelecidos e declarados. Déficits de desempenho podem estar relacionados ao suporte institucional, à execução da missão, ou a qualquer um ou mais dos seguintes domínios de execução da missão: segurança, técnico, custo e cronograma (Nasa, 2011b, p 3).

Os riscos são caracterizados por três elementos constituintes: (i) uma descrição do cenário em que o risco se materializa como um evento, (ii) a probabilidade de ocorrência do evento associado ao risco, e (iii) o impacto no

programa / objetivos do projeto (NASA, 2017a). A Tabela 2.4 detalha estas definições.

Tabela 2.4: Caracterização do risco no processo de gerenciamento de risco da NASA.

Cenário	o (s) cenário (s) que levam à degradação em relação a uma ou mais medidas de desempenho (por exemplo, cenários que levam a lesões, fatalidade, destruição de ativos principais; cenários que levam à ultrapassagem dos limites de massa; cenários que levam a ultrapassagem do limite do custo; cenários que levam a atrasos no cronograma)
Probabilidade	a (s) probabilidade (s) (qualitativa ou quantitativa) do (s) cenário (s) considerado (s)
Impacto	a (s) consequência (s) (gravidade qualitativa ou quantitativa da degradação do desempenho) que resultariam se o (s) cenário (s) ocorressem

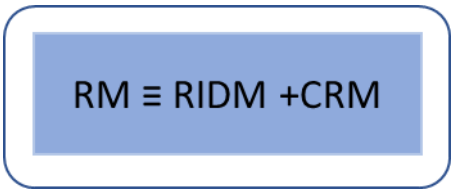
Fonte: Adaptado de NASA (2017a).

A metodologia adotada pela NASA para gerenciar os riscos é parte integrante do processo de engenharia de sistemas e tem como objetivo analisar os riscos que impactam os domínios de execução da missão (NASA, 2011b).

A abordagem da gestão de riscos preconizada pela NASA busca balancear o tratamento de riscos nos domínios da segurança e técnico com a realidade gerencial de projetos nos domínios de cronograma e custo. A implementação de uma abordagem de gestão de risco introduz custo ao projeto, sendo, assim, essencial que a abordagem seja usada de maneira econômica. Como consequência, os métodos propostos ensejam o uso de análise de forma ponderada, de modo que custos de análise possam ser controlados.

Assim, através da otimização de custos de análise, busca-se atingir uma situação em que a economia alcançada, tratando riscos antes que se tornem problemas, exceda o custo de implementação da abordagem de gestão de risco. O processo de gestão de riscos da NASA é composto por dois processos complementares: Risk-Informed Decision Making (RIDM) e Continuous Risk Management (CRM) (NASA,2011b), conforme ilustrado na Figura 2.17.

Figura 2.17: Processo de gestão de risco segundo a NASA.



Fonte: Adaptado de NASA (2011b).

O processo RIDM é desenvolvido durante o ciclo de vida do projeto e é usado para a tomada de decisões de grande repercussão, com características complexas, em que haja, por exemplo, a possibilidade de impacto significativo sobre a segurança (NASA, 2011b, p 5). As etapas do processo RIDM estão ilustradas na Figura 2.18.

A identificação de alternativas de caráter geral assenta-se na compreensão dos objetivos dos stakeholders. Estes são decompostos em uma hierarquia de alternativas específicas e quantificadas em termos de medidas de desempenho, estabelecendo uma base para a seleção de alternativas de decisão que podem ser comparadas, objetivamente, entre si. A medida de desempenho de cada alternativa é quantificada considerando as incertezas que incidem sobre a alternativa e o cumprimento dos objetivos. A seleção de uma dada alternativa é efetuada pelos stakeholders e o tomador de decisão, que seleciona o conjunto de alternativas (NASA, 2011b, p 9).

Quando aplicado à fase de design de um programa / projeto, o RIDM ajuda a garantir que as escolhas entre as alternativas sejam realizadas com base na probabilidade dos riscos associados a elas, diminuindo, assim, a possibilidade de alterações tardias no design, que podem se mostrar como fatores críticos de risco, com repercussões negativas em custos, cronograma ou, mesmo, o cancelamento do programa / projeto (NASA, 2011b).

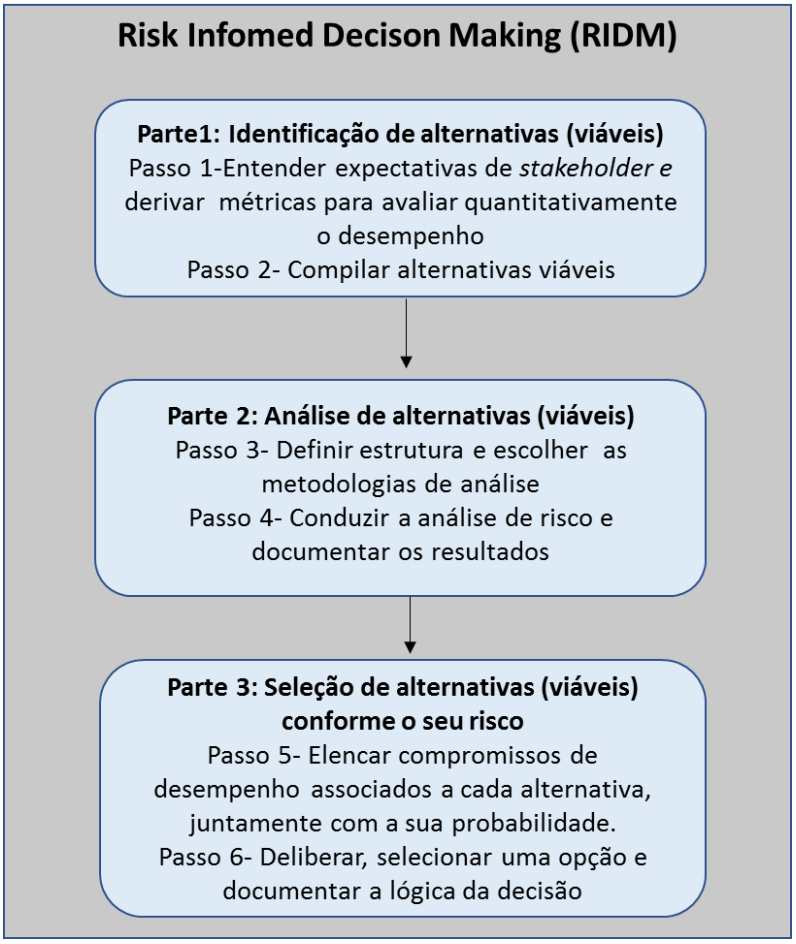
O processo CRM é aplicado após o RIDM e envolve o gerenciamento contínuo de risco para atingir os requisitos de desempenho, em todas as fases do projeto, sendo usado em qualquer nível da hierarquia organizacional da NASA (NASA, 2011b). A Figura 2.19 mostra as etapas do processo de CRM.

Na etapa de identificação, o objetivo é capturar eventos que apresentem risco ao cumprimento dos requisitos de desempenho do programa/projeto, tanto

técnico quanto programático. Na etapa de análise, estimam-se a probabilidade e a magnitude das consequências dos riscos, classificando-os por severidade. A etapa *planejar* objetiva definir as estratégias de respostas a riscos e seu planejamento de operacionalização, incluindo a definição de responsáveis pela implementação e acompanhamento. Na etapa *rastrear*, é efetuada a implementação das decisões de gestão de risco. Coletam-se e compilam-se dados para assim acompanhar o progresso da implementação. Finalmente, as ações de controle objetivam garantir que as ações planejadas são eficazes. Ações de controle são exercitadas em casos em que o rastreamento sinaliza que uma decisão não está impactando o risco como o previsto (NASA, 2011, p 16).

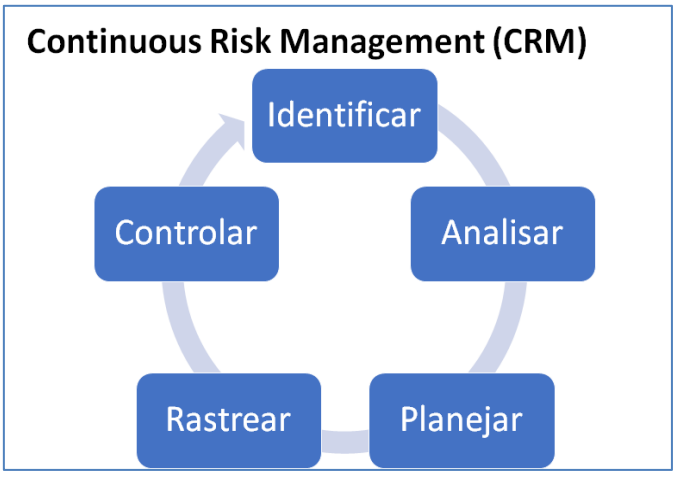
A gestão de riscos é considerada como sendo constituída pelos dois processos, RIDM e CRM, considerados como complementares. Cada unidade organizacional tem autonomia para executar o processo de RIDM, assim como efetuar o processo de CRM, a fim de gerenciar os riscos identificados. A unidade poderá transferir riscos identificados para a instância a que se subordina, caso estes extrapolem o seu escopo de responsabilidades. Os dois processos se integram à medida que os cenários que podem levar a problemas de desempenho são levantados e compilados durante o processo de RIDM e o tomador de decisão seleciona e implementa a melhor alternativa. As informações advindas do RIDM é a entrada para o processo de CRM como ilustra a Figura 2.20 (NASA, 2011b, p 23).

Figura 2.18: Etapas do processo de RIDM.



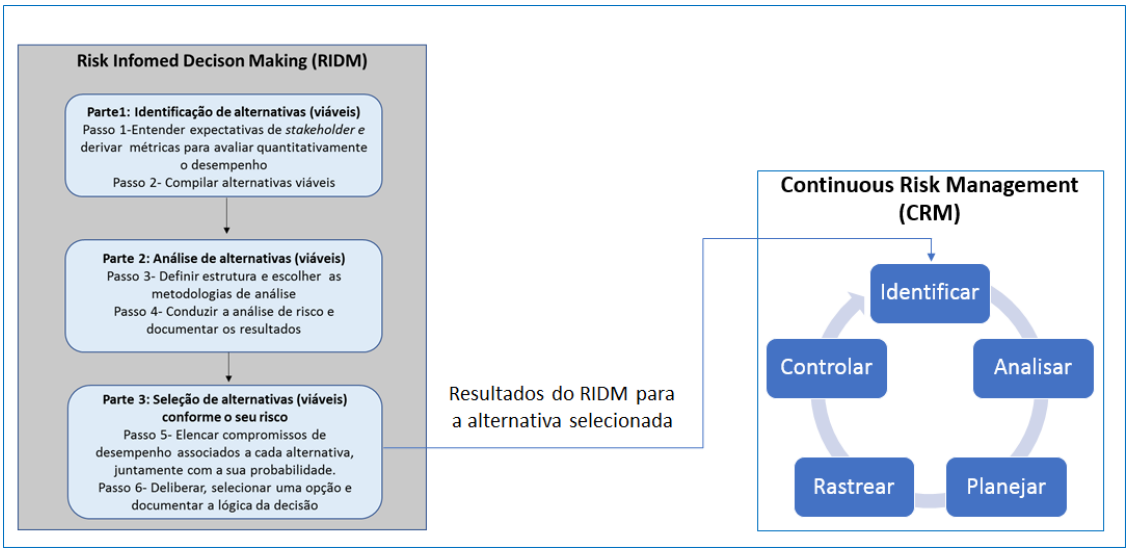
Fonte: Adaptado de NASA (2011a).

Figura 2.19: Processo de gerenciamento contínuo de risco.



Fonte: Adaptado de NASA (2011b).

Figura 2.20: Integração entre processos de RIDM e CRM.



Fonte: Adaptado de NASA (2011b).

O documento NASA-NPD 8700.1E define a Política de Segurança e Sucesso da Missão e apresenta os objetivos do programa de segurança da NASA como: (i) proteger o público, (ii) garantir a segurança da força de trabalho da NASA, (iii) proteger o meio ambiente, e (iv) evitar danos a equipamentos e propriedades de alto valor. O programa de segurança desempenha um papel fundamental em afetar positivamente a taxa de sucesso de missões e operações (NASA, 2008).

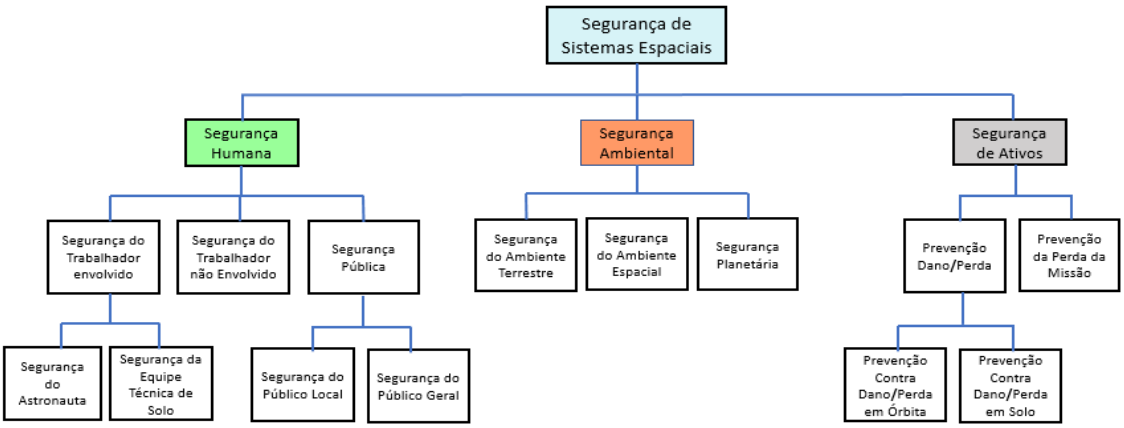
O documento *NASA system safety handbook*, dividido em dois volumes, constitui-se no manual de segurança da NASA. O primeiro volume apresenta a estrutura geral de um arcabouço de segurança de sistema e provê diretivas gerais para implementar esta estrutura, garantindo que os requisitos de segurança sejam atendidos em todas as atividades do ciclo de vida do sistema. O segundo volume fornece orientações para que se implementem estruturas de segurança de sistemas, considerando os conceitos apresentados no volume 1 (NASA, 2011a).

O programa de segurança da NASA é executado em todas as estruturas verticais e horizontais da Agência, concomitantemente (NASA, 2017). Durante a execução de um programa ou projeto, as atividades de segurança associadas são realizadas tanto na instância do programa ou projeto, quanto nas

organizações que apoiam a fabricação, integração, testes e operações do correspondente sistema espacial

De acordo com a norma MIL-STD-882D, a segurança é a capacidade de controlar, de forma planejada, aquelas condições que podem causar danos ou perda de equipamento ou propriedade, danos ao meio ambiente, danos à vida humana, representada por trabalhadores diretamente envolvidos ou não nas interações do sistema, bem como membros do público em geral (NASA, 2011a, p 3). A Figura 2.21 de Genaro (2019) foi adaptada de (NASA, 2014) ilustra as populações potencialmente impactadas a que o conceito de segurança pode ser aplicado segundo a NASA.

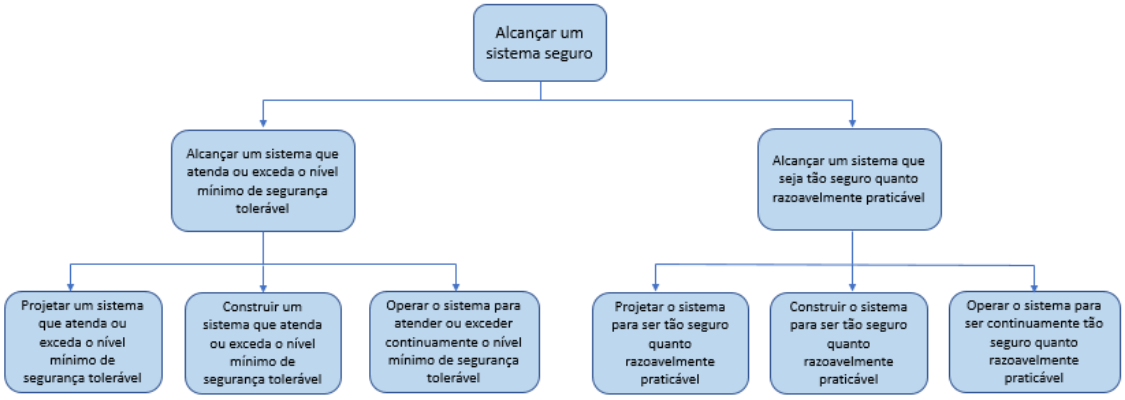
Figura 2.21: Populações Impactadas dentro do escopo de segurança



Fonte: Genaro (2019)

Conforme o padrão NASA, um sistema adequadamente seguro é um sistema que segue os dois princípios fundamentais de segurança da NASA, quais sejam: (i) o sistema deve ser (*As Safe As Reasonably Practicable*) (ASARP) e (ii) manter o nível mínimo de segurança que pode ser determinado por meio de análise, experiência operacional ou ambos, como ilustrado na Figura *2.22* (NASA, 2011a, p 4).

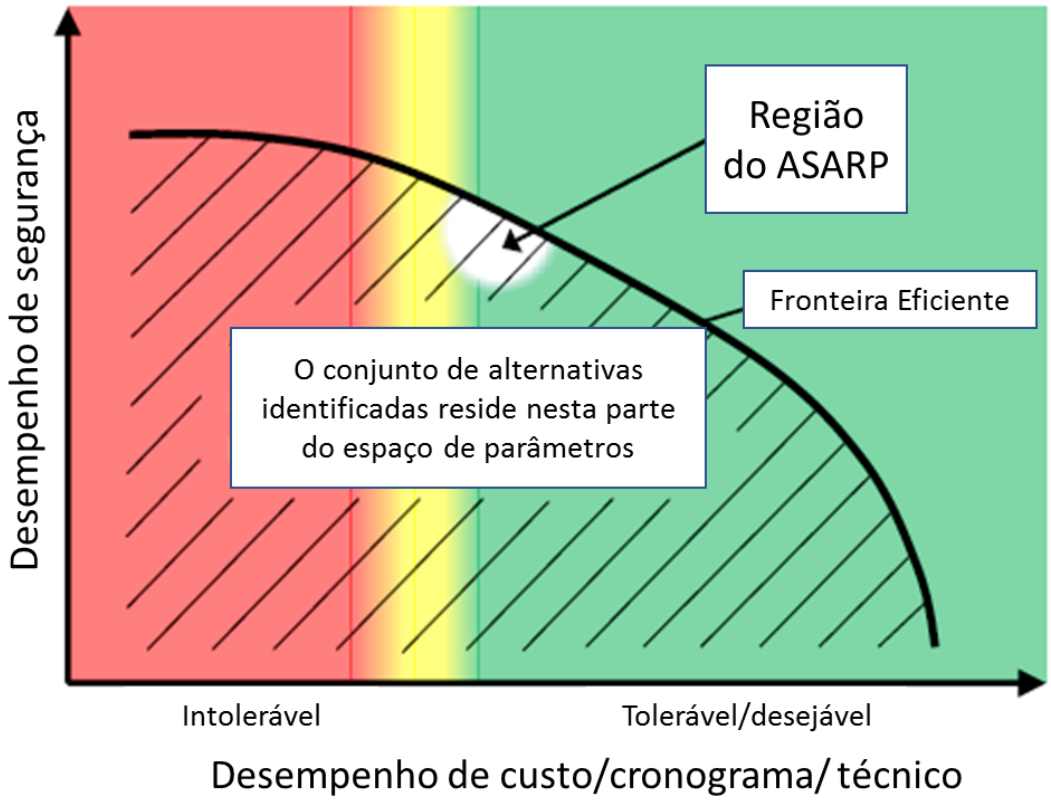
Figura 2.22: Ilustração dos dois princípios na obtenção da segurança adequada.



Fonte: Adaptado de NASA (2014).

Para a NASA, um sistema é considerado ASARP quando a melhoria contínua da segurança é prioridade, mas dentro de limites de eficácia operacional, tempo e custo, ou seja, busca-se equilibrar o nível de ganhos em segurança com o sacrifício necessário para obtê-lo, em termos de desempenho técnico, tempo e custo (NASA, 2011a, p 15). Assim, o conceito ASARP não faz referência a um máximo absoluto do desempenho de segurança de um sistema, pois considera o desempenho factível frente ao esforço necessário para obtê-lo, traduzido na forma de cenários alternativos (DEZFULI et al, 2014). A Figura 2.23 ilustra, figurativamente, o universo de cenários cujo desempenho de segurança é compatível com as restrições advindas de um ou mais dos outros domínios, quais sejam custo, cronograma e desempenho técnico (DEZFULI et al, 2014).

Figura 2.23: Ilustração do princípio ASARP ”Tão Seguro quanto Razoavelmente Praticável”.



Fonte: Adaptado de NASA (2011a).

As atividades de segurança são desempenhadas como parte integrante do processo de engenharia de sistemas e normalmente se encaixam nas categorias apresentadas a seguir (NASA,2011a, p 11):

- condução da análise de segurança integrada (ISA);
- satisfação de requisitos de segurança;
- suporte ao projeto do sistema;
- suporte ao desenvolvimento de requisitos;
- suporte ao monitoramento de desempenho;
- controle de programa e suporte a obrigações.

O conceito de análise de segurança integrada (ISA) designa a investigação sobre as possíveis falhas de segurança do sistema através da identificação e análise de cenários que possam levar a consequências de

segurança indesejadas; Tal análise de cenários pode ser qualitativa ou quantitativa. O conceito ISA integra diversos tipos de análise de segurança, como, por exemplo, FMEA (*Failure Mode and Effect Analysis*), PRA (*Probabilistic Risk Assessment*), entre outros (NASA, 2011a, p 11).

A análise de segurança integrada é ainda usada para demonstrar que os requisitos de segurança foram satisfeitos, como os que são derivados dos limites e metas de segurança da NASA, além de fornecer o suporte ao projeto do sistema, pois quanto mais cedo ele for inserido no ciclo de vida do sistema maior será a influência dele nas decisões que afetam a segurança do projeto (NASA, 2011a, p 11).

A garantia da segurança do sistema fornece o suporte para o desenvolvimento de requisitos de duas formas distintas: (i) provendo meios para cumprir os requisitos definidos para a organização e (ii) desenvolvendo a base para alocar requisitos de segurança (NASA, 2011a, p 12).

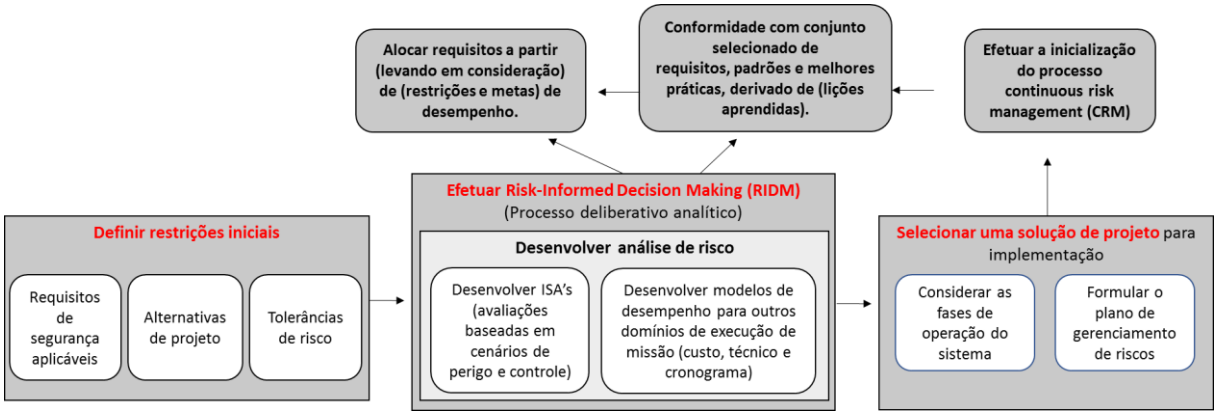
A garantia da segurança também fornece suporte para o monitoramento de desempenho, apoiando o desenvolvimento de protocolos de monitoramento e na resposta aos dados de desempenho. Para tal, a ISA é usada para estimar o risco associado aos atributos de desempenho que serão monitorados. *(NASA, 2011a,* p 12*)*

O apoio de outras áreas a obrigações cobertos pela estrutura de segurança do sistema incluem gerenciamento de configuração, garantia de qualidade, treinamento e certificação de pessoal, uso das melhores práticas e lições aprendidas além da garantia de que os requisitos estão sendo cumpridos. (NASA, 2011a, p12).

Para fins de agrupar atividades de safety, a NASA divide o ciclo da missão em quatro fases: (i) desenvolvimento de conceito e projeto inicial do sistema; (ii) o projeto detalhado do sistema; (iii) a fabricação e integração do sistema; e a (iv) operação do sistema (NASA, 2014, p 33). A Figura 2.24 apresenta as atividades de segurança no âmbito da fase de *desenvolvimento de conceito e projeto inicial do sistema*. A Figura 2.25 ilustra as atividades de segurança na fase de *projeto detalhado*, enquanto a Figura 2.26 ilustra as atividades de segurança na fase de

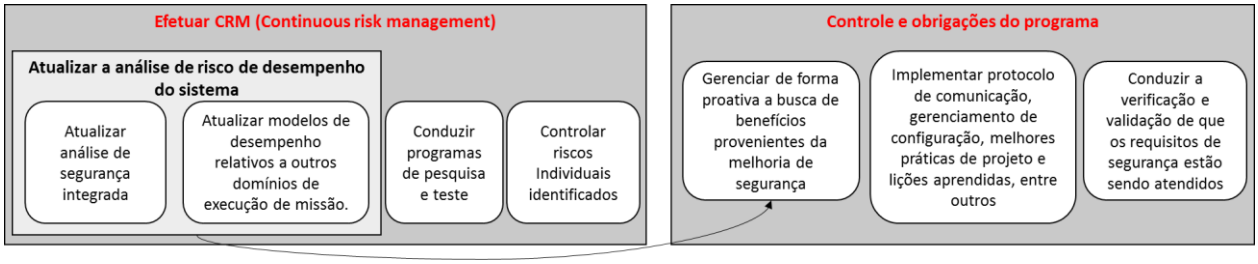
fabricação e integração do sistema. A Figura 2.27, por sua vez, mostra as atividades na fase de operação do sistema.

Figura 2.24: Principais atividades de segurança do sistema e processos relacionados durante o desenvolvimento do conceito e o projeto inicial do sistema.



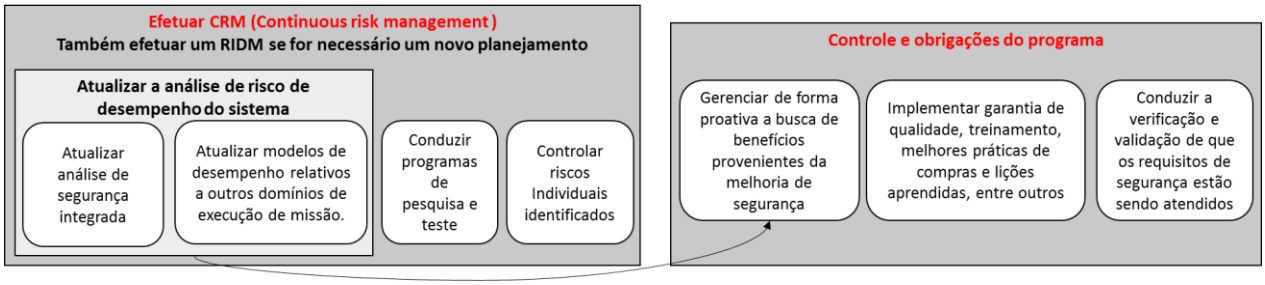
Fonte: Adaptado de NASA (2011a).

Figura 2.25: Principais atividades de segurança do sistema e processos relacionados durante o projeto detalhado do sistema.



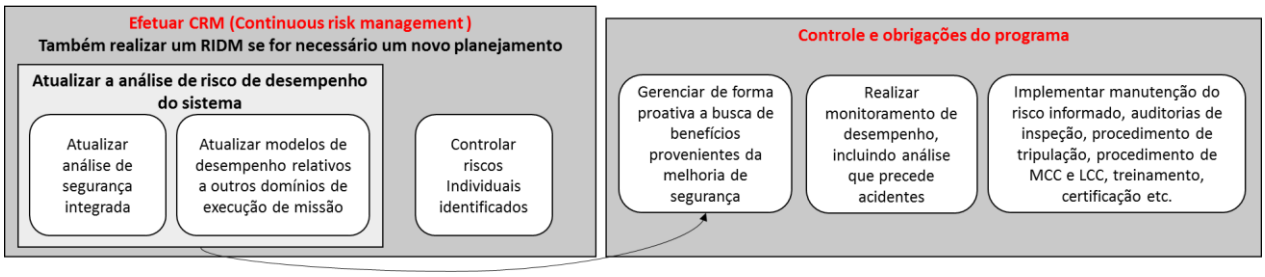
Fonte: Adaptado de NASA (2011a).

Figura 2.26: Principais atividades de segurança do sistema e processos relacionados durante a realização do sistema.



Fonte: Adaptado de NASA (2011a).

Figura 2.27: Principais atividades de segurança do sistema e processos relacionados durante a operação do sistema.



Fonte: Adaptado de NASA (2011a).

2.6.2 ECSS

A ECSS define risco como uma situação ou circunstância indesejável que tem uma probabilidade de ocorrência e uma consequência negativa potencial em relação às metas de um projeto. Os riscos são inerentes a qualquer projeto e podem surgir a qualquer momento durante o ciclo de vida do projeto (ECSS, 2012).

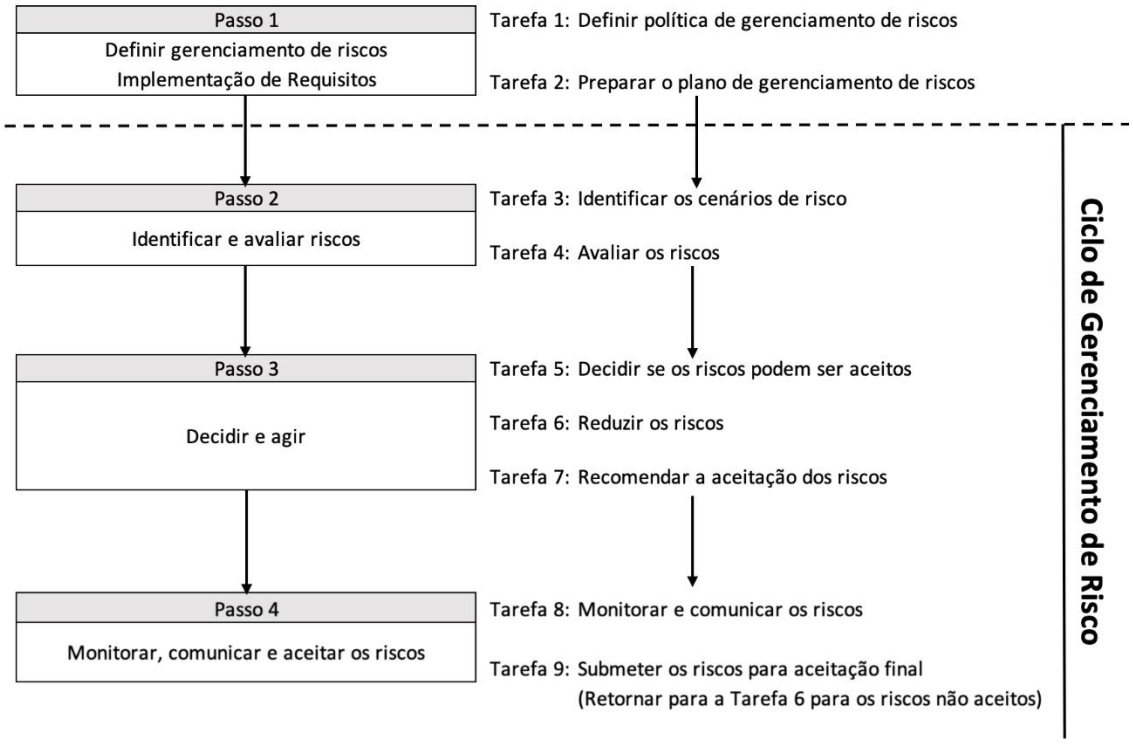
O padrão ECSS-M-ST-80C – *Space Project Management: Risk Management* define os princípios e requisitos para a gestão de riscos de um projeto, explicando como implementar uma política de gestão de riscos integrada ao projeto espacial. Conforme o padrão, o objetivo da gestão de riscos é identificar, avaliar, reduzir, aceitar e controlar os riscos de um projeto espacial de maneira sistemática, proativa, abrangente e econômica, levando em consideração as restrições técnicas e programáticas do projeto (ECSS, 2008a).

O padrão ainda define os princípios através dos quais um projeto espacial deve se pautar para fazer a gestão de riscos eficiente. Ele divide a gestão de riscos em quatro processos, cada um com suas atividades na seguinte ordem:

1 definir requisitos da implementação da gestão de riscos;
2 identificar e avaliar os riscos;
3 decidir e agir;
4 monitorar, comunicar e aceitar riscos.

A Figura 2-28 ilustra os processos da gestão de risco e suas respectivas atividades.

Figura 2-28: Tarefas associadas às etapas do processo de gerenciamento de riscos.



Fonte: Adaptado de ECSS (2012).

A primeira etapa do processo é composta pelas atividades *definição da política de gestão dos riscos* e *elaboração do plano de gestão de riscos do projeto*. A segunda etapa compreende as atividades *identificação de cenários de risco* e *avaliação dos riscos*. A etapa seguinte busca analisar a aceitabilidade dos riscos e suas opções de redução, conforme a política de gestão de riscos estabelecida, além de determinar a estratégia apropriada de redução de riscos. A última etapa é dedicada a monitorar e comunicar os riscos e aceitar os riscos. As etapas e suas respectivas atividades estão ilustradas nas Tabela 2.5, Tabela 2.6, Tabela 2.7 e Tabela 2.8.

No Apêndice A, encontra-se uma lista de requisitos referentes a gestão de riscos e garantia da segurança apresentados no padrão.

Tabela 2.5: Atividades da definição da política de gerenciamento de riscos.

Definir os requisitos de implementação da gestão de riscos	
Atividades	**Descrição**
Definição da política de gestão de riscos	• Identificação do conjunto de recursos com impacto nos riscos. • Identificação das metas do projeto e restrições de recursos. • Descrição da estratégia do projeto para lidar com riscos • Definição de esquema para classificar as metas de risco de acordo com os requisitos do projeto. • Estabelecimento de esquemas de pontuação para a gravidade das consequências e a probabilidade de ocorrência. • Estabelecimento de um esquema de índice de risco para denotar as magnitudes dos riscos dos vários cenários de risco. • Estabelecimento de critérios para determinar as ações a serem tomadas em relação a riscos de várias magnitudes. • Definição de critérios de aceitação de riscos para riscos individuais. • Estabelecimento de um método para a classificação e comparação de riscos. • Estabelecimento de um método para medir o risco geral. • Definição da estratégia para monitorar os riscos • Descrição do fluxo de revisão, decisão e implementação no projeto.
Preparar o plano de gestão de riscos	• Descrição da organização de gestão de riscos do projeto, incluindo sua função e responsabilidade. • Resumo da política de gestão de riscos. • A documentação relacionada a gestão de riscos e o conceito de acompanhamento. • O escopo da gestão de riscos ao longo da duração do projeto.

Fonte: ECSS (2008a).

Tabela 2.6: Atividades do processo de identificar e avaliar os riscos.

Identificar e Avaliar os Riscos	
Atividades	**Descrição**
Identificar Cenários de Risco	• Identificação dos cenários de risco, incluindo causas e consequências, de acordo com a política de gestão de riscos. • Identificação dos meios de alerta precoce (detecção) para a ocorrência de um evento indesejável, para evitar a propagação de consequências. • Identificação dos objetivos do projeto que se encontram em risco.
Avaliar os Riscos	• Determinação da gravidade das consequências de cada cenário de risco. • Determinação da probabilidade de cada cenário de risco. • Determinação do índice de risco para cada cenário de risco. • Utilização das fontes de informação disponíveis e aplicação de métodos adequados para apoiar o processo de avaliação. • Determinação da magnitude do risco de cada cenário de risco. • Determinação do risco geral do projeto por meio de uma avaliação dos riscos individuais identificados, suas magnitudes e interações e o impacto resultante no projeto.

Fonte: ECSS (2008a).

Tabela 2.7: Atividades do processo de Decidir e Agir.

Decidir e Agir	
Atividades	**Descrição**
Decidir se o Risco Pode ser aceito.	•Aplicação dos critérios de aceitação dos riscos. •Identificação de riscos aceitáveis.
Reduzir os Riscos	• Determinação de medidas preventivas e mitigadoras para cada risco inaceitável. • Determinação dos critérios de sucesso e falha da redução de risco. • Determinação do potencial de redução de risco de cada medida em conjunto com a otimização de recursos negociáveis. • Seleção das melhores medidas de redução de risco e decisão sobre prioridades de implementação • Verificação de redução de risco. •Identificação dos riscos que não podem ser reduzidos para um nível aceitável. • Identificação dos riscos reduzidos para os quais a redução de risco não pode ser verificada. • Identificação do potencial de redução de riscos em relação ao risco geral. • Documentação dos riscos reduzidos com sucesso em uma lista de riscos resolvidos; e os riscos reduzidos sem êxito em uma lista de riscos não resolvidos.
Recomendar Aceitação	• Opções de decisão para aceitação de riscos. • Aprovação de riscos aceitáveis e resolvidos. • Apresentação de riscos não resolvidos para ações adicionais

Fonte: ECSS (2008a).

Tabela 2.8: Atividades do processo de Monitorar, Comunicar e Aceitar riscos.

Monitorar, comunicar e aceitar riscos	
Atividades	**Descrição**
Monitorar e comunicar os riscos	• Avaliação e revisão periódica de todos os riscos identificados e atualização dos resultados após cada iteração do processo de gestão de riscos. • Identificação de mudanças nos riscos existentes e início de nova análise de risco necessária para diminuir as incertezas. • Verificação do desempenho e efeito da redução de risco correspondente. • Representação da tendência de risco ao longo da evolução do projeto, identificando como as magnitudes de risco mudaram ao longo do tempo do projeto. • Um exemplo de uma tendência de risco para riscos técnicos. • Comunicação dos riscos e da tendência de risco. • Implementação de um sistema de alerta para novos riscos.
Enviar riscos para aceitação	• Submissão dos riscos para aceitação formal de riscos pelo nível apropriado de gerenciamento. • Retornar para a atividade de reduzir os riscos para riscos não aceitos.

Fonte: ECSS (2008a).

A ECSS define segurança como um estado em que exista um nível aceitável de risco relacionados aos seguintes eventos: lesão ou doença, danos ao hardware do lançador ou a instalações do local de lançamento, danos a um elemento de um sistema de voo tripulado, funções do próprio sistema de voo, poluição do meio ambiente, atmosfera ou espaço exterior e danos à propriedade pública ou privada (ECSS, 2017a).

Segundo o padrão ECSS-Q-ST-40C – *Space product assurance: Safety*, o programa de segurança, assim como os requisitos de segurança, objetivam garantir que todos os riscos de segurança associados a projeto, desenvolvimento, produção e operações do produto espacial sejam identificados, para proteger a tripulação de voo, o veículo lançador, as cargas

úteis, equipamento e equipe de apoio no solo, público em geral e propriedade pública e privada. Os riscos de segurança devem ser adequadamente avaliados, minimizados, controlados e aceitos por meio da implementação de um programa de garantia de segurança (ECSS, 2017a).

O padrão ECSS-ST-40C preconiza que a execução de atividades perigosas esteja condicionada à aprovação do responsável de segurança, após análise e revisão (ECSS, 2017a). O padrão ainda determina que a função de segurança tenha um representante em todos os assuntos que envolvam requisitos de segurança e funções críticas de segurança. Por exemplo, os *boards* de controle de configuração (CCB), revisão de não conformidade (NRB), revisão de testes (TRB) e análises de qualificação e aceitação devem acomodar um ou mais representantes da função segurança (ECSS, 2017a).

O risco de segurança é definido a partir de cenários de perigo e suas consequências. Conforme o padrão ECSS, o risco de segurança encontra-se associado a um ou mais cenários de perigo. Quando associado a somente um cenário, é definido como um risco individual, enquanto se associado a um conjunto de cenários de perigo, com a mesma consequência, é definido como um risco geral (ECSS, 2017a). O padrão caracteriza risco de segurança como uma combinação entre o impacto e a probabilidade de ocorrência de cenários de perigo (ECSS, 2017a).

O padrão ECSS preconiza que o processo de identificar, reduzir e controlar os riscos de segurança seja parte do processo de gestão de riscos do projeto. Este, por sua vez, deve ser executado, de forma contínua e interativa, durante o ciclo de vida do projeto, conforme a seguinte ordem de atividades (ECSS, 2017a):

1. definição dos requisitos de segurança;
2. identificação de perigos e riscos de segurança;
3. avaliação (incluindo categorização) da severidade dos riscos;
4. redução e controle de perigos e riscos de segurança;
5. encerramento e aceitação de riscos residuais.

As tabelas a seguir listam as atividades do programa de garantia de segurança que devem ser desenvolvidas em cada etapa do ciclo de vida do produto espacial (ECSS, 2017a).

Tabela 2.9: Atividades de garantia de segurança durante a Fase 0.

Fase	Atividades de Segurança
Análise da missão	-Analisar os requisitos de segurança e as lições aprendidas associadas a missões anteriores semelhantes; -Realizar uma análise preliminar de perigos do sistema proposto e do conceito de operações -Realizar uma avaliação comparativa dos riscos de segurança das opções conceituais; -Identificar os requisitos de segurança relevantes do projeto; -Planejar atividades de segurança para a fase de viabilidade; -Apoiar a revisão da definição da missão.

Fonte: ECSS (2017a).

Tabela 2.10: Atividades de garantia de segurança durante a fase A.

Fase	Atividades de Segurança
Viabilidade do Projeto	-Iniciar as análises de perigo dos conceitos de projeto e operações, a fim de identificar perigos aplicáveis no nível do sistema, condições perigosas e possíveis eventos e consequências perigosos; -Apoiar as negociações conceituais, identificando aspectos críticos de segurança das opções conceituais; -Eliminar e minimizar os riscos além de fazer recomendações de segurança; -Realizar avaliações comparativas de riscos de segurança das opções conceituais; -Identificar funções críticas de segurança no nível do sistema; -Identificar requisitos de segurança específicos do projeto em nível de sistema; -Planejar atividades de segurança para a fase de definição do projeto; -Apoiar a revisão preliminar de requisitos.

Fonte: ECSS (2017a).

Tabela 2.11: Atividades de garantia de segurança durante a fase B.

Fase	Atividades de Segurança
Definição Preliminar	-Atualizar a análise de perigos em apoio às atividades de definição de conceito de projeto e missão e identificar requisitos adicionais de segurança específicos do projeto; -Atualizar a identificação das funções críticas de segurança e definir os requisitos de tolerância a falhas; -Identificar situações de emergência que exijam atenção e cautela. -Atualizar a avaliação de riscos de segurança do sistema como parte da contribuição fornecida pelo domínio de segurança ao processo de gestão de riscos; -Identificar os requisitos de segurança do projeto; -Garantir que a documentação e as atividades do projeto estejam em conformidade com os requisitos de segurança do projeto; -Apoiar uma revisão de requisitos do sistema e uma revisão preliminar do projeto; -Planejar a verificação da implementação dos requisitos de segurança; -Preparar o plano de segurança para a definição detalhada, fase de produção e qualificação.

Fonte: ECSS (2017a).

Tabela 2.12: Atividades de garantia da segurança durante a fase C e D.

Fase	Atividades de Segurança
Definição Detalhada/Qualificação e Produção	-Realizar uma análise detalhada dos perigos no nível do sistema; -Realizar análises de segurança de suporte; -Atualizar os requisitos técnicos de segurança do projeto para integrar os resultados das análises de segurança; -Garantir que o programa de implementação e verificação do projeto cubra as atividades de verificação de controle de perigos identificados; -Atualizar a identificação de funções críticas de segurança, requisitos de tolerância a falhas e identifique itens críticos de segurança; -Implementar programa de controle para itens críticos de segurança; -Realizar avaliação de risco de segurança em apoio à melhoria do projeto. -Monitorar a verificação da implementação dos requisitos de segurança; -Verificar e documentar a implementação do controle de riscos; -Verificar se todos os itens de verificação em aberto estão registrados e se os procedimentos acordados estão em vigor; -Apoiar a revisão crítica do projeto, a revisão da qualificação e a revisão da aceitação; -Realizar análises de segurança interna do projeto e auditorias internas; -Identificar, monitorar e controlar as operações de montagem, integração, teste e manuseio do projeto que sejam potencialmente perigosas para o pessoal ou o hardware; -Revise e aprove procedimentos operacionais críticos e de segurança; -Realizar relatórios e investigações de acidentes; -Apoiar as análises de segurança do cliente nos marcos definidos do programa; -Preparar um relatório de “lições aprendidas” de segurança do projeto; Preparar o plano de segurança da fase operacional.

Fonte: ECSS (2017a).

Tabela 2.13: Atividades de garantia de segurança durante a fase E.

Fase	Atividades de Segurança
Operações	-Emitir o plano de segurança da fase operacional; -Revisar os procedimentos operacionais; -Aprovar procedimentos operacionais críticos de segurança; -Identificar e monitorar operações perigosas; -Apoiar a revisão de prontidão de voo, revisão de prontidão operacional, revisão de prontidão de lançamento e análises de qualificação de voo; -Apoiar operações terrestres e de voo; -Executar controle de itens críticos de segurança; -Monitorar e avaliar a evolução da configuração e operações do sistema resultantes de correções e atualizações de projeto; -Atualizar as análises de riscos e implementar controles adicionais de riscos, conforme necessário; -Investigar anomalias e tendências de voo relacionadas à segurança; -Atualizar a avaliação de risco de segurança conforme necessário para apoiar as decisões operacionais; -Preparar o plano de segurança da fase de descarte.

Fonte: ECSS (2017a).

Tabela 2.14: Atividades de garantia de segurança durante a fase F.

Fase	Atividades de Segurança
Descarte	-Realizar uma análise de perigos com relação às operações de descarte; -Verificar se a operação de descarte está em conformidade com os regulamentos internacionais de segurança, executando a análise de segurança necessária; -Revisar os procedimentos das operações de descarte; -Apoiar a revisão de encerramento da missão.

Fonte: ECSS (2017a).

2.6.3 INPE

No INPE, a disciplina de Garantia da Segurança de Sistemas foi formalmente incluída à estrutura do Serviço de Engenharia de Qualidade (SEQ) em meados do ano de 2016. Desde então, a referida unidade tem se dedicado à definição, no âmbito organizacional, de processos, metodologias e ferramentas

de trabalho, bem como a implementação destes em projetos espaciais desenvolvidos pelo instituto.

Como referência para este trabalho, foram adotados os padrões de segurança adotado pela ESA, ou seja, os padrões da ECSS de segurança.

As atividades de montagem, integração e testes do satélite CBERS 04A, lançado em 2019, contaram, já, com auditorias e inspeções de segurança, em instalações do INPE. A realização destas atividades, deu-se através da definição de requisitos de segurança de sistemas para os testes ambientais de satélites, por meio do estudo comparativo de padrões internacionais (GENARO, 2019).

Para exercitar a ferramenta de análise de perigos foi utilizado o projeto do carro de basculamento do satélite Amazonia-1. A metodologia adotada foi adaptada da norma ECSS-Q-ST-40-02C (*Hazard Analysis*), tornando possível a validação de ferramenta de trabalho, validada como metodologia padrão de análise de segurança para projetos futuros. (GENARO, 2019)

Cabe ressaltar que as abordagens destacadas acima foram necessárias para validar as ferramentas e as rotinas de trabalho para esta nova área. No entanto, como os projetos CBERS 04A e Amazonia-1 já estavam no final da Fase D e que a definição e implementação de requisitos de segurança é uma atividade que acontece durante as fases A e B do projeto espacial, não foi possível implementar os requisitos mínimos de segurança esperados para um projeto espacial para os satélites supracitados.

A gestão de riscos dos projetos é uma atividade realizada sob supervisão do gerente do projeto e segue a metodologia definida pela ECSS e pelo PMBOK.

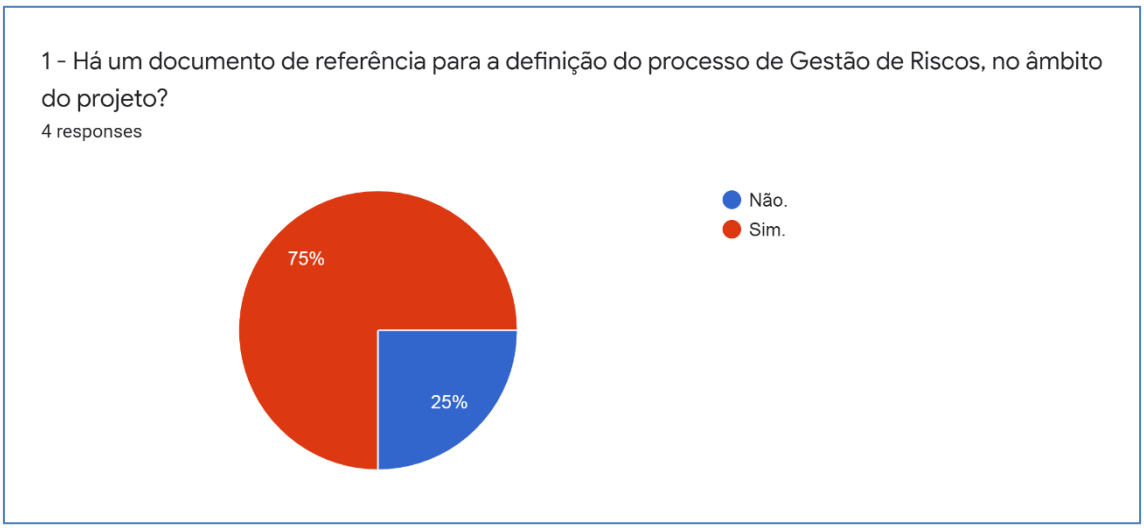
Atualmente, o INPE possui um documento dedicado aos requisitos para garantia do produto, incluindo segurança, dependabilidade e qualidade. O Grupo de Segurança de Sistemas Espaciais do INPE já possui todos os seus processos de trabalho mapeados e procedimentos operacionais já publicados e disseminados pelos membros da equipe.

Para retratar o cenário e entender como é tratada a gestão de riscos e a garantia de segurança, dentro de projetos no INPE, foram elaborados questionários e enviados aos gerentes de três projetos diferentes: CBERS 4A, AMAZONIA-1, EQUARS e NANOSATC-BR1. A Figura 2.29 apresenta a primeira parte do

questionário. A partir desse questionário, pode-se constatar que os referidos projetos exercitaram a gestão de riscos em nível de sistema. Três dos quatro projetos desenvolveram documento de referência e de acompanhamento para a gestão de riscos, durante o projeto. As revisões e atualizações relativas à gestão de riscos em 50% dos projetos estudados são efetuadas de forma contínua, com a emissão de relatórios periódicos com a exceção de um projeto, os relatórios de gestão de ricos são preservados após a conclusão do projeto.

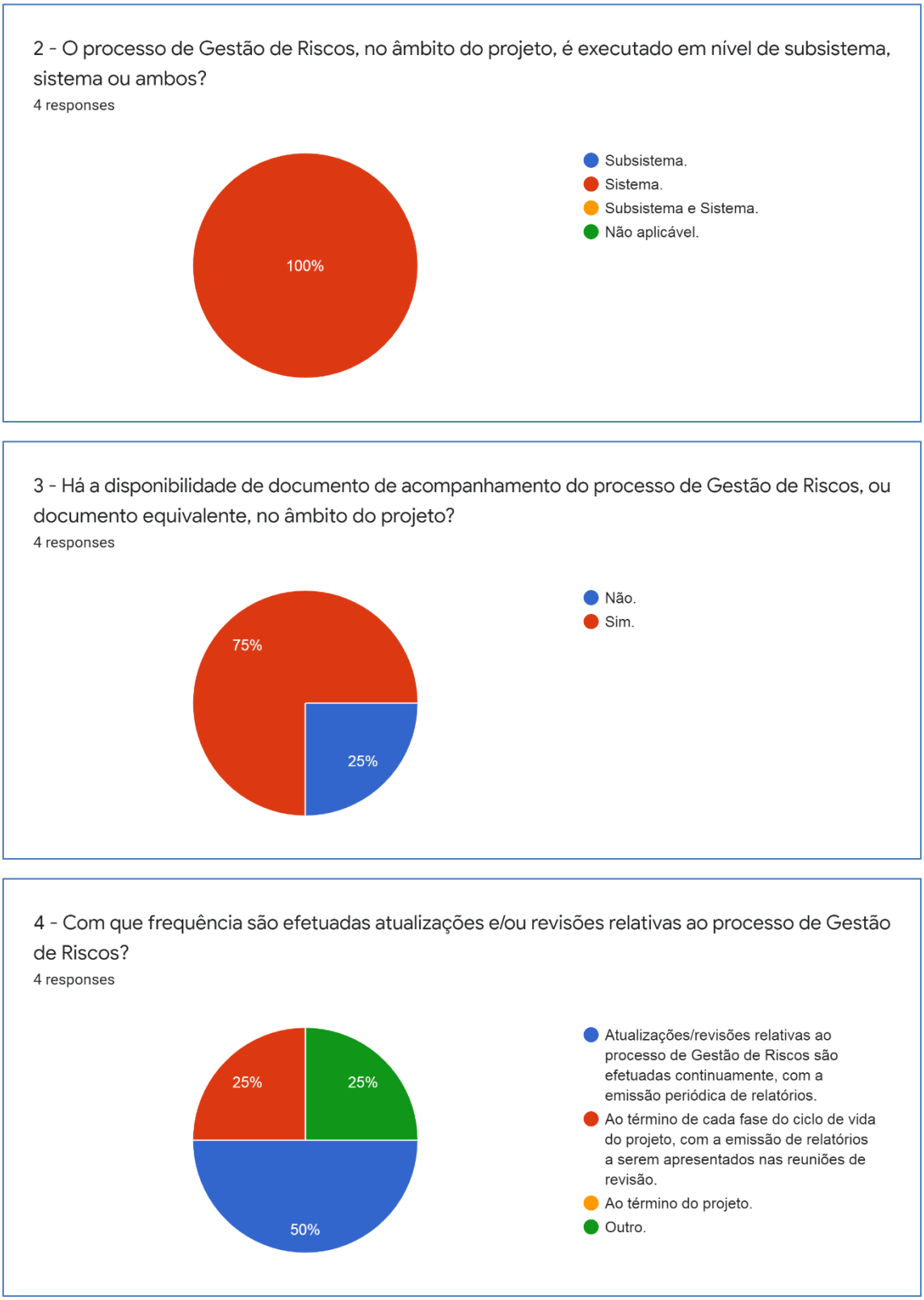
No que se refere à garantia da segurança, observa-se que em 50% dos projetos a garantia da segurança é realizada em nível de sistema e subsistema, e que 75% dos projetos possuem um documento de referência, bem como documentos de acompanhamento ao longo do projeto. As revisões e atualizações relativas à garantia de segurança acontecem de forma contínua em 75% dos projetos avaliados, com relatórios emitidos periodicamente. Em todos estes casos, os relatórios são preservados para consulta após a conclusão do projeto.

Figura 2.29: Questionário INPE – Primeira parte.



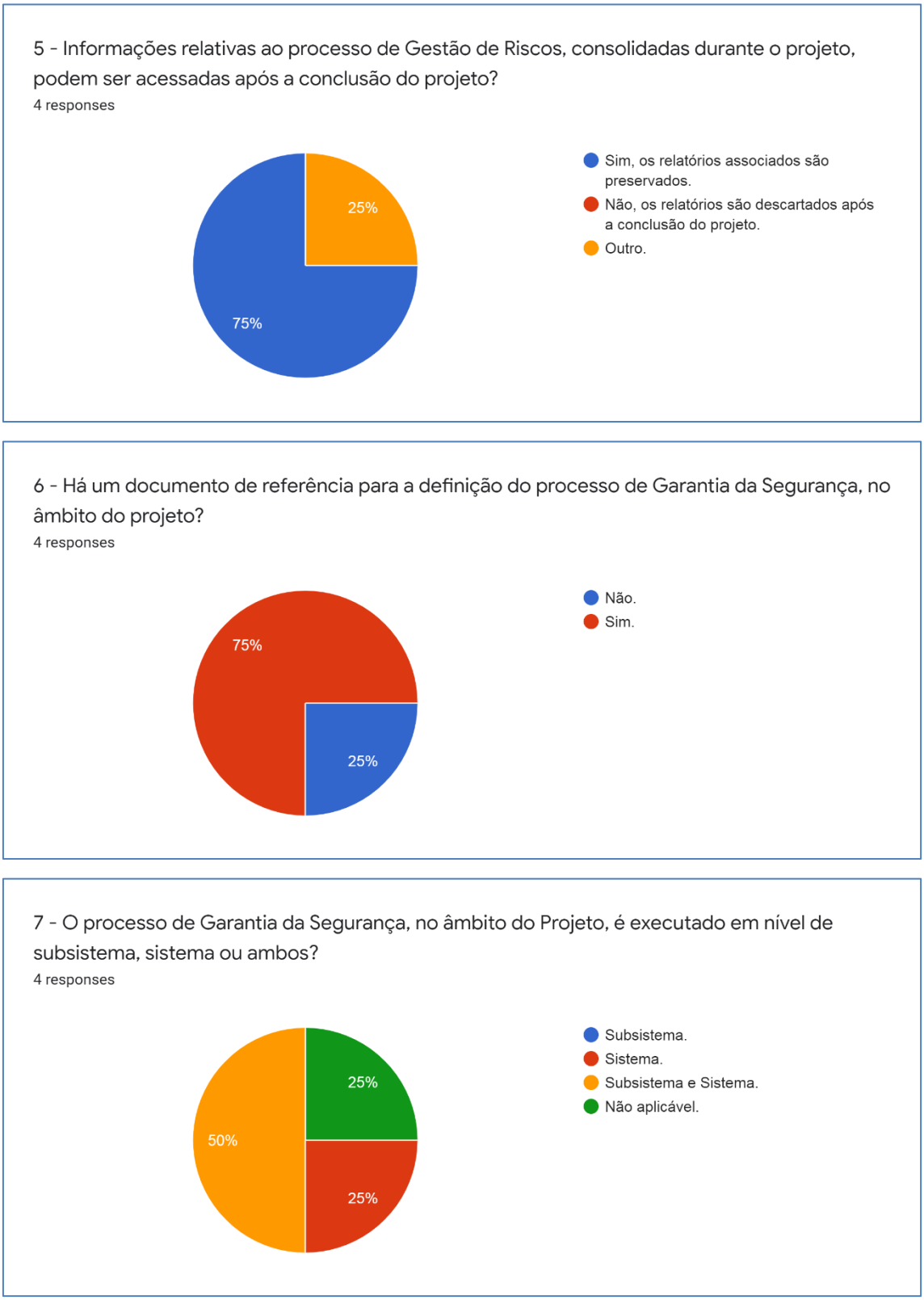
continua

Figura 2.29 – Continuação.



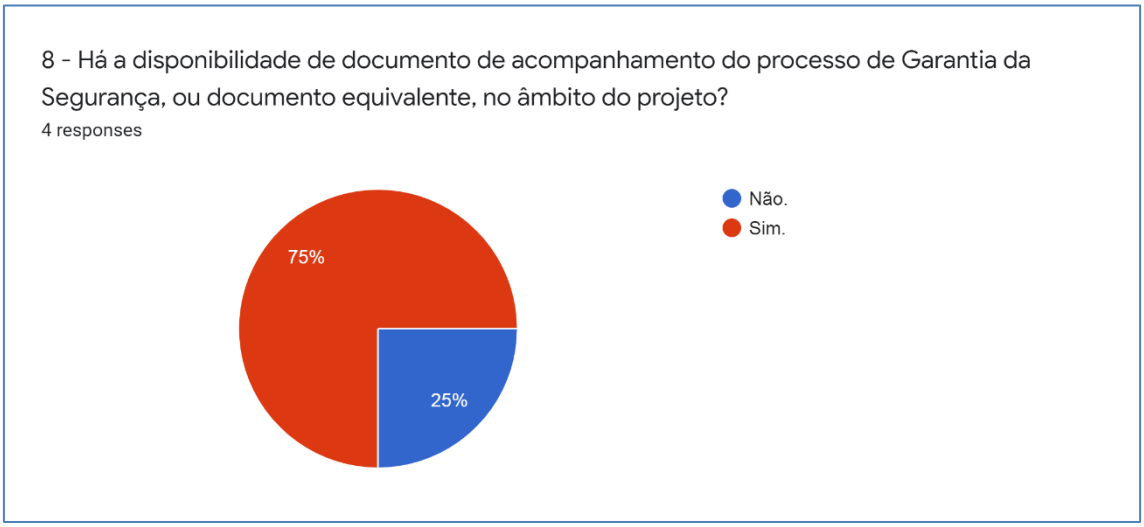
continua

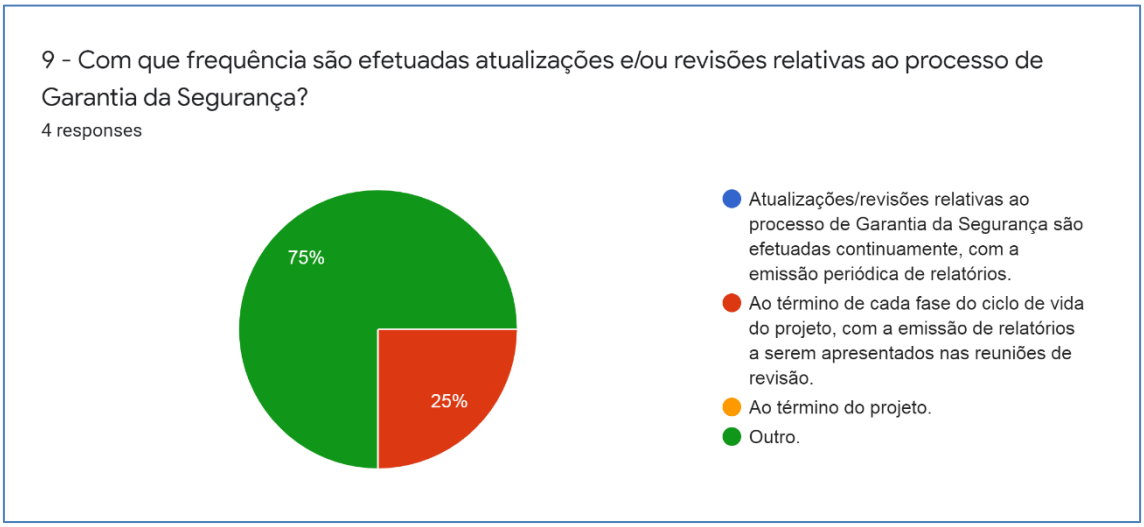
Figura 2.29 – Continuação.

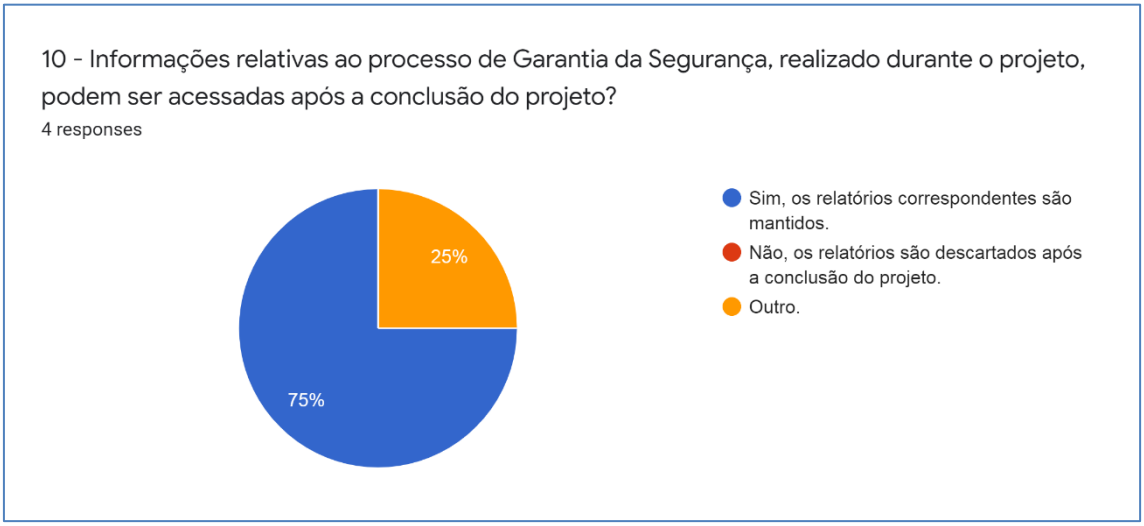


continua

Figura 2.29 – Continuação.

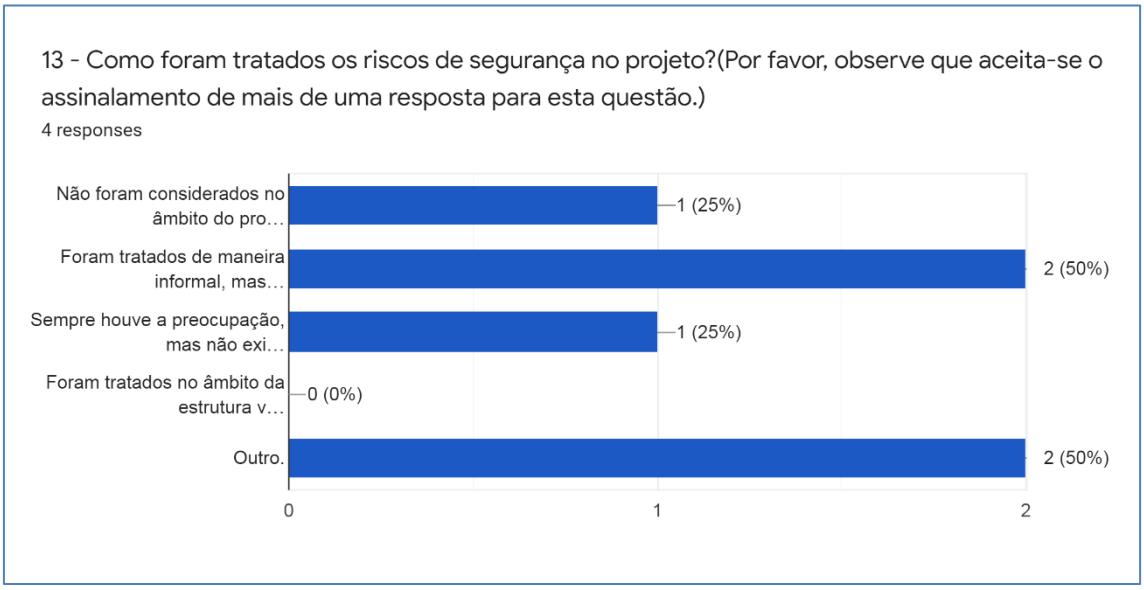






continua

Figura 2.19 – Conclusão.



Fonte: Produção da autora.

2.7 Classificação de satélites

Para Kramer e Cracknell (2008), existem inúmeras formas de classificar satélites artificiais, tais como por função, tipo de órbita, custo, tamanho, desempenho, entre outras. A presente seção dedica-se a uma breve revisão de classificações de satélites disponíveis na literatura.

2.7.1 Classificação de missões por órbita

A órbita para uma dada missão é definida em função da aplicação pretendida. É comum que missões sejam classificadas conforme a órbita planejada para a missão. (NASA, 2020a)

Conforme classificação usual na área espacial, utilizada pela NASA, distinguem-se, grosseiramente, os seguintes tipos de órbitas terrestres: *high Earth* e *geosynchronous orbit*, *medium Earth orbit* e *low Earth orbit*. A Tabela 2.15 apresenta a altitude típica destas órbitas. (NASA, 2020a)

Tabela 2.15: Classificação de órbitas segundo a NASA.

Órbitas	Distância
High Earth & Geosynchronous Orbit	≥ 35,780 km
Mid Earth Orbit	2,000 – 35,780 km
Low Earth Orbit	180 – 2,000 km

Fonte: Adaptado de NASA (2020a).

Já, a ESA faz uso de classificação que distingue as seguintes órbitas para missões: *Geostationary orbit (GEO), Low Earth orbit (LEO)* e *Medium Earth orbit (MEO).* Órbitas LEO são adicionalmente classificadas como *Polar orbit and Sun-synchronous orbit (SSO)* (ESA, 2020).

Tabela 2.16: Classificação de órbitas segundo a ESA.

Órbitas	Distância
Geostationary orbit (GEO)	> 35.786 km
1000 – 35.786 km	1000 – 35.786 km
Low Earth orbit (LEO)	< 1000 km

Fonte: Adaptado de ESA (2020).

2.7.2 Classificação de satélites por uso

Outra classificação existente baseia-se na principal aplicação prevista para a missão. No âmbito desta classificação, as categorias usuais são: observação da Terra, observação astronômica, comunicações, aplicações militares, aplicações científicas e geoposicionamento. Dentro da categoria de observação da Terra, estão inseridos satélites de sensoriamento remoto, meteorologia, oceanografia, entre outros (SOUZA, 2002)

Já a NASA divide as missões em tópicos como: Terra, sistema solar, universo e humanos no espaço. A Tabela 2.17 ilustra os diferentes usos dentro de cada categoria.

Tabela 2.17: Tabela de categorias de missão.

Earth	Solar System	Humans in Space	Universe
Atmosphere	Asteroids	International space station	Big Bang and Cosmology
Climate	Comets	Future exploration plans	Black Holes
Continental Drift and Geodynamics	Jupiter	-	Galaxies
Gravity	Mars	-	Gamma-Ray Bursts
Hurricanes	Mercury	-	Gravity
Ice	Moon	-	Interstellar Medium
Land and Vegetation	Neptune	-	Life in the Universe
Oceans	Planets	-	Nebulae
Ozone	Pluto	-	Planets Beyond the Solar System
Sun and its Influence on Earth	Saturn	-	Stars
Water Cycle	Sun and its Influence on Earth	-	Supernovae
Weather	Uranus	-	-
Wildfires	Venus	-	-

Fonte: Adaptado de NASA (2020c).

Segundo Konecny (2004), o uso de pequenos satélites nas décadas de 1980 e 1990 está listado na Tabela 2.18.

Tabela 2.18: Uso de satélites segundo Konecny 2004.

Uso	Porcentagem
Comunicações	69,2%
Ciência	14,4%
Demonstração Tecnológica	11,0%
Militares	2,3%
Educação	1,7%
Observação da Terra	1,4%

Fonte: Konecny (2004).

2.7.3 Classificação de satélites por massa

É sabido que existem inúmeras maneiras de classificar satélites, porém, a classificação de acordo com a massa é uma das principais métricas para definir o tamanho dos veículos de lançamento e os custos para lançar em órbita. Massa e tamanho são os principais parâmetros que afetam na definição de requisitos

como custo de missão, tipo de órbita e muitos outros, mas principalmente o *launch lifting Power* (KRAMER; CRACKNELL, 2008)

Segundo Rogers et al (2014) a massa de um satélite está diretamente relacionada a um grande componente do custo do programa, o veículo de lançamento (ROGERS et al, 2014).

Martin Sweeting, da SSTL, em seu artigo de 1991 propôs a primeira classificação conhecida de satélites. (KRAMER; CRACKENELL, 2008 apud SWEETING, 1991) Tabela 2.19.

Mais tarde, Konecny em seu artigo de 2004 substitui a classe de pequenos satélites por médios e divide a classe de nano satélites em três grupos nanossatélites (1 - 10 kg), pico satélite (0,1 - 1 kg) e fenito satélite (0,001 - 0,1 kg ou 1 - 100 g) ilustrado pela Tabela 2.20 (KONECNY, 2004).

Segundo Botelho e Xavier, Kramer e Cracknell em seu artigo de 2008 revisaram a classificação de Konecny e mesclaram as classes de satélites médios (500 - 1000 kg) e mini-satélites(100 - 500 kg) na faixa de 100 - 1000 kg (BOTELHO; XAVIER, 2019).

Posteriormente Sweeting diz que o advento da microeletrônica possibilitou que satélites menores fossem construídos, sendo assim, em outro artigo inclui mais duas classes de satélites com massa menor do que 10kg (SWEETING, 2018). A Tabela 2.21 apresenta a classificação.

Segundo Botelho e Xavier (2019), a ESA e a EADS Astrium não definem claramente as classes de médio e grandes satélites, se atendo somente a classificação a partir de pequeno. A ESA classifica pequenos satélites como sendo os com massa entre (350-700 kg), minissatélites entre (80-350 kg) e microssatélites entre (50-80 kg). Por outro lado, o EADS Astrium definiu os satélites miniXL (1000-13000 kg), mini (400-700 kg) e micro (100-200 kg) (NAG; LEMOIGNE; DE WECK, 2014). A Tabela 2.22 e Tabela 2.23 apresentam a classificação.

Tabela 2.19: Primeira classificação de satélites por Sweeting.

Classe	Massa
Nanosatellite	< 10kg
Microsatellite	10 – 100kg
Minisatellite	100 – 500kg
Small Satellite	500 – 1000kg
Large Satellite	> 1000kg

Fonte: Sweeting (1991) Apud Kramer e Cracknell (2008).

Tabela 2.20: Classificação de satélites por Konecny.

Classe	Massa
Large Satellite	> 1000kg
Medium Satellite	500 - 1000kg
Mini Satellite	100 - 500kg
Micro Satellite	10 – 100kg
Nano Satellite	1 – 10kg
Pico Satellite	0.1 – 1kg
Fenito Satellite	< 100kg

Fonte: Konecny (2004).

Tabela 2.21: Classificação geral de satélites por Sweeting.

Classe	Massa
Large Satellite	> 1000kg
Small Satellite	500 - 1000kg
Mini Satellite	100 - 500kg
Micro Satellite	10 – 100kg
Nano Satellite	1 – 10kg
Pico Satellite	0.1 – 1kg
Femto Satellite	< 0.1kg

Fonte: Sweeting (2018).

Tabela 2.22: Classificação de Satélites ESA.

Classe	Massa
Small satellite	350 – 700 Kg
Minisatellite	80 – 350 Kg
Microsatellite	50 – 80 Kg

Fonte: Botelho e Xavier (2019).

Tabela 2.23: Classificação EADS/Astrium.

Classe	Massa
Mini XL Satellite	1000 – 1300 Kg
Minisatellite	400 – 700 Kg
Microsatellite	100 – 200 Kg

Fonte: Botelho e Xavier (2019).

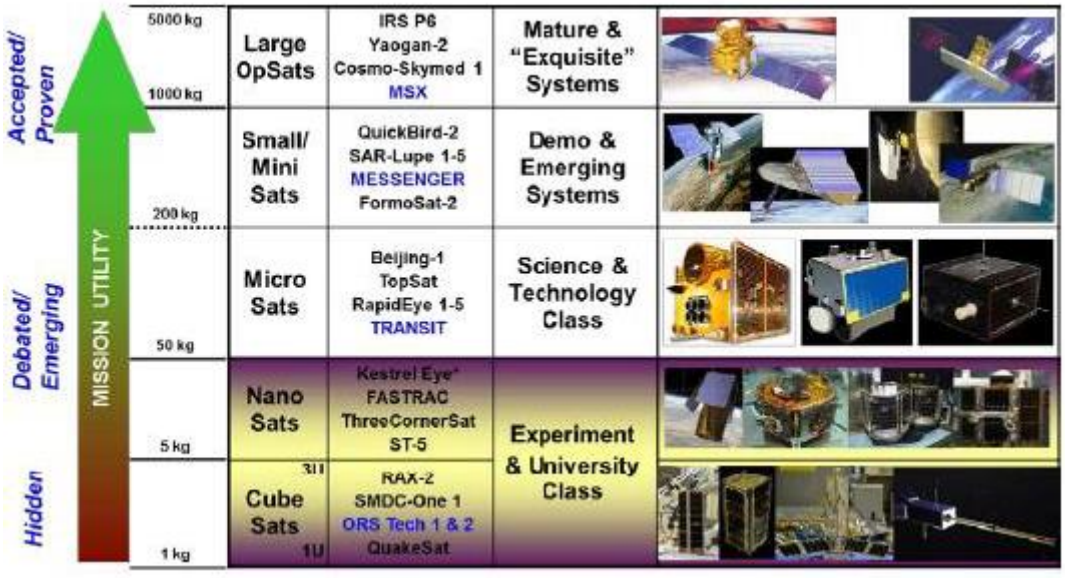
O *Small Spacecraft Technology Program (SSTP) da NASA* define que uma nave espacial é de pequeno porte quando sua massa é inferior a 180kg. Elas são agrupadas de acordo com a massa e incluem minissatélites com massa entre (180 -100 kg), micosatélites com massa entre (100-10 kg), nanosatélites com massa entre (10-1 kg), picosatélites com massa (1 – 0.1kg) e Femtosatélites com massa (0.01 – 0.09kg) como mostra a Figura 2.30 (NASA, 2020b). A NASA também não define claramente classes de médio e grande porte para satélites.

Figura 2.30: Overview das naves espaciais que se enquadram na categoria pequena.

Fonte: NASA (2020b).

O The Johns Hopkins University Applied Physics Laboratory (JHU/APL), classifica as naves espaciais como mostra a Figura 2.31. E também classificam os satélites com massa entre 200 kg e 1000 kg como pequenos ou minissatélites. (ROGERS et al, 2014 apud PESSOTA, 2018).

Figura 2.31: Classificação das naves espaciais pelo JHU/APL de acordo com sua massa.



Fonte: Rogers et al (2014) Apud Pessota (2018).

2.8 Garantia da segurança de sistemas espaciais

2.8.1 Segurança de sistemas espaciais

Para a NASA, sistema é uma entidade integrada que executa uma função especificada, constituído por hardware, software e elemento humano, operando em um ambiente especificado. A segurança de sistema (*system safety*), por sua vez, consiste na aplicação de princípios, critérios e técnicas de engenharia e gerenciamento de projetos com o objetivo de aprimorar e otimizar a segurança, respeitando limitações de eficácia operacional, tempo e custo em todas as fases do ciclo de vida do sistema (NASA, 2011a).

Segundo Marshall (2009, p. 1, *apud* ROLAND; MORIARTY, 1990) "... *A segurança em um sistema pode ser definida como a característica de um sistema de operar sob condições predeterminadas com um risco mínimo (e) aceitável de perda acidental* ...".

Para Levenson (2008), segurança "... *é uma abordagem planejada, disciplinada e sistemática para identificar, analisar, eliminar e controlar os perigos por meio de análise, projeto e procedimentos de gerenciamento ao longo do ciclo de vida de um sistema* ...". Ainda segundo esta autora "... *As atividades de segurança do sistema começam nos primeiros estágios de desenvolvimento do conceito de um projeto e continuam durante o projeto, produção, teste, uso operacional e descarte*. ...".

2.8.2 Política de segurança

Segundo a ECSS-Q-ST-40C, a política de segurança deve:

• garantir que os sistemas espaciais não causem perigo na seguinte ordem de prioridade:

- vida humana;
- meio ambiente;
- propriedade pública e privada (incluindo instalações de lançamento); espaçonave e lançador;

- equipamentos e instalações de apoio no solo.

• determinar e avaliar os riscos de segurança associados às atividades do projeto;

• minimizar os riscos de segurança de maneira tecnicamente eficaz e econômica;

• garantir a verificação adequada das medidas de controle de segurança.

Ainda conforme a ECSS a política de segurança deve ser implementada por meio de um programa de segurança que estabeleça meios gerenciais e técnicos para garantir que: (i) a segurança seja projetada no sistema, (ii) os requisitos de segurança sejam atendidos, (iii) os perigos sejam identificados e devidamente tratados, (iv) os controles de segurança sejam adequadamente implementados no plano de verificação (ECSS, 2017a).

Para a NASA, a política de segurança aborda a questão de proteger o público, a força de trabalho da NASA, equipamentos e propriedades de alto valor, além do meio ambiente contra possíveis danos causados pelas atividades e operações. A segurança é considerada como um recurso inerente de programas, projetos, tecnologias, operações e instalações (NASA, 2008, p. 1).

A política de segurança preconizada pela NASA também deve:

- estabelecer linhas de comunicação independentes para o fluxo irrestrito de informações que afetem a segurança da missão e comprometam seu sucesso;
- responsabilizar os líderes, gerentes, supervisores e funcionários da NASA pela segurança e pelo sucesso da missão;
- definir e documentar os requisitos de segurança e sucesso da missão nos programas e projetos da NASA para usar como base para desenvolver programas seguros e confiáveis;
- verificar e validar a implementação dos processos de *Safety Mission Assurance* (SMA) através da vigilância contínua dos processos do programa, projeto e empreiteiro;

- certificar a segurança e a prontidão operacional de hardware, software e missão crítica através de um processo de revisão formal compilando informações de validação e verificação;
- abordar questões de segurança e sucesso da missão, não cumprimento de requisitos, riscos e aceitação de riscos, lições aprendidas em todas as principais revisões da gerência;
- usar técnicas qualitativas e quantitativas para avaliar riscos de forma a criar uma base para tomada de decisões sobre segurança;
- processar todas as decisões técnicas que resultem em segurança residual e / ou risco de sucesso da missão, obtendo a aprovação da autoridade técnica conhecedora (Engenharia, SMA ou Saúde / Medicina), além de aceitação do risco pelo programa, projeto ou gerente de operações e instalações respectivos;
- relatar e acompanhar todas as ações corretivas resultantes de investigações de contratempos, incidentes, não conformidades, anomalias e auditorias de segurança e garantia de missão; distribuir e usar as lições aprendidas para melhorar atividades e operações;
- incentivar, apoiar e monitorar programas, atividades e eventos que fortaleçam e sustentem uma cultura de segurança na NASA (NASA,2008).

2.8.3 Programa de segurança

A NASA determina que a segurança de pessoas, instalações e sistemas de missão são de responsabilidade da organização. Sendo assim, para garantir a segurança, a organização deve estabelecer um programa de segurança com o objetivo de proteger o público de danos, garantir a segurança dos funcionários e melhorar a taxa de sucesso das missões e operações por meio da prevenção de danos a equipamentos e propriedades de alto valor (NASA, 2017, p 2).

De acordo com a ECSS, um programa de segurança é um programa que garante a conformidade com a política e os requisitos de segurança do projeto espacial, com o objetivo de identificar e avaliar os riscos, com base em análises qualitativas e quantitativas. Objetiva, também, controlar os riscos selecionados

conforme critérios de hierarquização, definidos para o programa ou projeto, durante todo o ciclo de vida do projeto. A política de segurança da ECSS é implementada por meio da aplicação de um programa de segurança que garanta que:

- a segurança é projetada no sistema;
- os controles de segurança são implementados adequadamente e confirmados por um plano de verificação;
- requisitos de segurança, incluindo regulamentos de segurança do centro de lançamento são atendidos;
- os perigos são identificados e eliminados ou, quando isso não for possível, minimizados, classificados e controlados de acordo com os objetivos do projeto, de maneira aceitável (ECSS, 2017a).

A norma MIL STD 882C preconiza os requisitos para o desenvolvimento e implementação de um programa de segurança com o objetivo de eliminar ou reduzir os riscos e perigos a um nível aceitável (DOD, 1993). A norma determina que os requisitos gerais de um programa de segurança devem garantir que:

- a segurança seja projetada no sistema considerando o cronograma e o custo;
- os perigos e riscos associados a cada sistema são identificados, rastreados, avaliados e eliminados, ou o perigo associado reduzido a um nível aceitável ao longo do ciclo de vida inteiro de um sistema;
- dados históricos de segurança, incluindo lições aprendidas que precisam ser considerados e usados;
- ao aceitar e usar novas tecnologias, materiais, novas técnicas de produção teste e operação deve-se buscar eliminar os perigos associados ou reduzir até um nível aceitável;
- as ações tomadas para eliminar perigos ou reduzir os riscos a um nível aceitável sejam documentados;
- as ações de modernização necessárias para melhorar a segurança sejam minimizadas por meio da inclusão oportuna de recursos de segurança

durante pesquisas, desenvolvimento de tecnologia e aquisição de um sistema;

- as alterações nos requisitos de projeto, configuração ou missão sejam realizadas de maneira que mantenha os riscos em um nível aceitável;
- ao se projetar o sistema no início do ciclo de vida, considerar a segurança e a facilidade de descarte de materiais (incluindo descarte de materiais explosivos e perigosos). Ações devem ser tomadas para minimizar o uso de materiais perigosos e, diminuindo os riscos e os custos do ciclo de vida associados ao seu uso;
- dados significativos de segurança sejam documentados como "lições aprendidas" e submetidos a bancos de dados (DOD,1993).

3 RELAÇÃO ENTRE GESTÃO DE RISCO E GARANTIA DA SEGURANÇA

O capítulo a seguir aborda a relação entre a gestão de risco e a garantia da segurança, segundo o PMBOK, INCOSE e AS9100. Aborda, também, o tratamento desta relação nas organizações espaciais NASA, ESA e INPE, focando a dinâmica deste relacionamento durante o desenvolvimento de projetos espaciais.

3.1 Relação entre as disciplinas de gestão de risco e garantia de segurança segundo INCOSE, PMBOK e AS9100

3.1.1 INCOSE

O manual do INCOSE trata explicitamente do processo de gestão de risco associado ao sistema desenvolvido. Os riscos típicos considerados são os riscos gerenciais que afetam objetivos de projeto, como custo e cronograma, e riscos técnicos, que afetam o desempenho e a qualidade do sistema O Processo de Gestão de Riscos é um dos processos do arcabouço de engenharia de sistemas proposto no manual INCOSE. O manual diferencia os riscos técnicos dos gerenciais. Os riscos técnicos tratam do sistema, não do programa ou projeto, mas podem interferir nos riscos do programa ou projeto. As atividades de gestão de risco relacionadas à organização não são consideradas explicitamente.

O manual aborda os riscos técnicos de segurança, mas não o amplo espectro de riscos de segurança. Não considera de forma explícita o processo de garantia da segurança. As atividades de segurança se concentram no sistema, a partir do ponto de vista da engenharia de segurança do sistema, que é considerada uma atividade de engenharia especializada. O objetivo da engenharia de segurança do sistema é auxiliar o projeto com a proposição de requisitos que garantam a segurança do sistema, em todas as fases de seu ciclo de vida: desenvolvimento, produção, utilização, suporte e descarte. O guia preconiza que o esforço de engenharia de segurança do sistema seja incorporado aos processos de engenharia de sistemas desde o início do projeto, de modo que a segurança seja projetada no sistema, à medida que as decisões de projeto de engenharia sejam realizadas.

3.1.2 PMBOK

No âmbito do guia PMBOK, a gestão de riscos é considerada uma área de conhecimento. Os riscos mencionados relacionam-se aos objetivos gerenciais do projeto, como escopo, cronograma, custo. Os riscos técnicos não são considerados explicitamente.

As atividades de gestão de risco associadas à organização não são explicitamente consideradas. No entanto, o guia discute o fluxo para cima e para baixo dos riscos ao longo da estrutura hierárquica. No âmbito das organizações com estrutura matricial, os projetos fazem parte de um programa ou portfólio, o qual, por sua vez, se subordina a alguma instância organizacional. Os objetivos em cada um dos níveis da organização estão sujeitos a riscos, os quais são, geralmente, gerenciados neste mesmo nível organizacional. Porém, alguns riscos podem ser transferidos para níveis mais altos se, por exemplo, sua probabilidade ou impacto superar valores de referência predefinidos. O guia considera, também, a hipótese de transferência de determinados riscos para uma instância de nível inferior. Em essência, os riscos advindos do desenvolvimento de um programa ou projeto, são distribuídos entre o programa ou projeto e diferentes níveis da organização.

O guia não aborda explicitamente os requisitos de segurança do sistema e da organização. Também, é apontado que as necessidades específicas do projeto podem exigir áreas de conhecimento adicionais, além das áreas tradicionais descritas no guia. Dentro desta diretriz, se um projeto espacial requer um processo de gestão de segurança ou atividades relacionadas, deverá recorrer a pessoal especializado em áreas do conhecimento que vão além daquelas definidas no guia.

3.1.3 AS9100

A norma AS9100- *Quality Management Systems* fornece requisitos para a configuração de um sistema de gerenciamento de qualidade em uma organização aeroespacial. Um requisito central é que o sistema de qualidade deve abordar os riscos e oportunidades em cada um de seus processos. Esse conceito significa que, em vez de estabelecer um processo de gerenciamento de

risco que auxilie o sistema de gerenciamento de qualidade de forma centralizada, a norma requer a implementação de um gerenciamento de risco distribuído em todos os processos do sistema de gerenciamento de qualidade. Essencialmente, o pensamento baseado em risco requer que as empresas avaliem o risco ao estabelecer processos, controles e melhorias em um sistema de gestão da qualidade.

A norma AS9100 define segurança de produto como o estado em que um produto é capaz de executar a função para o qual ele foi projetado, sem causar riscos inaceitáveis ou danos a pessoas e danos à propriedade. Com relação às atividades de segurança, a norma exige que a organização planeje, implemente e controle os processos necessários para garantir a segurança do produto durante todo o ciclo de vida do sistema desenvolvido. Este requisito pode ser entendido como a implementação de um processo de gestão da segurança que supervisione e conduza as atividades de segurança com foco no sistema desenvolvido. Este requisito também implica o estabelecimento de um processo de gestão da segurança na instância da organização, conforme apropriado. Sendo assim, a relação de gestão de riscos e segurança não é tratada de forma clara. (SAE, 2016)

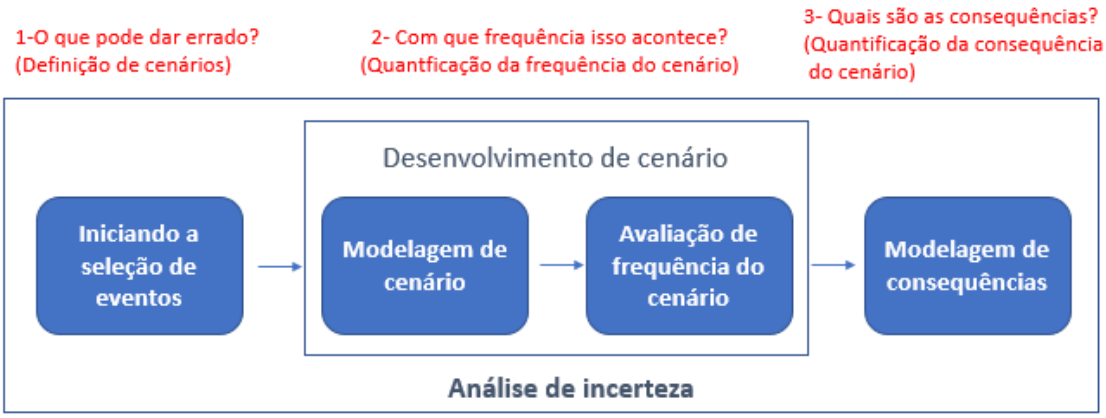
3.2 Relação de gestão de risco e garantia de segurança em organizações da área espacial

3.2.1 NASA

A NASA em seu *System Engineering Handbook* define risco como sendo o potencial para deficiências de desempenho, que podem estar relacionadas a qualquer um ou mais dos seguintes domínios de execução de missão: segurança, técnico, custo e cronograma. Em seu capítulo que trata de gestão de risco técnico, cita que as deficiências de desempenho podem estar relacionadas ao apoio institucional para execução da missão ou ainda aos domínios citados acima. O engenheiro de sistemas deve estar envolvido no processo de gestão de riscos, que segue o modelo mostrado a Figura 3.1, em que a caracterização do risco é dada por três itens: os cenários, a probabilidade de ocorrência desses

cenários e as consequências ou a severidade da ocorrência de tais cenários (NASA, 2016).

Figura 3.1: Desenvolvimento de cenário de risco.

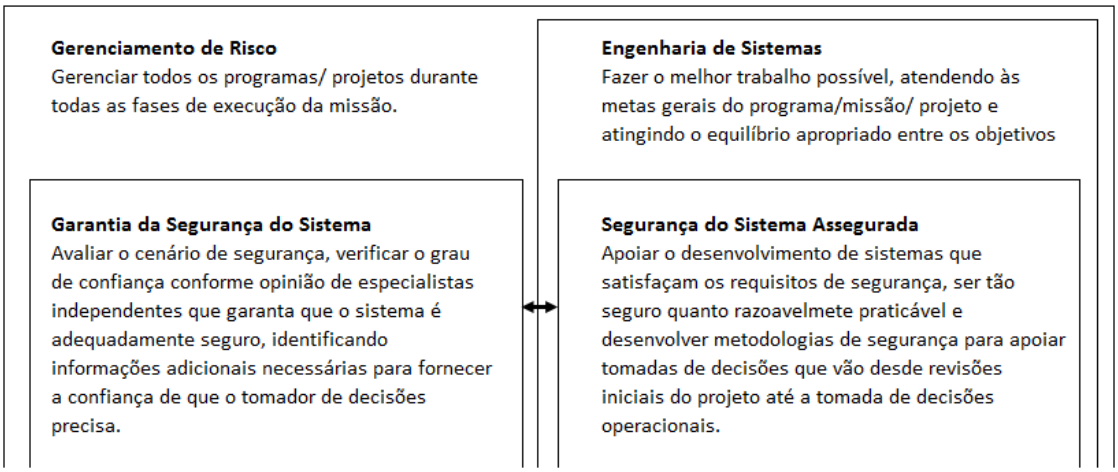


Fonte: Adaptado de NASA (2016).

A NASA, em seu *Risk Management Handbook*, também, define que o risco é o potencial para deficiências de desempenho, que podem estar relacionadas a qualquer um ou mais dos seguintes domínios de execução de missão: segurança, técnico, custo e cronograma. Reconhecendo a segurança como um objetivo do projeto, ao fazer o levantamento de riscos que ameaçam o projeto, os riscos de segurança devem ser considerados (NASA, 2011b).

De acordo com o documento *Systems Safety Handbook*, a NASA possui uma abordagem de segurança que reconhece a substancial sobreposição entre engenharia de sistemas, gestão de riscos e segurança do sistema. De um modo geral, a engenharia de sistemas é o modo pelo qual os objetivos são alcançados. O papel da gestão de risco é o de fornecer uma função de controle para a engenharia de sistemas, de forma a assegurar que o desenvolvimento esteja no caminho certo, em todos os domínios de execução da missão (NASA, 2014). Essa relação é ilustrada na Figura 3.2.

Figura 3.2: Relação entre gestão de riscos, engenharia de sistemas e segurança de sistemas em um projeto.



Fonte: Adaptado de NASA (2014).

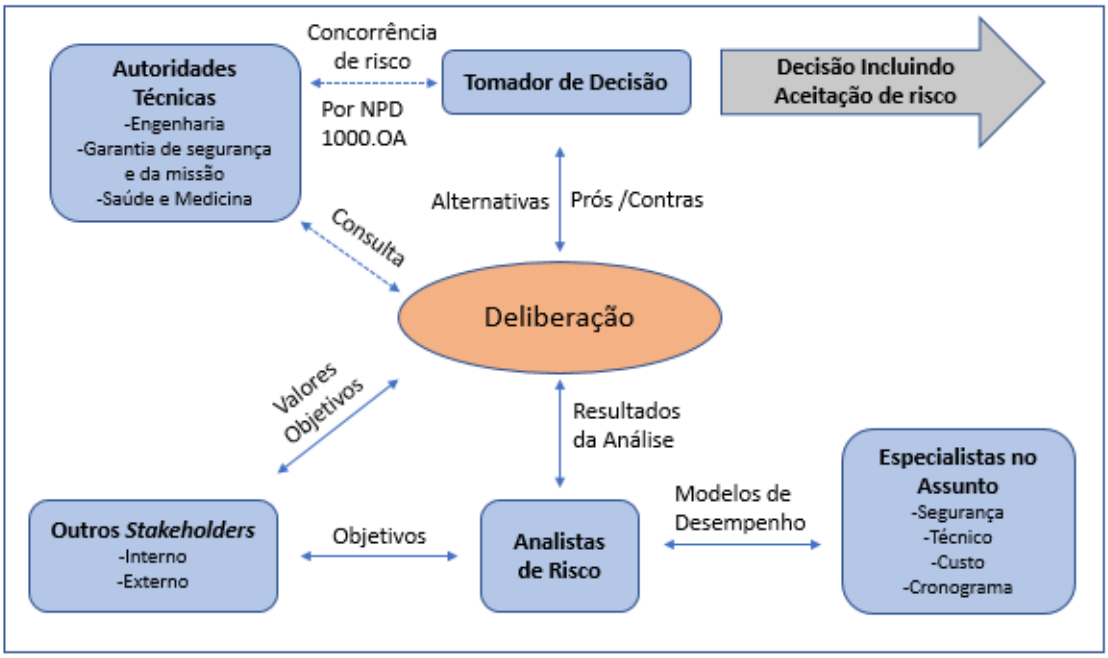
A segurança do sistema é uma entrada para a engenharia de sistemas e gestão de riscos. Considerando que o desempenho de segurança de um sistema é uma preocupação das partes interessadas, da mesma forma que o desempenho técnico, a segurança de sistemas pode, em princípio, ser considerada como parte integrante dos esforços de engenharia de sistemas, para desenvolver um sistema que satisfaça os objetivos das partes interessadas (NASA, 2014, p. 14).

A garantia de segurança do sistema é uma atividade de avaliação que mantém a independência funcional da engenharia de sistemas para ser mais eficaz no fornecimento de confiança de que o sistema é de fato adequadamente seguro (NASA, 2014, p. 14).

Durante o processo de RIDM da NASA, é prevista a interação entre as partes interessadas, os *Subject Matters Experts* (SMEs), as autoridades técnicas e os analistas de risco. A análise de risco de alternativas é executada por ou com o apoio de SMEs no assunto dos domínios relacionados aos objetivos do projeto (segurança, custo, técnico e cronograma) (NASA, 2011b). Após a conclusão das análises de risco, cabe ao tomador de decisão, junto com as autoridades técnicas em questão, selecionar uma alternativa a implementar. (NASA, 2011b).

A Figura 3.3 apresenta a interface e a troca de informações entre as partes durante o processo de RIDM.

Figura 3.3: Fluxo de informações no RIDM.



Fonte: Adaptado de NASA (2011b).

Como demonstrado pela figura, durante o RIDM, os analistas de riscos e os especialistas de garantia de segurança devem trocar informações, pois, apesar de a integração de modelos de risco ser de responsabilidade de gerenciamento de riscos (RM), o desenvolvimento de modelos individuais necessitam da interação entre especialistas de risco e segurança (NASA, 2011a). A participação de representantes técnicos de garantia da segurança e da missão também é prevista, pois elas também devem participar da escolha de uma alternativa de análise de risco (NASA, 2011a).

Da mesma forma que a interação da equipe de garantia de segurança e a equipe de gestão de risco dentro do processo de RIDM fica explícita a partir da figura acima apresentada, a mesma interação é abordada e explicitada na Figura 2.24, dentro das atividades de garantia de segurança em sua primeira fase (NASA, 2011a).

A função do CRM ao ser aplicado no início do projeto é concluir a modelagem de riscos iniciada no RIDM, incluindo todos os cenários que afetam a magnitude dos riscos de desempenho (NASA, 2011a). Logo após a conclusão esses cenários são introduzidos na atividade identificar do processo de CRM (NASA, 2011b).

A interação entre a equipe de gestão de riscos do projeto e de garantia de segurança durante o processo de CRM também fica evidenciada a partir da Figura 2.24. Isso se deve ao fato de a atividade de inicialização do CRM fornecer modelos e resultados aprimorados que a equipe de segurança do sistema pode usar para avaliar melhor as compensações do ASARP e adaptar os requisitos de segurança (NASA, 2011a).

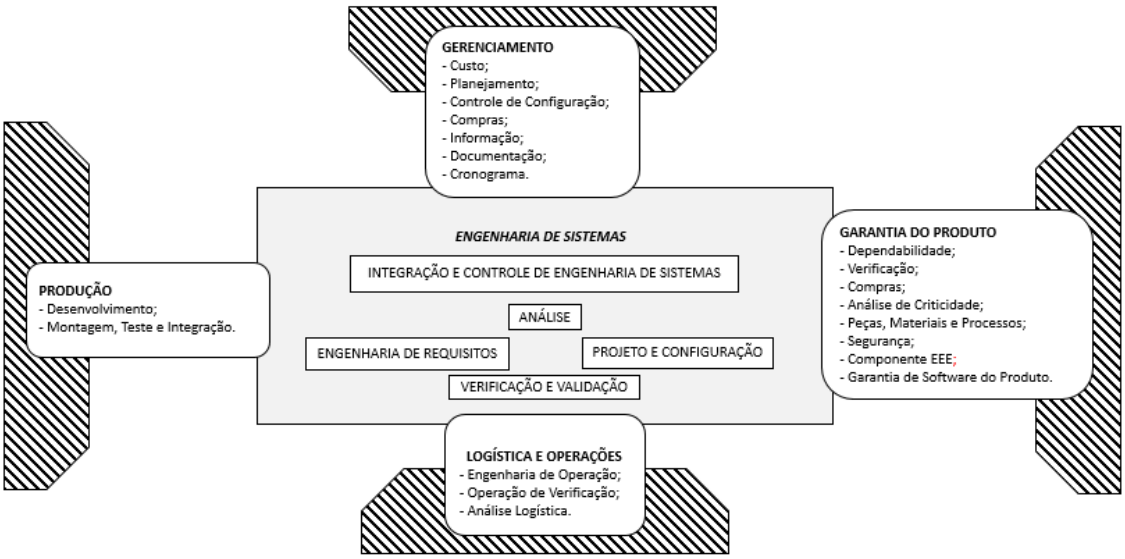
3.2.2 ECSS

A ECSS, em seu documento *Systems Engineering General Requirements* (ECSS-E-ST-10C), especifica os requisitos para desenvolver e implementar sistemas e produtos espaciais à luz da engenharia de sistemas. Dentre seus objetivos principais se destaca a implementação dos requisitos de engenharia de sistemas para estabelecer uma base técnica firme e a minimização de riscos. A engenharia de sistema deve contribuir para a identificação e mitigação de riscos do sistema ou produto espacial (ECSS, 2017b).

Este documento define engenharia de sistemas como uma abordagem interdisciplinar que transforma requisitos em uma solução de sistema. Para tanto, se faz necessária a integração e interface com disciplinas, tais como: produção, operações, garantia de produto e gerenciamento. A

Figura 3.4 ilustra a abrangência da disciplina de engenharia de sistemas e sua interação com as demais disciplinas. (ECSS, 2017b)

Figura 3.4: Limites da disciplina de engenharia de sistemas.



Fonte: Adaptado de ECSS (2017b).

Segundo a ECSS, as avaliações iniciais dos riscos técnicos e programáticos de um projeto são realizadas pelo cliente e as avaliações de risco mais abrangentes são realizadas em cada grande revisão do projeto. Na fase A, que corresponde à análise de missão e identificação de necessidades, declaram-se, também, os objetivos de segurança e de confiabilidade, e efetua-se a avaliação de riscos. Na fase B, ocorre a definição preliminar, tendo como principais atividades a avaliação de confiabilidade e segurança e a atualização da avaliação de riscos (ECSS, 2009).

O padrão (ECSS-Q-ST-20C) - *Quality Assurance* aborda a temática de *safety* quando cita os princípios da garantia da qualidade para *ground support equipment* (GSE). É citado que os requisitos devem ser definidos e implementados de forma a garantir a segurança (ECSS, 2018).

Quando se refere a requisitos de garantia da qualidade, a ECSS inclui, também, requisitos referentes à área de segurança (safety). Por exemplo, é citada a situação em que ao monitorar-se o desempenho de testes de um equipamento, se, em algum momento, a equipe de qualidade perceber a possibilidade de uma ameaça relacionada à segurança, afetando vida humana, ou danos a itens e equipamentos, a equipe de qualidade terá total autoridade para interromper a atividade (ECSS, 2018, p 35).

Segundo a ECSS, o objetivo da gestão de riscos de um projeto é identificar, avaliar, reduzir e aceitar os riscos do projeto espacial em relação ao domínio programático (custo, cronograma) e ao domínio técnico (confiabilidade, segurança). Afirma, ainda, que a prática de análise de segurança para lidar com riscos faz parte do processo de gestão de riscos (ECSS, 2008a).

A (ECSS-M-ST-80C) – *Risk Management* reconhece que a gestão de riscos requer troca de informações entre domínios do projeto, como engenharia de sistemas e garantia de segurança. A primeira etapa da gestão de riscos, segundo a ECSS, tem como atividades a definição da política de gestão de riscos e o plano de gestão de riscos que, em coordenação com outras disciplinas do projeto, como engenharia de sistemas, garantia do produto, produção e operações, entre outras, garante uma abordagem coerente ao gerenciar riscos do projeto (ECSS, 2008a). Dentre as disciplinas que compõem a garantia do produto, estão a garantia da qualidade, garantia de segurança e dependabilidade (ECSS, 2008a).

De acordo com a (ECSS-Q-ST-40C) – *Space Product Assurance: Safety*, o processo de identificar, reduzir e controlar os riscos associados à segurança deve ser parte integrante da gestão de riscos do projeto, seguindo a especificação dada pela ECSS-M-ST-80, referente à gestão de riscos (ECSS, 2017a).

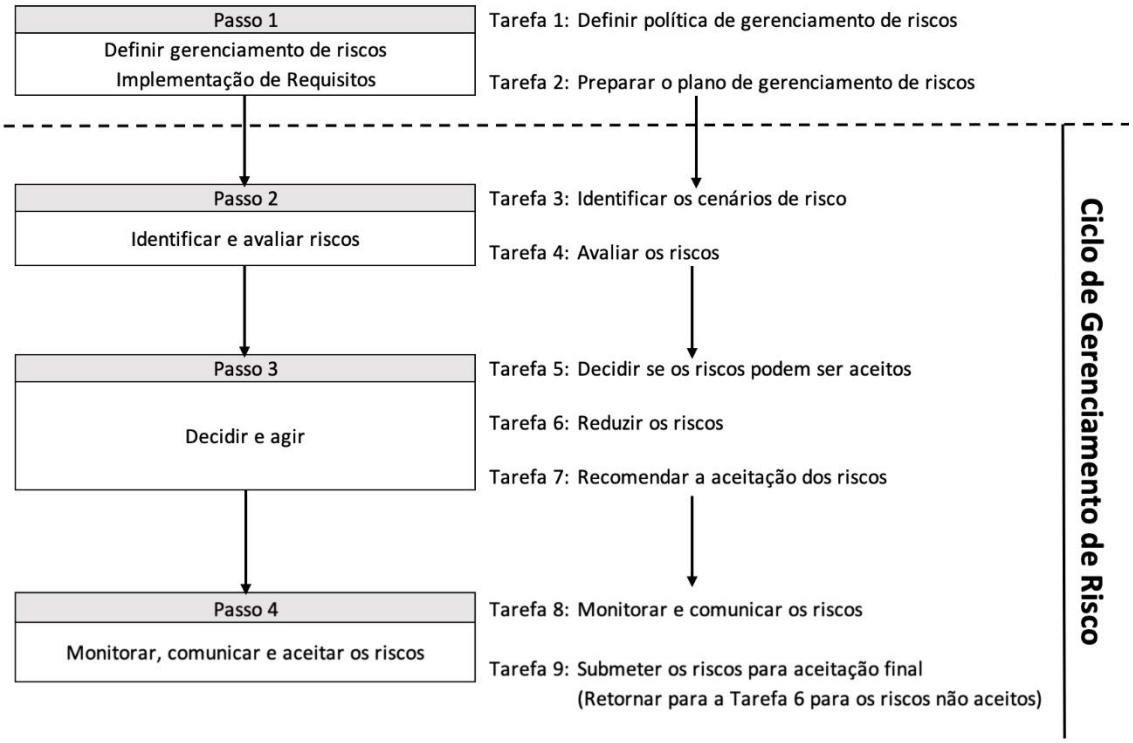
De acordo a determinação da ECSS, as atividades de gestão de riscos ocorrem durante todas as fases do projeto espacial, desde a fase de viabilidade até a fase de descarte. Dentre as atividades do projeto, encontram-se várias que se relacionam, concomitantemente, com a gestão de riscos e a garantia de segurança, tais como (ECSS, 2008a, p 23):

- estudos de viabilidade, negociações e análise de projetos como por exemplo, design, produção, segurança, confiabilidade e operações;
- a alocação de tarefas, mão de obra e recursos de acordo com a classificação de riscos;
- a evolução do conceito técnico através da avaliação de risco iterativa.
- avaliação de mudanças para impacto no risco;

- o desenvolvimento, qualificação, aceitação e execução do projeto, usando a avaliação de riscos como uma ferramenta de diagnóstico e para identificar ações corretivas;
- avaliação do status geral de risco dos projetos como parte de todas as revisões formais do projeto.

O processo de gestão de riscos deve trocar informações com os domínios do projeto em que cada risco é monitorado e controlado, conforme regras do domínio ao qual estes riscos pertencem. A interface entre a garantia de segurança e a gestão de riscos ocorre na primeira etapa do processo de gestão de riscos, composto por duas tarefas. A primeira relaciona-se à definição da política de gestão de risco e do plano de gestão de risco (ECSS, 2008a). A garantia de segurança insere-se através da garantia do produto (ECSS,2008a). A Figura 3.5 ilustra o processo de gestão de riscos à luz de suas atividades.

Figura 3.5:Tarefas associadas às etapas do processo de gerenciamento de riscos.



Fonte: Adaptado de ECSS (2008a).

A tarefa seguinte relaciona-se à identificação e avaliação dos riscos, em que são utilizadas informações de todos os domínios do projeto, por exemplo, cronograma e técnico, entre outros. Não é citado o domínio da garantia da segurança (ECSS, 2008a). Nas etapas seguintes do processo, a relação entre a garantia da segurança e gestão de risco não foi abordada de forma clara em nenhuma das atividades (ECSS, 2008a).

3.2.3 INPE

Para entender como a relação entre risco e segurança é abordada nos projetos do INPE, questionários foram aplicados aos gerentes dos seguintes projetos: CBERS 4A, AMAZONIA-1, EQUARS e NANOSATC-BR1.

De acordo com os resultados dos questionários, constatou-se que em 50% dos projetos houve a interação entre a equipe de garantia da segurança e de gestão de riscos, durante a execução e o planejamento dos respectivos processos. Porém nenhum documento foi gerado advindo de tal interação. Nesses projetos, a interação se deu ao término de cada fase do ciclo de vida. Ainda, pode-se observar que 50% dos riscos de segurança dos projetos acima citados foram tratados de maneira informal. Registros associados podem, porém, ser encontrados. A Figura 3.6 apresenta a segunda parte do questionário.

Figura 3.6: Questionário INPE – Segunda parte.

Fonte: Produção da autora.

A interação entre equipes de gestão de risco e garantia da segurança só ocorre em projetos mais recentes, pois a disciplina de garantia da segurança foi formalmente incluída na estrutura de serviço da instituição no ano de 2016. Por isso, não foi possível definir requisitos de segurança desde o início para os projetos CBERS 04A e Amazonia-1, pois estes já se encontravam no final da Fase D, à época da inclusão da disciplina na estrutura da instituição.

Para o projeto EQUARS, a implementação das atividades foi considerada desde o início do projeto, pois tão logo o projeto foi estruturado a disciplina de Garantia da Segurança de Sistemas passou a fazer parte do Estrutura de Divisão do Trabalho do projeto. Ou seja, o projeto EQUARS já possui seus requisitos

específicos de segurança definidos e a gestão de riscos já está sendo gerida por meio de um escritório de projetos local.

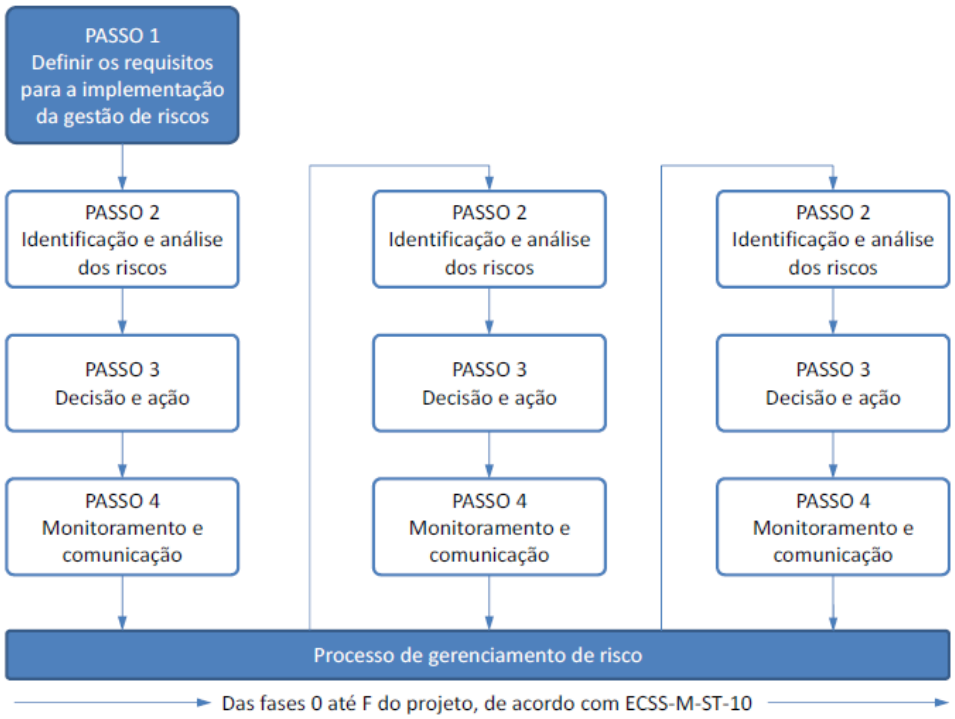
O programa EQUARS possui um plano de gerenciamento de riscos em que aborda riscos como sendo eventos incertos, com efeitos negativos nos objetivos do projeto, e especifica os processos e ferramentas para gerenciar riscos. No gerenciamento de riscos do projeto, está prevista a interação entre as equipes de safety e de gerenciamento de riscos, como ilustrado na Figura 3.7. A equipe de safety é responsável por identificar e relatar potenciais perigos ou incidentes, relacionados com o produto e os processos internos ou de fornecedores. É responsável, também, por encaminhar relatórios de perigo e incidentes, auxiliar na identificação e análise dos riscos e auxiliar na elaboração de planos de mitigação (INPE, 2017).

Figura 3.7: Atores no Processo de Gerenciamento de Risco da Missão EQUARS.

Fonte: INPE (2017).

O processo desenvolvido para o INPE, adaptado da ECSS, é iterativo e engloba quatro etapas para o gerenciamento de riscos: (i) definição de requisitos, (ii) identificação e análise de riscos, (iii) decisão e ação e (iv) monitoramento e comunicação, conforme ilustrado na Figura 3.8.

Figura 3.8: Processo de gerenciamento de risco.



Fonte: INPE (2017).

Na identificação e análise de riscos, serão realizados em reuniões com esta finalidade, o que não impede que os riscos sejam identificados e analisados fora desses eventos, de forma isolada. A partir do momento que um risco é identificado, a equipe preenche as informações necessárias referentes ao risco (INPE,2017).

O processo de *decisão e ação* pode ser acionado devido a três razões, quais sejam: novos riscos identificados ou a reabertura de riscos já fechados; solicitações especificas para análise ou avaliação do risco, após plano de ação ser incorporado; e situação em que o evento que poderia gerar o risco já foi superado. Os riscos identificados e analisados e até mesmo os reabertos devem passar pelo processo de decisão e ação, a fim de decidir qual abordagem será

realizada. Sendo assim, é necessário um alinhamento entre a equipe de gerenciamento e os que identificaram a ameaça e a equipe que executará a mitigação. Solicitações periódicas de análise ou avaliação do risco, após plano de ação ser incorporado, ocorrem devido a mudanças que ocorrem o longo do projeto. Nesse caso, novos cenários podem surgir fazendo com que os riscos já analisados mudem. Por isso, se faz necessário o monitoramento periódico. Quando um evento que poderia gerar o risco já foi superado, o risco deve ser encerrado e deverá ser explicada a razão pela qual o risco foi encerrado (INPE,2017).

Os riscos necessitam ser monitorados frequentemente ao longo do projeto. Sendo assim, na etapa de monitoramento e comunicação, o ambiente deve ser monitorado, com o objetivo de identificar novos riscos, detectar mudanças do cenário, revisar periodicamente os riscos, incorporar ações de resposta planejadas e reabrir riscos já fechados. Na comunicação entre partes interessadas, a alta gestão deve produzir relatórios quinzenais, com atualização do cenário de riscos do projeto. Os fornecedores devem produzir relatórios mensais sobre os riscos incidentes sobre suas atividades e sua tecnologia e as equipes do INPE devem produzir relatórios mensais sobre os riscos do programa (INPE,2017).

A Tabela 3.1 mostra as atividades desenvolvidas em cada etapa do processo de gerenciamento de riscos.

Tabela 3.1: Atividades desenvolvidas em cada passo do processo de gestão de riscos.

Etapa	Atividades
Passo 1	Definir a política de gerenciamento de riscos
	Elaborar o plano de gerenciamento de riscos
Passo 2	Identificar os cenários de risco
	Avaliar os riscos
Passo 3	Decidir se os riscos podem ser aceitos
	Reduzir os riscos
	Recomendar aceitação
Passo 4	Monitorar e comunicar riscos
	Submeter os riscos para aceitação (retornar à atividade 6 para riscos não aceitos)

Fonte: Adaptado de INPE (2017).

4 REQUISITOS DE SEGURANÇA DE PROJETOS ESPACIAIS

No presente capítulo, apresenta-se uma proposta de requisitos de segurança para um projeto de satélite, levando em consideração a classificação da missão por massa do satélite. Os requisitos propostos abordam a relação entre gestão de risco e garantia da segurança.

4.1 Classificação dos satélites

Konecny (2004) propôs uma classificação abrangente para satélites, de satélites grandes, com massa de toneladas, até femto nano satélites, com massas da ordem de kg, conforme apresentado na Tabela 2.20. Para chegar à uma classificação que melhor se adequasse aos projetos do INPE, efetuou-se uma adaptação desta classificação, de modo a enquadrar satélites do INPE em cada categoria proposta. Como resultado dessa classificação, gerou-se as quatro classes apresentadas abaixo na Tabela 4.1.

Tabela 4.1: Divisão proposta de satélite por categoria.

Classe	Massa
Satélite Grande	> 1000 Kg
Satélite Médio	1000 - 200 Kg
Satélite Pequeno	300 - 20 Kg
Satélite Nano	< 20 Kg

Fonte: Produção da autora.

A tabela a seguir apresenta satélites do INPE que se enquadram nas classes acima citadas.

Tabela 4.2: Satélites do INPE.

Características	Satélites			
	CBERS 4A	Amazonia 1	EQUARS	NanosatC BR1
Local de lançamento	China	Índia	EUA/Índia/Alcântara	Rússia
Lançamento	2019	2021	2023	2014
Massa	1730 Kg	640 Kg	210 Kg	1.33 Kg

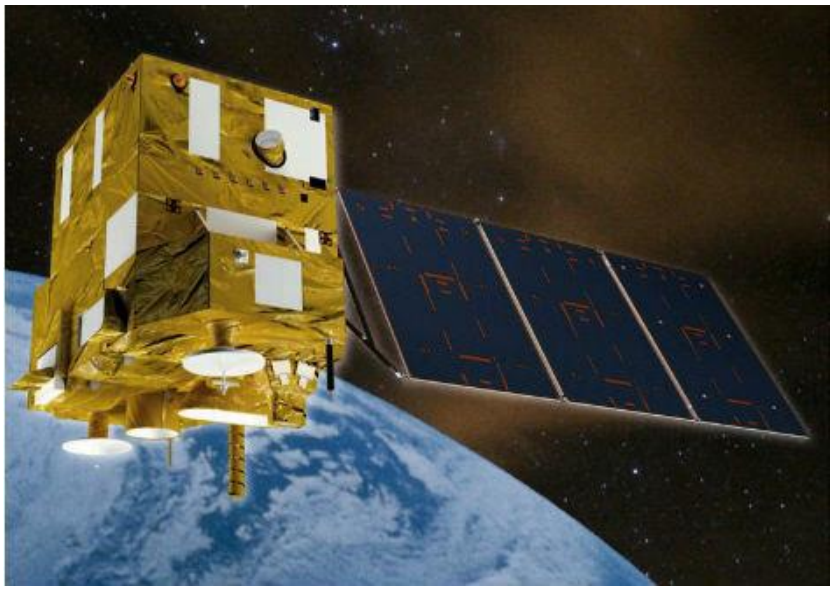
Fonte: Produção da autora.

O programa CBERS é uma parceria entre Brasil e China, que possui ao todo seis satélites de sensoriamento remoto. Suas imagens são usadas para monitorar desmatamento e queimadas na Amazônia Legal, monitorar recursos hídricos, áreas agrícolas, o crescimento urbano e ocupação do solo. (CBERS/INPE, 2020)

O CBERS 4A é um satélite de sensoriamento remoto de média resolução, sua configuração é parecida com a dos satélites CBERS-3&4, com melhorias para acomodar a nova câmera imageadora chinesa que possui qualidade superior na resolução geométrica e espectral. (CBERS/INPE, 2020)

A Figura 4.1 traz uma ilustração artística do CBERS 4A.

Figura 4.1: Representação artística do satélite CBERS 4A.

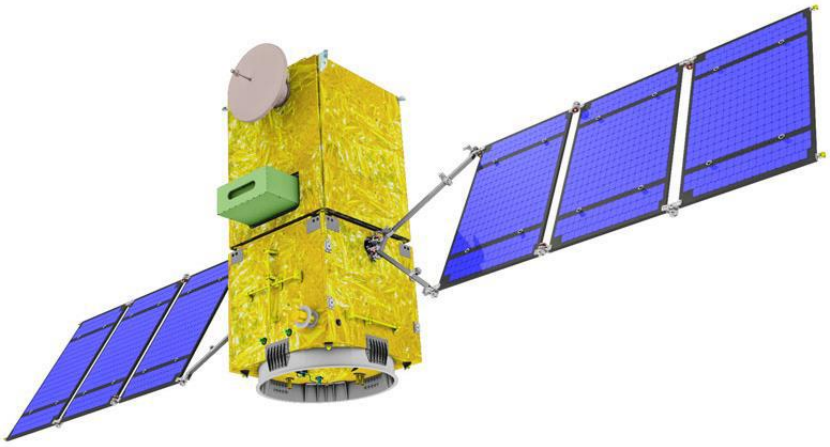


Fonte: Genaro (2019).

O Amazonia 1 é o primeiro dos satélites da missão Amazonia, que prevê três satélites: Amazonia 1, Amazonia-1B e Amazonia 2. A missão tem por objetivo gerar imagens de sensoriamento remoto para monitorar o desmatamento na região amazônica, assim como observar a agricultura de todo o território nacional. Os dados gerados ainda podem atender outras aplicações, como monitoramento de região costeira, reservatórios de água, florestas naturais e cultivadas, desastres ambientais (AMAZONIA/INPE,2020).

O satélite Amazonia 1 foi lançado em fevereiro de 2021, e é o primeiro satélite de observação da Terra a ser completamente projetado, integrado, testado e operado pelo Brasil. Sua principal característica é que sua órbita foi projetada para ter uma alta taxa de revisita o que para aplicações como alerta de desmatamento na Amazônia é de extrema importância (AMAZONIA/INPE, 2020). A Figura 4.2 demonstra uma representação artística do satélite AMAZONIA1.

Figura 4.2: Representação artística do satélite AMAZONIA 1.



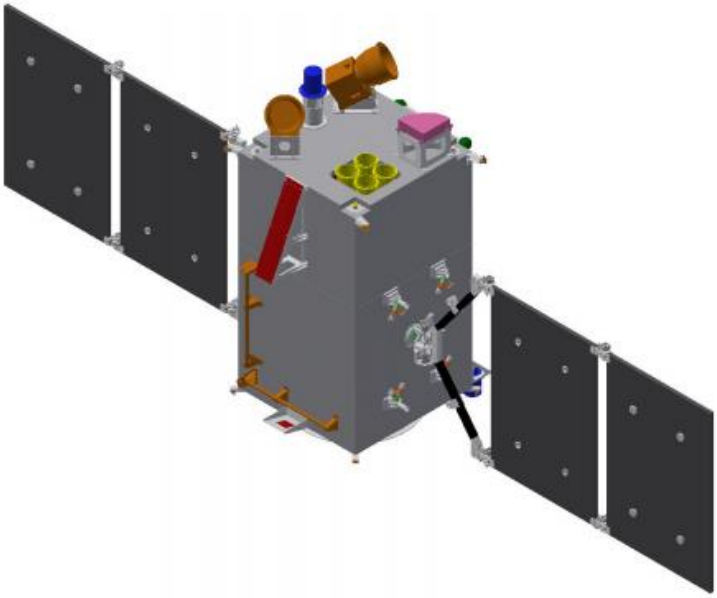
Fonte: Genaro (2019).

A missão EQUARS *Equatorial Atmosphere Research Satellite* é uma missão científica para monitorar a atmosfera de todo o globo terrestre na região equatorial com o objetivo de compreender o acoplamento atmosférico entre os processos dinâmicos, elétricos, fotoquímicos e ionosféricos, aplicando os dados obtidos em estudos de clima espacial, atmosférico e estudos climáticos (EQUARS/INPE, 2020).

A missão é composta por um satélite de pequeno porte e de custo moderado com vida útil prevista de dois anos. Seu lançamento está previsto para 2023 e será colocado em uma órbita quase circular, a 635 quilômetros de altitude e inclinação de 18 graus em relação ao plano equatorial. A

Figura 4.3 apresenta uma representação artística do satélite EQUARS.

Figura 4.3: Representação artística do satélite EQUARS.



Fonte: INPE (2019).

O NanosatC- BR1 é um satélite de missão científica e foi o primeiro cubesat nacional e foi desenvolvido pelo INPE em parceria com a Universidade Federal de Santa Maria (UFSM), além de ter o apoio da AEB, com o objetivo de capacitar recursos humanos, desenvolver áreas da ciência e tecnologias espaciais, coletar dados do Campo Magnético Terrestre sobe as regiões da anomalia magnética do sul (AMAS) e do eletrojato ionosférico equatorial sobre a região do BRASIL (NANOSATBR/INPE, 2020). O NanosatC-BR2 foi lançado em março de 2021.

A missão também tem um caráter tecnológico, onde busca testar circuitos integrados projetados no Brasil, assim como também educacional, onde através da parceria entre o INPE e a UFSM alunos podem trabalhar podem participar de todas as fases de desenvolvimento do projeto (NANOSATBR/INPE, 2020).

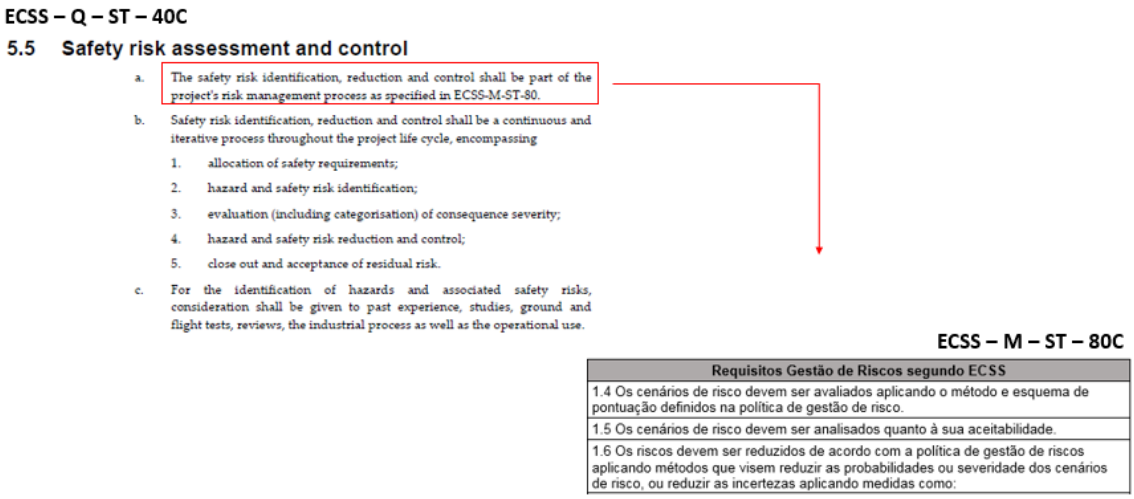
4.2 Requisitos de segurança para diferentes tipos de satélites

Genaro (2019) desenvolveu um trabalho onde com base no estudo comparativo de padrões de segurança da área espacial propôs requisitos para projetos de satélites do INPE. Para se obter uma relação de requisitos de

segurança que cumpra aos objetivos propostos, o trabalho de Genaro (2019) precisou ser adaptado de maneira a rever os requisitos propostos pela autora, verificando se existiam alguns requisitos de gestão de riscos que explicitassem a relação entre as duas disciplinas durante o desenvolvimento de um projeto espacial que não tivessem sido contemplados no levantamento de requisitos.

Ao analisar a (ECSS-Q-ST-40C) - *Space Product Assurance: Safety,* observou -se que ao tratar da avaliação e controle dos riscos de segurança o padrão determina que a identificação, redução e controle dos riscos de segurança devem ser parte integrante do gerenciamento do projeto conforme especificado pela (ECSS-M-ST-80C) – *Risk Management.* A partir disso, foram coletados os requisitos referentes ao processo de gestão de risco no padrão, conforme ilustrado pela Figura 4.4. Como resultado gerou-se uma na lista de requisitos apresentados na Tabela 4.3.

Figura 4.4: Requisitos referentes a relação entre gestão de risco e garantia da segurança.



Fonte: Produção da autora.

Tabela 4.3: Tabela de requisitos de gestão de riscos de segurança.

Requisitos de gestão de riscos de segurança
1.5.1 a) A base para a gestão de riscos deve ser o processo de quatro etapas e nove tarefas, como apresentado na ECSS-M-ST-80C
1.5.1 b) Os cenários de risco devem ser identificados de forma estruturada para todos os domínios usando como fontes de informação:
1) Análises anteriores, lições aprendidas e dados históricos;
2) Entrevistas com especialistas e dados de experiência;
3) Extrapolação de dados;
4) Simulações, dados de teste e modelos;
5) Análise detalhada de segurança e confiabilidade (consulte ECSS - Q - ST - 30 e ECSS - Q - ST - 40);
6) Análise de todas as estruturas e níveis de decomposição do trabalho;
7) Comparação de metas e planos;
8) Análise de recursos;
9) Análise de fornecedores;
10) Análise das mudanças propostas;
11) Resultado dos testes;
12) Relatórios de não conformidade;
13) consideração do cronograma;
14) Criticidade da tecnologia e disponibilidade de soluções de backup.
1.5.1 c) Os cenários de risco devem ser avaliados aplicando o método e esquema de pontuação definidos na política de gestão de risco.
1.5.1 d) Os cenários de risco devem ser analisados quanto à sua aceitabilidade.
1.5.1 e) Os riscos devem ser reduzidos de acordo com a política de gestão de riscos aplicando métodos que visem reduzir as probabilidades ou severidade dos cenários de risco, ou reduzir as incertezas aplicando medidas como:
1) Modificação de requisitos ou acordo comercial;
2) Mudança de design, *baseline* ou estrutura do projeto;
3) Introdução de tolerância a falhas de acordo com os documentos ECSS - Q - ST - ST;
4) Aquisição de recursos adicionais ou redirecionamento de recursos;
5) Aumento do teste ou análise.
1.5.1 f) As opções para aceitação dos riscos resolvidos, aceitáveis e gerais devem ser definidas quando apropriado e apresentadas ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para eliminação.
1.5.1 g) Os riscos não resolvidos devem ser apresentados ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para posterior disposição.
1.5.1 h) Os riscos residuais ao final de um ciclo de gestão de risco devem ser submetidos ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para aceitação.
1.5.1 j) Os riscos devem ser monitorados, comunicados e os resultados devem ser exibidos em conformidade com o relatório de avaliação de risco apresentado no padrão.

Fonte: Produção da autora.

Após avaliar os requisitos propostos pela autora foi identificado que existem requisitos que devem ser cumpridos pela organização e os que devem ser cumpridos pelo projeto, sendo assim, dividiu-se os requisitos em duas tabelas. A Tabela *4.4* apresenta o total de 18 requisitos levantados referente à organização de segurança e a Tabela 4.5 apresenta uma parte do total de 68 requisitos levantados referente a projeto.

Tabela 4.4: Tabela de requisitos referentes à organização de segurança.

Requisitos aplicáveis à organização
1 Programa de segurança de sistema
1.1 Escopo
1.1.1) O escopo e conteúdo do programa de segurança visam estabelecer um sistema de gestão de segurança para implementar os itens previstos nesta tabela de acordo com os requisitos do projeto espacial.
1.1.1.a) O fornecedor deve estabelecer e manter um programa de segurança de sistema.
1.1.1.b) O fornecedor deve garantir que todos os regulamentos e leis de segurança nacionais ou internacionais aplicáveis sejam identificados.
1.1.1.c) Os requisitos do programa de segurança do sistema contidos nesta tabela devem ser aplicados.
1.1.2) Adaptações não podem diminuir o grau de proteção do pessoal, de equipamento ou material de voo, de equipamento de apoio no solo, do público em geral, de propriedade pública e privada e do meio ambiente contra os riscos associados aos sistemas espaciais.
1.2 Plano do programa de segurança
1.2.1 Definição
O plano deve definir:
1.2.1.a) as tarefas do programa de segurança a serem implementadas;
1.2.1.b) o pessoal ou fornecedor responsável pela execução das tarefas;
1.2.1.c) o cronograma de tarefas do programa de segurança relacionadas aos marcos do projeto;
1.2.1.d) interface da atividade do programa de segurança com a engenharia do projeto e com outras atividades de garantia do produto;
1.2.1.e) como o fornecedor realiza as tarefas e verifica se foram concluídas satisfatoriamente (ex.: procedimentos internos).
1.2.2 Conformidade
1.2.2.a) O plano deve garantir que os requisitos e regulamentos de segurança aplicáveis a quaisquer outras instalações e serviços que sejam utilizados durante o curso do projeto sejam identificados.
1.3 Organização de segurança
1.3.1 Representante de Segurança
1.3.1.a) Cada fornecedor deve nomear um representante de segurança, qualificado por treinamento ou experiência, para desempenhar as funções de segurança do sistema, de acordo com a legislação brasileira.

continua

Tabela 4.4: Conclusão.

1.3.2 Independência
1.3.2.a) O representante de segurança deve ter acesso direto para reportar com o gerente de projeto e à alta gerência e ser independente da linha hierárquica dentro do projeto.
1.4.3 Auditorias de Segurança
1.4.3.a) O fornecedor deve realizar auditorias ou revisões de segurança para verificar a conformidade com a política e os requisitos de segurança do projeto.
1.4.3.b) As auditorias de segurança devem estar de acordo com os procedimentos estabelecidos.
1.4.3.c) O cliente deve ser informado do cronograma de auditoria.
1.4.4 Aprovação de Relatórios
1.4.4.a) O fornecedor deve permitir que os relatórios do projeto que tratam de questões relacionadas à certificação de segurança sejam emitidos com a assinatura apenas do representante de segurança.
1.4.5 Representação em Conselhos
1.4.5.a) A segurança deve estar representada em reuniões de controle de configuração (CCBs), reuniões de controle de não conformidade (NRBs), reuniões de prontidão de teste (TRBs) e em qualificações e revisões de aceitação, onde os requisitos de segurança e funções críticas de segurança estão envolvidos.
1.6.2.5 Teste Detalhado de Definição, Produção e Qualificação - Fases C / D
1.6.2.5.d) O centro de testes espaciais deve estabelecer um programa de segurança para garantir a segurança de todo o pessoal do centro de testes, incluindo o cliente e visitantes, o espécime em teste, as instalações e infraestrutura associada, de acordo com a norma ECSS-Q-ST-20-07C.

Fonte: Produção da autora.

Tabela 4.5:Tabela de requisitos referentes a projeto.

Requisitos aplicáveis a projetos
1.6.2.2 Análise da Missão / Identificação de Necessidades - Fase 0
1.6.2.2.a) O fornecedor deve preparar uma análise de segurança para dar suporte à identificação de fontes de risco de segurança, bem como a realização de análises preliminares de *trade-off* entre os conceitos de sistemas alternativos.
1.6.2.2.b) Durante a Fase 0, o fornecedor deve demonstrar que:
1) Os requisitos de segurança e as lições aprendidas de projetos anteriores foram analisados e foi dado apoio ao projeto e para ao *trade-off* do conceito de operações;
2) Os principais requisitos de segurança do sistema foram identificados.
1.6.2.3 Viabilidade - Fase A
1.6.2.3.a) A análise de segurança deve apoiar análises de *trade-off* para se chegar ao conceito que tenha um risco de segurança aceitável, considerando-se as restrições do projeto e da missão.
1.6.2.3.b) A tecnologia de projeto selecionada e o conceito operacional a ser implementado devem ser selecionados com base nos dados de análise para a arquitetura de sistema mais segura, a fim de eliminar ou reduzir os riscos a níveis aceitáveis.
1.6.2.4 Definição Preliminar - Fase B
1.6.2.4.a) A análise de segurança deve apoiar uma otimização contínua e mais detalhada da segurança do projeto e das operações do sistema, bem como a identificação dos requisitos técnicos de segurança e sua aplicabilidade.
1.6.2.4.b) A análise também deve fornecer dados para a avaliação de riscos de segurança em apoio à avaliação de riscos de segurança, identificação de contribuintes de risco no projeto e no conceito operacional.
1.6.2.5 Teste Detalhado de Definição, Produção e Qualificação - Fases C / D
1.6.2.5.a) A análise de segurança deve apoiar o projeto detalhado, produção, qualificação e teste.
1.6.2.5.b) A análise de segurança deve também apoiar a otimização da segurança operacional, a avaliação da implementação de requisitos de segurança, a verificação da redução de riscos e a aceitação de riscos.
1.6.2.5.c) A análise das operações também deve apoiar a identificação de requisitos de planejamento e treinamento de resposta a emergências e contingências, bem como o desenvolvimento de procedimentos.
1.6.2.5.e) Tarefas críticas envolvendo alto nível de risco devem ser executadas após aprovação prévia do representante de segurança do INPE.
1.6.2.6 Utilização - Fase E
1.6.2.6.a) A análise de segurança deve avaliar o projeto e as mudanças operacionais por impacto na segurança, assegurando que as margens de segurança sejam mantidas e que as operações sejam conduzidas dentro do risco aceito.
1.6.2.6.b) A análise deve também apoiar a avaliação de anomalias operacionais por impacto na segurança e a avaliação contínua das tendências de risco.

Fonte: Produção da autora.

Feito isso, renumerou-se os requisitos e criou-se uma nova tabela com quatro colunas adicionais, cada uma para cada tipo de satélite, onde é determinado se o requisito é ou não aplicável para cada tipo de satélite, conforme classificação apresentada na Tabela 4.1.

A Tabela 4.6 é um extrato da tabela apresentada no apêndice B, onde constam os requisitos mínimos de segurança abrangendo os referentes à organização e os referentes ao projeto, considerando a relação de gestão de risco de projeto e a garantia de segurança ao tratar riscos comuns ao desenvolver projetos de sistemas espaciais.

Tabela 4.6: Amostra da tabela geral de requisitos.

Requisitos aplicáveis à organização	**Grande**	**Médio**	**Pequeno**	**Nano**
1 Programa de segurança de sistema				
1.1 Escopo				
1.1.1) O escopo e conteúdo do programa de segurança visam estabelecer um sistema de gestão de segurança para implementar os itens previstos nesta tabela de acordo com os requisitos do projeto espacial.				
1.1.1.a) O fornecedor deve estabelecer e manter um programa de segurança de sistema.	A	A	A	NA
1.1.1.b) O fornecedor deve garantir que todos os regulamentos e leis de segurança nacionais ou internacionais aplicáveis sejam identificados.	A	A	A	NA
1.1.1.c) Os requisitos do programa de segurança do sistema contidos nesta tabela devem ser aplicados.	A	A	A	NA
1.1.2) Adaptações não podem diminuir o grau de proteção do pessoal, de equipamento ou material de voo, de equipamento de apoio no solo, do público em geral, de propriedade pública e privada e do meio ambiente contra os riscos associados aos sistemas espaciais.	A	A	A	A
1.2 Plano do programa de segurança				
1.2.1 Definição				
O plano deve definir:				
1.2.1.a) as tarefas do programa de segurança a serem implementadas;	A	A	A	NA
1.2.1.b) o pessoal ou fornecedor responsável pela execução das tarefas;	A	A	A	NA
1.2.1.c) o cronograma de tarefas do programa de segurança relacionadas aos marcos do projeto;	A	A	A	A
1.2.1.d) interface da atividade do programa de segurança com a engenharia do projeto e com outras atividades de garantia do produto;	A	A	A	NA
1.2.1.e) como o fornecedor realiza as tarefas e verifica se foram concluídas satisfatoriamente (ex.: procedimentos internos).	A	A	A	NA

Fonte: Produção da autora.

5 RESULTADOS E DISCUSSÃO

Este capítulo condensa e discute os resultados alcançados pela pesquisa. A fim de facilitar o entendimento, optou-se por dividir os resultados em quatro partes. A primeira parte aborda o resultado do estudo de gestão de risco e garantia de segurança tanto em padrões e normas, quanto em organizações espaciais, enquanto a segunda parte aborda o resultado do estudo sobre a relação da gestão de riscos e garantia da segurança em projetos espaciais. A terceira parte discorre sobre a dinâmica dos processos de gestão de riscos e garantia da segurança segundo instâncias organizacionais. E finalmente a quarta parte apresenta os resultados do levantamento de requisitos mínimos de segurança para diferentes tipos de satélites.

5.1 Resultado do estudo da gestão de risco e garantia da segurança em padrões e organizações da área espacial

Efetuou-se o estudo e revisão dos padrões INCOSE e PMBOK e da norma AS9100 a fim de verificar como as disciplinas de gestão de riscos e garantia da segurança são abordadas em padrões e normas da área espacial, utilizando a metodologia apresentado na Seção 1.4.2. No caso de organizações, foram efetuadas revisões relativas à NASA, ESA (ECSS) e INPE.

Em relação ao guia PMBOK, obteve-se como resultados que o guia trata a gestão de riscos como uma das áreas de conhecimento na gestão de projetos, enquanto trata a garantia da segurança como uma das áreas de conhecimento externas à gestão de projetos, a serem agregadas ao esforço do projeto conforme a necessidade. A norma AS9100, como visto na Seção 2.5.2, estabelece requisitos para um sistema de gestão da qualidade. A *Tabela* 2.2 e Tabela 2.3 resumem os requisitos preconizados pela norma para as disciplinas de gestão de riscos e gestão da segurança. Conforme o princípio de pensamento baseado em risco, preconizado pela norma, o sistema de qualidade deve abordar os riscos e oportunidades em seus próprios processos. Essencialmente, requer que as organizações avaliem o risco ao estabelecer processos, controles e

melhorias em um sistema de gestão da qualidade. A norma, em diversos requisitos, requer que a organização implemente a gestão de riscos, tanto em nível de projetos, quanto em nível da organização. Relativamente a atividades de segurança, a norma exige que a organização planeje, implemente e controle os processos necessários para garantir a segurança do produto durante o ciclo de vida do sistema desenvolvido. Este requisito pode, em princípio, ser entendido como a implementação de um processo de gestão da segurança, em nível de projeto, que supervisione e conduza as atividades de segurança com foco no sistema desenvolvido. Entende-se, também, que a norma requeira o estabelecimento de um processo de gestão da segurança na instância da organização, conforme apropriado. Referentemente à NASA, os documentos Risk Management Handbook (NASA, 2001b) e System Safety Handbook (NASA, 2011a) mostram de forma clara que tanto a gestão de risco quanto a gestão de segurança devem ser implementadas nos níveis de programas/projetos e da organização. De acordo com a ECSS, o objetivo da gestão de risco é identificar, avaliar, reduzir e aceitar os riscos do projeto espacial no que se refere ao domínio programático (custo, cronograma) e ao domínio técnico (confiabilidade, segurança). Também afirma que a análise de segurança faz parte do processo de gerenciamento de risco (ECSS, 2008a). Muito do escopo da garantia da segurança é tratado no âmbito da garantia do produto (ECSS, 2008a). No caso do INPE, questionários respondidos por gerentes de projetos de satélites, especificamente CBERS 4A, AMAZONIA-1, EQUARS e NANOSATC-BR1, conforme descrito na Seção 1.4.2, permitiram concluir-se que, correntemente, tanto a gestão de risco quanto a garantia de segurança são implementadas, concomitantemente, em projetos do INPE. Conforme apresentado na Figura 2.29.

5.2 Resultado do estudo da relação entre garantia de segurança e gestão de riscos

Para investigar a relação entre a gestão de riscos e a garantia da segurança em projetos espaciais, a metodologia descrita na Seção 1.4.3 foi seguida.

Como resultado geral, a pesquisa realizada mostrou que a relação entre a gestão de risco e a garantia de segurança não é abordada de forma explícita, em padrões de caráter geral, como os padrões AS9100, PMBOK e INCOSE. Padrões como o PMBOK, que foca a gestão de projetos, e INCOSE, que foca a engenharia de sistemas, tratam a gestão de riscos como uma atividade primária nos arcabouços propostos, enquanto que a gestão de segurança é tratada como uma atividade coadjuvante, abordada no âmbito da própria gestão de riscos e de processos de engenharia.

Ao se tratar de organizações, tal relação é abordada de forma mais clara, como pode-se constatar em padrões da ECSS, em que o padrão referente à garantia da segurança (ECSS-Q-ST-40C) explicita que riscos de segurança devem ser tratados de acordo com o especificado no padrão que trata de gestão de riscos (ECSS-M-ST-80C), Além disso, explicita que o processo de identificar, reduzir e controlar os riscos associados à segurança deve ser parte integrante da gestão de riscos do projeto. A

Figura 3.4 apresenta os limites da engenharia de sistemas, conforme padrões ECSS, e seu relacionamento com as outras disciplinas, dentre as quais a disciplina de segurança, inserida na garantia do produto, e gestão de riscos, como parte do gerenciamento do projeto.

Referentemente à NASA, percebe-se que a relação entre a gestão de riscos e a garantia da segurança é bem delineada. Risco é definido como o potencial de deficiências nos domínios de execução da missão, sendo tal definição adotada no *Systems Safety Handbook* e no *Risk Management Handbook* da agência espacial americana. A sobreposição entre a engenharia de sistemas, a gestão de riscos e a gestão da segurança, no âmbito de um sistema, encontra-se ilustrada na Figura 3.2. A Figura 3.3 ilustra a relação entre especialistas no âmbito de um processo (RIDM) da gestão de riscos. Em relação ao INPE, através de entrevistas a gerentes de projeto, observou-se que, correntemente, tanto a gestão de risco quanto a garantia de segurança são implementadas, concomitantemente, em projetos do INPE, com interação entre especialistas e responsáveis. Conforme apresentado na Figura 3.6.

5.3 Processos de gestão de riscos e segurança e instâncias organizacionais

Em uma organização, diferentes níveis da estrutura organizacional têm participação na execução de um programa/projeto. Nas organizações com estrutura matricial, a gestão do programa/projeto é realizada em uma estrutura horizontal, enquanto a estrutura vertical ou funcional fornece os recursos necessários para a execução do programa/projeto. As estruturas horizontal e vertical compartilham riscos segundo a dinâmica exposta a seguir.

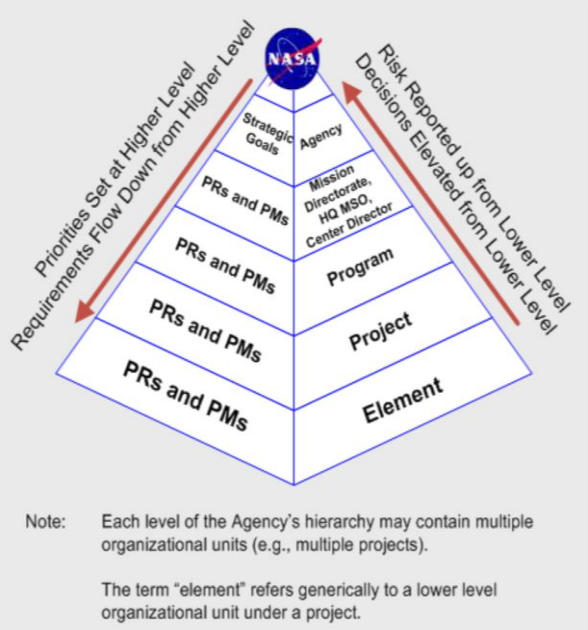
Uma visão sobre a dinâmica da alocação de risco dentro da organização pode ser obtida utilizando-se o modelo organizacional da NASA, esquematicamente reproduzido na Figura 5.1. Em uma organização, tipicamente, ocorre o fluxo descendente de objetivos de alto nível, ao longo da estrutura hierárquica. Estes objetivos se traduzem, progressivamente, em requisitos de desempenho incidentes sobre os produtos (sistemas) da organização. No caso de um programa/projeto, tais requisitos de desempenho definem, em última instância, os objetivos do programa/projeto. No âmbito deste fluxo descendente de requisitos, ao longo da hierarquia organizacional, cada unidade organizacional acorda com a(s) unidade(s) sob sua supervisão um conjunto de elementos de gestão, tais como objetivos estratégicos, produtos a serem entregues (sistemas), requisitos e medidas de desempenho, recursos, custos, cronogramas, entre outros, que definem o escopo do trabalho a ser executado pela(s) unidade(s). Assim, uma vez definidos os objetivos, cada unidade está pronta para identificar e analisar os riscos associados aos objetivos estabelecidos.

Em resposta ao fluxo descendente de objetivos organizacionais, observa-se o fluxo ascendente de informações associadas ao cumprimento destes objetivos, entre elas, informações sobre os riscos identificados ao longo da estrutura hierárquica da organização. Esta dinâmica pode ser assim descrita. No nível do programa/projeto, a equipe de gerenciamento, primeiramente, identifica e avalia os riscos para cumprir os objetivos do programa/projeto. Com base em limites de risco predefinidos, negociados entre a gestão do programa/projeto e o nível hierárquico imediatamente superior, riscos identificados podem, então, ser

transferidos do nível do programa/projeto para este nível imediatamente superior, que passa, então, a gerir tais riscos. Uma ilustração dos fluxos acima referidos é mostrada na Figura 5.1.

Em conclusão, pode-se dizer que os riscos do programa/projeto em uma organização podem ser gerenciados em diferentes níveis da organização. Como corolário, pode-se concluir que as diferentes instâncias hierárquicas de uma organização realizam atividades rotineiras de gerenciamento de riscos. Os riscos definidos localmente, em um dado nível organizacional, podem, assim, coexistir com os riscos transferidos de unidades de nível hierárquico inferior, que atuam sob a supervisão da unidade em questão. A Nasa desenvolve atividades de gestão de risco nos níveis da sede da Agência, suas instituições e seus programas e projetos.

Figura 5.1: Exemplo ilustrativo do fluxo de requisitos de desempenho e riscos do projeto ao longo da hierarquia de uma organização.



Fonte: NASA (2011b).

5.4 Resultado do levantamento de requisitos de segurança mínimos para diferentes tipos de projeto de satélite

5.4.1 Resultados da verificação de critérios para classificação de satélites

A aplicação da metodologia descrita na Seção 1.4.4 propiciou um esquema para a classificação de missões em termos da massa do satélite, a partir da classificação de Konecny (2004). Como resultado deste exercício, obteve-se a classificação apresentada na Tabela 4.1, adaptada aos projetos do INPE. Para representar e exemplificar, foram escolhidos quatro satélites do INPE, que se enquadram nessas categorias, como apresentado na Tabela 4.2.

5.4.2 Resultado do levantamento de requisitos de segurança

A fim de se obter os requisitos mínimos de segurança, aplicou-se a metodologia descrita na Seção 1.4.4. Como anteriormente abordado no Item 4.2 deste trabalho, o trabalho de Genaro (2019) precisou ser adaptado para que os requisitos propostos sejam coerentes com a relação entre gestão de riscos e garantia da segurança como demonstrado ao longo deste trabalho. Os requisitos que compõem a Seção 1.5 da tabela de requisitos presente no Apêndice B que correspondem à gestão de riscos de segurança, foram levantados a partir do padrão de gestão de riscos da ECSS (ECSS-M-ST-80C) e os selecionados foram os referentes ao processo de gestão de riscos.

Importante salientar, que há requisitos de segurança que devem ser cumpridos pela organização, assim como há os requisitos que são cumpridos pelo projeto. Dessa forma, foram identificados e divididos os requisitos que são referentes a cada um no trabalho de Genaro (2019). Como resultado final obteve-se uma tabela com uma lista de requisitos mínimos de segurança em uma coluna e quatro colunas adicionais, cada uma para cada categoria de satélite, conforme apresentado na Tabela 4.1, indicando se o requisito é aplicável ou não para cada categoria, com a seguinte legenda: (A) quando o requisito é aplicável, (NA) quando o requisito não é aplicável e (D) quando o requisito é desejável de acordo com o perfil do projeto. O produto final, se encontra no apêndice B deste trabalho.

6 CONCLUSÕES

Os projetos de sistemas espaciais constituem-se em empreendimentos de grande elaboração, em que os riscos associados à operação no ambiente espacial se sobrepõem aos riscos gerenciais, decorrentes de custos, prazos, e outros inerentes a projetos com aplicações na área espacial. Tanto a gestão de riscos quanto a gestão da segurança têm-se mostrado como disciplinas relevantes para o sucesso de missões espaciais. Esta pesquisa, além de apresentar uma revisão sobre o tratamento da gestão de riscos e da gestão de segurança em referências formais, adotadas por organizações do setor aeroespacial, procurou mostrar a existência de sobreposição dos processos de gestão de risco e de gestão de segurança, como, hoje, implementados em projetos da área espacial.

Abordaram-se, também, os possíveis níveis organizacionais em que os processos de gestão de riscos e segurança são instanciados em uma organização. A pesquisa mostrou que os riscos de um programa/projeto em uma organização podem ser gerenciados em diferentes níveis da organização, com diferentes instâncias hierárquicas realizando atividades rotineiras de gerenciamento de risco. Em uma dada instância, a gestão dos riscos definidos localmente pode coexistir com a gestão de riscos transferidos de unidades de nível inferior. Para a gestão da segurança, uma conclusão semelhante se aplica, observando-se que as questões de segurança, relativas ao sistema desenvolvido, são, geralmente, tratadas no nível do programa/projeto, enquanto as questões de segurança relativas a operações organizacionais, instalações, saúde de pessoal e requisitos normativos e legais, geralmente são tratados na instância funcional.

Observou-se que há grande superposição de escopo entre os processos de gestão de risco e segurança. A pesquisa mostrou que somente a documentação da NASA, relativa às gestões de risco e segurança, aborda a questão da superposição entre as disciplinas de gestão de risco, gestão da segurança e engenharia de sistemas.

O restante deste capítulo resume as conclusões do trabalho, estruturadas em três partes. A primeira aborda as conclusões referentes ao estudo de gestão

de risco e garantia de segurança em padrões e normas e organizações espaciais, enquanto a segunda parte aborda as conclusões sobre a relação da gestão de riscos e garantia da segurança em projetos espaciais. A terceira parte apresenta as conclusões do levantamento de requisitos mínimos de segurança para diferentes tipos de satélites. Finalmente, são apresentadas perspectivas para futuros trabalhos.

6.1 Conclusões do estudo da gestão de risco e garantia da segurança em padrões e organizações da área espacial

A norma AS9100, que fornece requisitos para a configuração de um sistema de gerenciamento da qualidade em uma organização aeroespacial, prevê requisitos referentes a gestão de riscos e garantia da segurança aplicáveis a três instâncias: organização, projeto do sistema e gerenciamentos de projeto.

O guia PMBOK dedica um capítulo à descrição do processo de gestão de riscos. São considerados os riscos que ameaçam os objetivos gerenciais do projeto como custo, cronograma, escopo e qualidade. O guia não trata de forma explícita os riscos de segurança. O manual do INCOSE aborda a gestão de riscos como um dos processos do arcabouço de engenharia de sistemas proposto. São abordados riscos gerenciais e riscos técnicos. O manual ainda discorre sobre os riscos técnicos de segurança, mas não sobre o processo da garantia da segurança.

A NASA, de forma clara, define que tanto a gestão de riscos quanto a gestão de segurança devem ser implementadas nos níveis de programas/projetos e da organização. Há manuais específicos, que detalham a gestão de risco e gestão de segurança. O documento System Safety Handbook, Vol. 2, aborda a relação entre segurança, engenharia de sistemas e gestão de riscos, em uma de suas seções. É ressaltado que o tratamento de segurança de sistemas (gestão da segurança) preconizado na literatura da NASA reconhece a sobreposição substancial entre engenharia de sistemas, gerenciamento de risco e segurança de sistema (NASA, 2104, p. 14).

A ESA, possui padrões específicos para garantia de segurança e gestão de riscos. O padrão *Space Project Management: Risk Management* (ECSS-M-

ST-80C) aborda os processos e requisitos para conduzir a gestão de riscos de um projeto espacial. O padrão *Space product assurance: Safety* (ECSS-Q-ST-40C) define o programa e os requisitos técnicos de segurança.

No INPE gestão de riscos é executada pelo gerente de projeto e em sua maioria é feita a nível de sistema. Não há documentos dedicados para a gestão de riscos de projetos do INPE., sendo assim a metodologia utilizada para tal é a preconizada pela ECSS e pelo PMBOK. Referente a disciplina de garantia da segurança, esta só foi formalmente incluída na estrutura de serviço da instituição no ano de 2016, o que impossibilitou a definição de requisitos dedicados de segurança desde o início dos projetos. Atualmente, o INPE possui um documento de requisitos para garantia do produto, que inclui as disciplinas de segurança, dependabilidade e qualidade.

6.2 Conclusão do estudo da relação entre garantia de segurança e gestão de riscos

Enquanto a gestão de riscos procura identificar e tratar os riscos do projeto, para que não se tornem uma ameaça ao sucesso da missão, a gestão de segurança visa garantir que a exposição aos perigos que atingem a missão ou ponham em perigo equipes, instalações e o meio ambiente sejam mantidos em um nível aceitável. Esta pesquisa procurou mostrar, a partir de um estudo de diferentes referências para organizações aeroespaciais, que pode haver uma grande sobreposição dos processos de gestão de risco e de gestão de segurança, quando operacionalizados em um projeto, sugerindo que há espaço para sinergias de atuação entre as equipes responsáveis pelas gestões de risco e de segurança, principalmente no tratamento de riscos técnicos comuns.

Observou-se que apesar da superposição de escopo entre os processos de gestão de risco e segurança, ainda há muito espaço para melhorias na maioria das referências estudadas no que se refere à descrição da relação entre esses dois processos, bem como no que diz respeito a relações entre engenharia de sistemas, gestão de riscos e gestão da segurança e, por fim, às instâncias organizacionais em que esses processos podem ocorrer concomitantemente.

6.3 Conclusão do levantamento de requisitos de segurança mínimos para diferentes tipos de projeto de satélite

De acordo com o quadro contendo o conjunto de requisitos mínimos de segurança apresentados no Apêndice B verificou-se que para as categorias de pequeno, médio e grande porte todos os requisitos propostos são aplicáveis. Para a categoria de nano, alguns requisitos relacionados ao programa de segurança de uma organização não são aplicáveis, pois existem projetos de nanosatélites que não são desenvolvidos por organizações, tornando assim, inviável a aplicação de tais requisitos. Ainda referente a categoria de nano, alguns requisitos relativos a fases do projeto e ciclo de revisão de segurança foram classificados como desejável mas não mandatório, pois segundo a classificação usada neste trabalho, a categoria engloba desde satélites simples desenvolvidos por estudantes com massa inferior a 1kg até satélites mais complexos com painel solar e dispositivos de separação pirotécnicos com massa de até 20kg. No caso desses satélites mais complexos, tais requisitos são desejáveis.

Ao se analisar o questionário presente neste trabalho, pode-se constatar que em 50% dos projetos estudados os riscos foram tratados de maneira informal durante a execução do projeto, salientando a importância e a necessidade de um conjunto de requisitos mínimos para os futuros projetos do INPE. Em 75% dos projetos do INPE estudados não fazem atualização ou revisão relativa à garantia da segurança ao final de cada fase do ciclo de vida com emissão de relatório, o que segundo os requisitos 1.6.2.1.(b) e 1.6.2.1.(c) contidos no Apêndice B mostram ser aplicáveis para os próximos satélites a serem desenvolvidos.

6.4 Perspectiva de trabalhos futuros

Para trabalhos futuros propõe-se o detalhamento da proposta de relacionamento entre gestão de risco e gestão da segurança em projetos da área espacial, focando o tratamento de riscos comuns. Bem como o desenvolvimento de uma metodologia de gestão integrada de riscos e segurança para projetos na área espacial.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA ESPACIAL BRASILEIRA - AEB. **Regulamentos de segurança do setor espacial.** 2007. Disponível em: https://www.gov.br/aeb/pt-br/servicos/regulamentos-de-seguranca-do-setor-espacial**.** Acesso em: 16 mar. 2020.

BOTELHO, A. S., XAVIER JUNIOR, A.L. A unified satellite taxonomy proposal based on mass and size. **Advances in Aerospace Science and Technology**, v.4, p. 57-73, 2019. Disponível em: https://www.scirp.org/journal/paperinformation.aspx?paperid=96030. Acesso em: 12 jul. 2020.

BRASIL - IMPRENSA NACIONAL. Portaria nº 62 de 9 de maio de 2017. **Diário Oficial Da União,** 2017, Disponível em: <https://www.in.gov.br/materia/ /asset_publisher/Kujrw0TZC2Mb/content/id/20203422/do1-2017-05-10-portaria-n-62-de-9-de-maio-de-2017-20203238>. Acesso em: 20 fev. 2021.

DEPARTMENT OF DEFENSE (DOD). **MIL-STD-882C:** standard practice for system safety. USA,1993. 117p.

DEPARTMENT OF DEFENSE (DOD). **MIL-STD-882D:** standard practice for system safety. USA, 2000.31p

DEPARTMENT OF DEFENSE (DOD). **MIL-STD-882E:** standard practice: system safety. USA, 2012. 104p.

DEZFULI, H.; EVERETT, C.; BENJAMIN, A.; YOUNGBLOOD, B.; FEATHER, M. The role of NASA thresholds and goals in achieving adequate safety. In: PROBABILISTIC SAFETY ASSESSMENT AND MANAGEMENT PSAM, 12., 2014, Honolulu, Hawaii. **Proceedings…** 2014. Disponível em: https://www.researchgate.net/publication/320353112_The_Role_of_NASA_Safety_Thresholds_and_Goals_in_Achieving_Adequate_Safety. Acesso em: 7 fev. 2019.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-E-ST-10C:** space engineering: system engineering general requirements. The Netherlands, 2017b.116p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-MST-10C:** space project management: project planning and implementation. The Netherlands, 2009. 50p

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-M-ST-80C:** space management: risk management. The Netherlands, 2008a. 43p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-Q-ST-20C:** space product assurance- quality assurance. The Netherlands, 2018. 68p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-Q-ST-40-02C:** space product assurance: hazard analysis. The Netherlands, 2008b. 36p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-Q-ST-40C:** space product assurance: safety. The Netherlands, 2017a. 79p.

EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS). **ECSS-S-ST-00-01C:** glossary of terms. The Netherlands, 2012. 63p.

EUROPEAN SPACE AGENCY (ESA). **Type of orbits**. 2020. Disponível em: https://www.esa.int/Enabling_Support/Space_Transportation/Types_of_orbits. Acesso em: 20 abr. 2020.

GENARO, A. F. S. **Levantamento e implementação de requisitos de segurança de sistemas espaciais durante o ciclo de vida de projetos de satélites**. 2019. 130p. Monografia (Especialização em Engenharia de Segurança do Trabalho) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2019.

GENARO, A.F.S. **Segurança de sistemas espaciais melhores práticas para o sucesso da missão**. São José dos Campos: INPE, 2018. Notas de aula.

GIL, A. C. **Como elaborar projetos de pesquisa**. 4.ed. São Paulo: Atlas, 2002. 175p.

INSTITUTO NACIONAL DE PEQUISAS ESPACIAIS - INPE. **Análise de arquitetura mecânica: p**rojeto EQUARS. São José dos Campos: INPE, 2019. 120p.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS – INPE. **CBERS/INPE**. 2019. Disponível em: http://www.cbers.inpe.br/sobre/cbers04a.php. Acesso em: 15 set. 2020.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - INPE. **AMAZONIA/INPE**. 2016 Disponível em: http://www.inpe.br/amazonia1. Acesso em: 13 set. 2020.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - INPE. **EQUARS/INPE**. 2020. Disponível em: http://www.dae.inpe.br/equars/. Acesso em: 20 ago. 2020.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - INPE. **NANOSATBR/INPE**. 2018. Disponível em: http://www.inpe.br/crs/nanosat/missao/nanosatc_br1.php. Acesso em: 13 set. 2020.

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - INPE. **Plano de gerenciamento de riscos:** projeto EQUARS. São José dos Campos: INPE, 2017. 24p.

INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING (INCOSE). **Systems engineering handbook:** a guide for system life cycle processes and activities. San Diego, 2015.

KONECNY, G. Small satellites: a tool for Earth observation? In: INTERNATIONAL SOCIETY FOR PHOTOGRAMMETRY AND REMOTE SENSING, 35., 2004, Istanbul, Turkey. **Proceedings...** 2004. p. 580-582. Disponível em: https://www.isprs.org/proceedings/XXXV/congress/comm4/papers/428.pdf/. Acesso em: 1 jun. 2020.

KRAMER, H.J.; CRACKNELL, A. P. An overview of small satellites in remote sensing. **International Journal of Remote Sensing**, v.29, n.15, p. 4285-4337, 2008. Disponível em: https://www.tandfonline.com/doi/full/10.1080/01431160801914952. Acesso em: 10 jun. 2020.

LEVENSON, N. An introduction to system safety. **ASK Magazine,** v.31, p 20-24, 2008. Disponível em: https://appel.nasa.gov/2008/06/01/an-introduction-to-system-safety. Acesso em: 10 jul. 2020.

LOUREIRO, G. **A systems engineering and concurrent engineering framework for the integrated development of complex products**. 1999. 607p. Tese (Doutorado em Manufacturing Engineering) - Loughborough University, Loughborough, 1999.

MARSHALL, Y. Y. Introduction to space safety. In**:** MUSGRAVE, G.E; LARSEN, A.M; SGOBBA, T. (Ed). **Safety design for space systems**. Oxford, UK: Elsevier, 2009. p. 1-5.

MUSGRAVE, G.E; LARSEN, A. M; SGOBBA, T. **Safety design for space systems**. Oxford, UK: Elsevier, 2009. 919p.

NAG, S.; LEMOIGNE, J.;DE WECK, O. Cost and risk analysis of small satellite constellations for Earth observation. In: AEROSPACE CONFERENCE, 35, 2014, Big Sky, Montana. **Proceedings…** IEEE, 2014. p. 1-16. Disponível em: https://ieeexplore.ieee.org/document/6836396. Acesso em: 12 jul. 2020.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Policy directive:** NASA policy for safety and mission success. NPD 8700.1E. Washington DC: NASA, 2008. 7p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Procedural requirements**: agency risk management procedural requirements. NPR-8000.4B, Washington DC: NASA, 2017a. 32p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Procedural requirements:** NASA general safety program requirements. NPR 8715.3D. Washington DC: NASA, 2017. 63p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Risk management handbook**. NASA/SP-2011-3422. Washington D.C: NASA, 2011b. 256p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **State of the art:** small spacecraft technology. NASA/TP—2020–5008734 Washington DC: NASA, 2020b. 327p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **System safety handbook volume 1:** system safety framework and concepts for implementation. NASA/SP-2010-580. Washington DC: NASA, 2011a. 120p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **System safety handbook volume 2:** system safety concepts guidelines and implementation examples. NASA/SP-2014-612. Washington DC: NASA, 2014.216p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Systems engineering handbook**. NASA SP-2016-6105 Rev2. Washington DC: NASA, 2016. 297p.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Earth observatory**. 2009. Disponível em: https://earthobservatory.nasa.gov/features/OrbitsCatalog. Acesso em: 12 abr. 2020.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Engineering and safety center technical update NESC**. 2018. Disponível em: https://www.nasa.gov/sites/default/files/atoms/files/nesc_technical_update_2018_-_2-page_view.pdf. Acesso em: 8 jul. 2019.

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **Missions**. 2020. Disponível em: https://www.nasa.gov/missions/. Acesso em: 5 abr. 2020c

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION - NASA. **What are SmallSats and CubeSats?**. 2015. Disponível em: https://www.nasa.gov/content/what-are-smallsats-and-cubesats. Acesso em: 10 mai. 2020b.

OLIVEIRA, F. **Caminhos para o espaço:** 30 anos do INPE. São José dos Campos: Contexto, 1991.112p.

PESSOTA, F. A. **Uma estratégia para tratamento de falhas sistêmicas (FDIR) em ACDHS de satélites de pequeno e médio porte INPE.** 2018. 291p. Tese (Doutorado em Engenharia e Gerenciamento de Sistemas Espaciais) – Instituto Nacional de Pesquisas Espaciais (INPE), São José dos Campos, 2018.

PROJECT MANAGEMENT INSTITUTE - PMI. **A guide to the project management body of knowledge:** PMBOK guide. 5 ed. Pennsylvania -USA: PMI, 2013. 589p

PROJECT MANAGEMENT INSTITUTE - PMI. **Um guia do conjunto de conhecimento em gerenciamento de projetos:** guia PMBOK. 6 ed. Pennsylvania -USA: PMI, 2017. 726p.

ROGERS, A. Q.; HUANG, P. M.; WELLS, V. E.; DARRIN, M. A.; SUTER, J. J. Small satellite initiatives: building on success. In: SPACE SYMPOSIUM, 30., 2014, Colorado Springs, USA. **Proceedings…** 2014. Disponível em: https://www.spacesymposium.org/wp-content/uploads/2017/10/A.Rogers_30th_Space_Symposium_Tech_Track.pdf. Acesso em: 11 ago. 2020.

SIMÃO, V. G.; BONINA, N.; LIMA, G. B. A.; QUELHAS, O. L. G.; MEIRIÑO, M. J. Análise comparativa entre as normas ABNT NBR ISO 9001:2015 e a ABNT NBR ISO 31000:2009: a mentalidade de riscos nos sistemas de gestão da qualidade. **Sistemas & Gestão**, v.14, n.3, p. 310 – 322, 2019. Disponível em: https://www.revistasg.uff.br/sg/article/view/1430/pdf. Acesso em: 5 dez. 2020.

SOCIETY OF AUTOMOTIVE ENGINEERING (SAE). **AS9100D: aerospace standard quality management systems:** requirements for aviation, space and defense organizations. [S.l.]: SAE, 2016. 54p

SOUZA, P. N. **Curso introdutório em tecnologia de satélites:** missões e segmentos. São José dos Campos -SP: INPE, 2002. Notas de aula. Disponível em: http://mtc-m21c.sid.inpe.br/col/sid.inpe.br/mtc-m21c/2019/08.22.14.06/doc/120_Missoes%20e%20Segmentos_P1.2_v1_2002.pdf. Acesso em: 15 fev. 2021.

SWEETING, M.N. Modern small satellites: changing the economics of space. **Proceedings of the IEEE**, v.106, n.3, p,343–361, 2018. Disponível em: https://ieeexplore.ieee.org/document/8303876. Acesso em: 15 jun. 2020.

YASSUDA, I. S; PERONDI, L. F. Estudo comparativo entre a gestão de projetos no setor espacial conforme padrão ECSS e projetos realizados pelo INPE. In: WORKSHOP EM ENGENHARIA E TECNOLOGIA ESPACIAIS, 1. (WETE)., 2010, São José dos Campos. **Anais...** São José dos Campos: INPE, 2010. Disponível em: http://urlib.net/rep/8JMKD3MGP7W/399KHUF. Acesso em: 7 mar. 2020.

APÊNDICE A

Quadro A.1: Requisitos de Gestão de Riscos Levantados ECSS.

Requisitos Gestão de Riscos segundo ECSS
1 Processo de gestão de risco
1.1 a) A base para a gestão de riscos deve ser o processo de quatro etapas e nove tarefas, como apresentado no padrão. O ponto de partida para a gestão de risco deve ser a formulação da política de gestão de risco no início do projeto.
1.1 b) A política de gestão de riscos deve:
1) Atender aos requisitos do cliente;
2) Cobrir todos os domínios do projeto, como gerenciamento, engenharia, desempenho, cronograma e custo;
3) Levar em consideração os recursos do projeto, como margens no cronograma, custo, desempenho e energia
4) Estabelecer critérios de pontuação e classificação de risco que permitam ações e decisões sobre o tratamento de riscos individuais e globais;
5) Definir requisitos para gestão de risco.
1.2 O plano de gestão de risco deve ser estabelecido por cada fornecedor em conformidade com a norma.
1.3 Os cenários de risco devem ser identificados de forma estruturada para todos os domínios usando como fontes de informação:
1) Análises anteriores, lições aprendidas e dados históricos;
2) Entrevistas com especialistas e dados de experiência;
3) Extrapolação de dados;
4) Simulações, dados de teste e modelos;
5) Análise detalhada de segurança e confiabilidade (consulte ECSS - Q - ST - 30 e ECSS - Q - ST - 40);
6) Análise de todas as estruturas e níveis de decomposição do trabalho;
7) Comparação de metas e planos;
8) Análise de recursos;
9) Análise de fornecedores;
10) Análise das mudanças propostas;
11) Resultado dos testes;
12) Relatórios de não conformidade;
13) consideração do cronograma;
14) Criticidade da tecnologia e disponibilidade de soluções de backup.
1.4 Os cenários de risco devem ser avaliados aplicando o método e esquema de pontuação definidos na política de gestão de risco.
1.5 Os cenários de risco devem ser analisados quanto à sua aceitabilidade.

continua

Quadro A.1: Continuação

Requisitos Gestão de Riscos segundo ECSS
1.6 Os riscos devem ser reduzidos de acordo com a política de gestão de riscos aplicando métodos que visem reduzir as probabilidades ou severidade dos cenários de risco, ou reduzir as incertezas aplicando medidas como:
1) Modificação de requisitos ou acordo comercial;
2) Mudança de design, *baseline* ou estrutura do projeto;
3) Introdução de tolerância a falhas de acordo com os documentos ECSS - Q - ST
4) Aquisição de recursos adicionais ou redirecionamento de recursos;
5) Aumento do teste ou análise.
1.7 O risco geral após consideração da redução de risco deve ser determinado.
1.8 As opções para aceitação dos riscos resolvidos, aceitáveis e gerais devem ser definidas quando apropriado e apresentadas ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para eliminação.
1.9 Os riscos não resolvidos devem ser apresentados ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para posterior disposição.
1.10 Os riscos residuais ao final de um ciclo de gestão de risco devem ser submetidos ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para aceitação.
1.11 Os riscos devem ser monitorados, comunicados e os resultados devem ser exibidos em conformidade com o relatório de avaliação de risco apresentado no padrão.
2 Implementação de gestão de risco
2.1 a) A gestão de riscos deve ser implementada em cada nível da rede cliente-fornecedor.
2.1 b) Em cada nível da rede cliente-fornecedor, as informações de risco recebidas do nível inferior devem ser integradas e avaliadas para relatar informações consolidadas.
2.2 A gestão de riscos deve ser implementada de maneira econômica, usando ao máximo a organização do projeto existente.
2.3 O processo de gestão de riscos deve ser monitorado.
2.4 Exercícios de lições aprendidas sobre o processo de gestão de risco devem ser realizados.
2.5 As melhorias reconhecidas no processo de gestão de riscos devem ser implementadas com o andamento do projeto.
2.6 Considerações gerais
2.6.1 a) A gestão de riscos deve ser realizada dentro da estrutura normal de gestão de projetos, garantindo uma identificação sistemática dos riscos, avaliação e acompanhamento dos riscos.
2.6.1 b) A gestão de riscos deve ser implementada como um esforço de equipe, com tarefas e responsabilidades atribuídas às funções e indivíduos dentro da organização do projeto com os conhecimentos mais relevantes nas áreas relacionadas a um determinado risco. É um esforço colaborativo de todos os atores do projeto de diferentes disciplinas.

continua

Quadro A.1: Continuação

Requisitos Gestão de Riscos segundo ECSS
2.6.1 c) Os resultados da gestão de riscos devem ser considerados no processo de gerenciamento de projetos de rotina e nas decisões relativas à evolução da *baseline.*
2.6.1 d) A gestão de riscos deve basear-se tanto quanto possível na documentação existente.
2.7 Responsabilidades
2.7.1 a) As responsabilidades pelos assuntos de gestão de riscos dentro da organização do projeto devem ser descritas no plano de gestão de riscos de acordo com a política de gestão de riscos. A seguinte abordagem se aplica:
1) O gerente de projeto atua como o integrador da função de gestão de risco em todos os domínios do projeto em questão. O gerente de projeto tem responsabilidade geral pela gestão de risco integrado dentro de um projeto e relata os resultados da tarefa de gestão de risco para o próximo nível superior na cadeia de clientes / fornecedores. O gerente de projeto define quem no projeto é responsável pelo controle dos riscos em seus respectivos domínios, e quais são suas linhas de comunicação, informação e relatórios e responsabilidades para questões de gestão de risco.
2) Cada domínio de projeto (como engenharia, software, verificação e controle de cronograma) gerencia os riscos que emanam de seu domínio ou que são atribuídos a ele para tratamento, sob a supervisão do gerente de projeto.
3) Os riscos são formalmente aceitos pelo próximo nível de responsabilidade superior na cadeia de clientes / fornecedores.
2.8 Considerações do ciclo de vida do projeto
2. 8.1 a) As atividades de gestão de risco devem ocorrer durante todas as fases do projeto. As seguintes atividades do projeto estão relacionadas com a gestão de risco:
1) Estudos de viabilidade do projeto, negócios e análises (como design, produção, segurança, confiabilidade e operações).
2) A alocação de tarefas, mão de obra e recursos de acordo com a classificação de riscos.
3) A evolução do conceito técnico através da avaliação de risco iterativa.
4) Avaliação de mudanças para impacto de risco.
5) O desenvolvimento, qualificação, aceitação e execução do projeto usando a avaliação de risco como ferramenta de diagnóstico e para identificação de ações corretivas.
6) Avaliação do status de risco geral dos projetos como parte de todas as revisões formais do projeto.

continua

Quadro A.1: Conclusão.

Requisitos Gestão de Riscos segundo ECSS
2.9 Visibilidade de risco e tomada de decisão
2.9.1 a) Os processos de gerenciamento e o fluxo de informações dentro da organização do projeto garantem uma alta visibilidade do risco predominante. As informações de risco devem ser apresentadas para apoiar a tomada de decisão da gestão, incluindo um sistema de alerta para novos riscos
2.9.1 b) Os planos de ação devem ser preparados cobrindo todos os itens de risco pendentes cujas magnitudes estão acima do nível especificado na política de gestão de risco do projeto para aumentar sua visibilidade, para permitir a tomada de decisão rápida e para garantir que seu status seja regularmente informado ao nível de gestão relevante, e para todos os atores impactados pelas consequências do risco.
2.9.1 c) As informações sobre todos os riscos identificados e sua disposição devem ser mantidas em um registro
2.10 Documentação de gestão de risco
2.10.1 a) Os documentos de gestão de risco devem ser mantidos de forma que cada etapa do processo de gestão de risco e os principais resultados e decisões da gestão de risco sejam rastreáveis e defensáveis
2.10.1 b) O processo de gestão de risco deve ser baseado nos dados existentes do projeto o máximo possível, mas a documentação estabelecida especificamente para gestão de risco inclui informações sobre a política de gestão de risco específica do projeto; objetivos e escopo; o plano de gestão de risco; os cenários identificados; probabilidade de eventos; resultados de risco; decisões de risco; registros de redução de riscos e ações de verificação; dados de tendência de risco; e dados de aceitação de risco.
2.10.1 c) Os dados provenientes das atividades de gestão de risco devem ser registrados em um banco de dados de gestão de risco contendo todos os dados necessários para gerenciar os riscos e devem documentar a evolução dos riscos ao longo de toda a duração do projeto. O banco de dados é um documento vivo e é mantido atualizado. Extratos do banco de dados são apresentados em reuniões, revisões e marcos do projeto, conforme exigido pelo plano de gestão de risco. Os itens a serem candidatos a “lições aprendidas” são identificados. O banco de dados está acessível aos atores conforme apropriado.

Fonte: Adaptado de ECSS (2008a).

Quadro A.2: Requisitos de garantia da Segurança Levantados ECSS.

Requisitos Garantia da Segurança Segundo ECSS
1 Programa de segurança de sistema
1.1 Escopo
1.1 a) O fornecedor deve estabelecer e manter um programa de segurança para garantir a conformidade com a política e os requisitos de segurança do projeto.
1.1 b) O programa de segurança deve estabelecer um sistema de gestão de segurança para implementar as disposições desta Norma - compatível com os requisitos do programa e adaptado pelo cliente
1.2 Plano do programa de segurança
1.2 a) O fornecedor deve estabelecer e manter um plano de programa de segurança em conformidade com o DRD no Anexo B da referida norma.
1.2 b) O fornecedor deve cobrir, em seu plano de programa de segurança, as tarefas de segurança para as fases do projeto em conformidade com as tarefas e análises do programa de segurança.
1.3 Conformidade
1.3 a) O fornecedor deve cumprir todos os regulamentos de segurança nacionais ou internacionais aplicáveis.
1.3 b) A implementação dos requisitos de segurança não deve ser comprometida por outros requisitos.
1.4 Organização de segurança
1.4.1 Gerente de Segurança
1.3.1 a) Cada fornecedor deve nomear um gerente de segurança com treinamento ou experiência apropriados
1.3.1 b) O gerente de segurança deve ter autoridade organizacional e independência para:
1)Estabelecer e manter um programa de segurança de acordo com os requisitos de segurança do projeto
2) Gerenciar todos os aspectos de garantia de segurança do projeto do sistema (incluindo software) e sua operação de acordo com o Plano de Segurança
3) Coordenar as interfaces: (a) com os organismos relevantes envolvidos no projeto de acordo com o plano de segurança, (b) com a autoridade do lançador de segurança.
1.4.2 Acesso e autoridade do gerente de segurança
1.4.2.1 Acesso
1.3.2.1 a) O gerente de segurança deve:
1) ter o direito de acesso aos dados relacionados à segurança relevantes para a segurança do projeto em conformidade com ECSS-M-ST-40,
2) ter acesso desimpedido a qualquer nível de gerenciamento sem restrição organizacional em qualquer aspecto da segurança do projeto.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
1.4.2.2 Autoridade
1.3.2.2 a) O gerente de segurança ou autoridade relevante de segurança deve ter autoridade para:
1) rejeitar qualquer documento de projeto ou interromper qualquer atividade de projeto que não esteja em conformidade com os requisitos ou procedimentos de segurança aprovados
2) interromper as operações perigosas quando ficar claro pelo Gerente de Segurança que a operação não está em conformidade com as medidas acordadas definidas no relatório de perigo correspondente e no procedimento de perigo aprovado derivado.
1.4.2.3 Auditorias de Segurança
1.3.2.3.a) O fornecedor deve realizar auditorias ou revisões de segurança para verificar a conformidade com a política e os requisitos de segurança do projeto.
1.3.2.3.b) As auditorias de segurança devem estar de acordo com ECSS-M-ST-10 e ECSS-Q-ST-10.
1.3.2.3.c) O cliente deve ser informado do cronograma de auditoria.
1.4.2.4 Aprovação da documentação
1.3.2.4.a) A documentação relacionada à segurança deve ser aprovada pelo gerente de segurança após sua verificação de integridade, conformidade com os requisitos de segurança declarados e fechamento formal de itens de verificação de segurança abertos (conforme definido e acordado durante auditorias e análises de segurança)
1.4.2.5 Aprovação de operações perigosas
1.3.2.5 a) O gerente de segurança (ou um representante designado) deve ter concluído a revisão e aprovado qualquer operação perigosa antes de ser executada.
1.4.2.6 Representação em conselhos
1.3.2.6 a) O gerente de segurança ou delegado designado deve ser representado nas comitê de controle de configuração (CCBs), comitê de revisão de não conformidade (NRBs), comitê de revisão de teste (TRBs) e nas revisões de qualificação e aceitação, onde os requisitos de segurança e funções críticas de segurança estão envolvidas.
1.3.2.6 b) A função de segurança deve ser ainda representada em todos os conselhos que tratam de questões de saúde onde os limites de exposição ou resistência são definidos para as tripulações de vôo e de solo.
1.4.2.7 Autoridade de aprovação de segurança
1.3.2.7 a) A autoridade de aprovação de segurança deve:
1) analisar e descartar os envios de dados de segurança
2) aprovar o encerramento de perigos
3) decidir sobre desvios e *waivers*
4) aceitar a declaração de conformidade de segurança

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
1.5 Avaliação e controle de risco de segurança
1.5 a) A identificação, redução e controle dos riscos de segurança devem fazer parte do processo de gestão de riscos do projeto, conforme especificado na ECSS-M-ST-80.
1.5 b) A identificação, redução e controle de riscos de segurança deve ser um processo contínuo e iterativo ao longo do ciclo de vida do projeto, executando-se as seguintes atividades:
1) atribuição de requisitos de segurança;
2) identificação de perigos;
3) avaliação de perigos;
4) prevenção, redução e controle de perigos; e
5) encerramento do perigo, incluindo aceitação de risco residual.
1.5 c) Para a identificação de perigos e riscos de segurança deve-se levar em consideração a experiência anterior, estudos, testes de solo e de vôo, análises críticas, o processo industrial, bem como o uso operacional.
1.6 Itens críticos de segurança
1.6 a) Os itens críticos de segurança devem fazer parte do programa geral de controle de itens críticos do projeto, conforme especificado no padrão de Controle de item crítico
1.7 Fases do projeto e ciclo de revisão de segurança
1.7.1 Tarefas e revisões do programa de segurança
1.7.1.1 Análise da Missão / Identificação de Necessidades - Fase 0
1.6.2.2.a) A análise de segurança deve apoiar a identificação de fontes de risco de segurança, bem como o desempenho de análises preliminares de trade-off entre conceitos de sistema alternativos.
1.6.2.2.b) As seguintes tarefas do programa de segurança devem ser aplicadas aos programas de voo espacial humano e sistemas críticos de segurança:
1) Analisar os requisitos de segurança e as lições aprendidas de missões anteriores semelhantes.
2) Realizar análises preliminares de risco do sistema proposto e do conceito de operações para apoiar as compensações de conceito
3) Realizar avaliação comparativa de risco de segurança das opções de conceito
4) Identificar os requisitos de segurança que são relevantes para o projeto.
5) Planejar as atividades de segurança para a fase de viabilidade.
6) Apoiar a revisão da definição de missão

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
1.7.1.2 Viabilidade - Fase A
1.6.2.3.a) A análise de segurança deve apoiar análises de *trade-off* para chegar ao conceito que tem risco de segurança aceitável, considerando-se as restrições projeto e as restrições da missão.
1.6.2.3.b) A tecnologia de projeto selecionada e o conceito operacional a ser implementado devem ser selecionados com base nos dados de análise para a arquitetura de sistema mais segura, para eliminar ou reduzir os riscos a níveis aceitáveis.
1.6.2.3.c) As seguintes tarefas do programa de segurança devem ser aplicadas aos programas de vôo espacial humano e sistemas críticos de segurança:
1) Iniciar análises de risco dos conceitos de projeto e operações, a fim de identificar os riscos aplicáveis a nível de sistema, condições perigosas e eventos e potenciais consequências perigosas
2) Apoiar negociações de conceito, identificando aspectos críticos de segurança das opções de conceito.
3) Aplicar a eliminação e minimização de perigos e fazer recomendações de segurança;
4) Realizar avaliações comparativas de risco de segurança das opções de conceito;
5) Identificar funções críticas de segurança em nível de sistema;
6) Identificar requisitos de segurança específicos do projeto a nível de sistema;
7) Planejar atividades de segurança para a fase de definição do projeto;
8) Apoiar a revisão de requisitos preliminares.
1.7.1.3 Definição Preliminar - Fase B
1.6.2.4.a) A análise de segurança deve apoiar uma otimização contínua e mais detalhada da segurança do projeto e das operações do sistema, bem como a identificação dos requisitos técnicos de segurança e sua aplicabilidade.
1.6.2.4.b) A análise também deve fornecer entradas para a avaliação de risco de segurança em apoio à avaliação de risco de segurança, a identificação dos contribuintes de risco no projeto e no conceito operacional.
1.6.2.4 c) As seguintes tarefas do programa de segurança devem ser aplicadas aos programas de vôo espacial humano e sistemas críticos de segurança:
1) Atualizar a análise de risco em apoio às atividades de definição de conceito de missão e projeto; identificar requisitos adicionais de segurança específicos do projeto;
2) Atualizar a identificação das funções críticas de segurança e definir os requisitos de tolerância a falhas;
3)Identificar situações de emergência, advertência e cuidado;
4) Atualizar a avaliação de risco de segurança do sistema como parte da contribuição fornecida pelo domínio de segurança para o processo de gestão de risco;

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
5) Identificar os requisitos de segurança do projeto;
6) Garantir que a documentação e as atividades dos requisitos do projeto cumpram os requisitos de segurança do projeto;
7) Apoiar uma revisão dos requisitos do sistema e uma revisão preliminar do projeto;
8) Planejar a verificação da implementação dos requisitos de segurança;
9) Elaborar o plano de segurança para a definição detalhada, fase de produção e qualificação.
1.7.1.4 Teste Detalhado de Definição, Produção e Qualificação - Fases C / D
1.6.2.5.a) A análise de segurança deve apoiar o projeto detalhado, produção, qualificação e teste.
1.6.2.5.b) A análise de segurança deve também apoiar a otimização da segurança operacional, a avaliação da implementação de requisitos de segurança, a verificação da redução de riscos e a aceitação de riscos.
1.6.2.5.c) A análise das operações também deve apoiar a identificação de requisitos de treinamento e planejamento de resposta a emergências e contingências, além do desenvolvimento de procedimentos.
1.6.2.5.d) As seguintes tarefas do programa de segurança devem ser aplicadas aos programas de vôo espacial humano e sistemas críticos de segurança:
1) Realizar análise detalhada de risco no nível do sistema;
2) Realizar análises de segurança de apoio;
3) Atualizar os requisitos técnicos de segurança do projeto para incorporar os resultados das análises de segurança;
4) Assegurar que a implementação do projeto e o programa de verificação cubram as atividades de verificação de controle de perigos identificados;
5) Atualizar a identificação das funções críticas de segurança, os requisitos de tolerância a falhas e identificar os itens críticos de segurança;
6) Implementar programa de controle para itens críticos de segurança;
7) Realizar avaliação de risco de segurança em apoio à melhoria do projeto, distribuição de recursos do projeto, programa de controle para itens críticos de segurança e revisões do projeto;
8) Monitorar a verificação da implementação dos requisitos de segurança;
9) Verificar e documentar a implementação do controle de perigos;
10) Verifique se todos os itens de verificação abertos estão registrados e se os procedimentos acordados estão em vigor;
11) Apoiar a revisão crítica do projeto, a revisão da qualificação e a revisão da aceitação;
12) Realizar análises de segurança interna do projeto e auditorias internas;
13) Identificar, monitorar e controlar as operações de montagem, integração, teste e manuseio do projeto que são potencialmente perigosas para o pessoal ou hardware;
14) Revisar e aprovar procedimentos operacionais perigosos e críticos para a segurança;

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
15) Realizar relatórios e investigações de incidentes de acidentes;
16) Apoiar as análises de segurança do cliente em marcos definidos do programa;
17) Preparar um relatório de “lições aprendidas” de segurança do projeto;
18) Preparar o plano de segurança da fase operacional.
1.7.1.5 Utilização - Fase E
1.6.2.6.a) A análise de segurança deve avaliar o projeto e as mudanças operacionais quanto ao impacto na segurança, garantindo que as margens de segurança sejam mantidas e que as operações sejam conduzidas dentro do risco aceito.
1.6.2.6.b) A análise também deve apoiar a avaliação de anomalias operacionais quanto ao impacto na segurança e a avaliação contínua das tendências de risco.
1.6.2.6 c) As seguintes tarefas do programa de segurança devem ser aplicadas aos programas de vôo espacial humano e sistemas críticos de segurança:
1) Emitir o plano de segurança da fase operacional;
2) Rever os procedimentos operacionais;
3) Aprovar procedimentos operacionais críticos de segurança;
4) Identificar e monitorar operações perigosas;
5) Apoiar a revisão de prontidão de voo, análise de prontidão operacional, análise de prontidão de lançamento e análises de qualificação de voo;
6) Apoiar as operações terrestres e de vôo;
7) Realizar controle de itens críticos de segurança;
8) Monitorar e avaliar a evolução da configuração do sistema e operações resultantes de correções e atualizações de projeto;
9) Atualizar as análises de perigo e implementar controles de perigo adicionais, conforme necessário;
10) Investigar anomalias e tendências de voo relacionadas à segurança;
11) Atualizar a avaliação de risco de segurança conforme necessário para apoiar as decisões operacionais;
12) Prepare o plano de segurança da fase de descarte.
1.7.1.6 Descarte - Fase F
1.6.1.6 a) A análise de segurança deve avaliar todas as operações de descarte e perigos associados.
1.6.1.6 b) As soluções de descarte devem ser identificadas que atendam aos requisitos de segurança do projeto.
1.6.1.6 c) As seguintes tarefas do programa de segurança devem ser aplicadas aos programas de vôo espacial humano e sistemas críticos de segurança:
1) Realizar análises de risco com relação às operações de descarte;
2) Verificar se a operação de descarte está em conformidade com os regulamentos internacionais de segurança, realizando a análise de segurança necessária;
3) Revisar os procedimentos das operações de descarte;
4) Apoiar a revisão final da missão.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
1.7.2 Reuniões de progresso
1.7.2 a) O fornecedor deve realizar reuniões regulares de status de segurança e progresso com o cliente e seus fornecedores de nível inferior como parte das reuniões de progresso do projeto, conforme especificado em ECSS-M-ST-10.
1.7.2 b) Os especialistas relevantes de clientes e fornecedores devem participar das reuniões.
1.7.3 Avaliações de segurança
1.7.3 a) O cliente deve definir, conduzir e presidir as análises de segurança para garantir a implementação satisfatória do programa de segurança e dos requisitos técnicos de segurança.
1.7.3 b) O fornecedor deve apoiar as análises de segurança do cliente e da autoridade de aprovação de segurança relevante, conforme especificado nos planos de análise relevantes.
1.7.3 c) Cada fornecedor participante de uma análise de segurança deve preparar e enviar para análise o pacote de dados de segurança.
1.7.3 d) As revisões de segurança devem ser realizadas e os objetivos da revisão alcançados, em conformidade com o ítem 1.7.1
1.7.4 Demonstração de conformidade de segurança
1.7.4 a) O fornecedor deve fornecer uma declaração de conformidade de segurança para demonstrar que os elementos do sistema espacial estão em conformidade com os requisitos de segurança declarados.
1.7.4 b) O fornecedor deve incluir em sua declaração de conformidade uma declaração de que as verificações abertas são acompanhadas no registro da verificação de segurança.
1.7.4 c) O projeto deve fornecer à autoridade homologadora de segurança todas as informações relacionadas com a segurança para a aceitação da declaração de conformidade de segurança.
1.7.5 Treinamento de segurança
1.7.5.1 Geral
1.7.5.1 a) O treinamento de segurança deve fazer parte do treinamento geral de acordo com ECSS-Q-ST-20.
1.7.5.1 b) Todo o treinamento de segurança de qualquer pessoa que trabalhe de forma permanente ou ocasional com elementos do sistema que podem ter propriedades perigosas deve ter três aspectos principais:
1) Briefings gerais de conscientização sobre medidas de segurança a serem tomadas em um determinado local ou ambiente de trabalho;
2) Treinamento técnico básico nas técnicas e habilidades de segurança exigidas, que é um pré-requisito para cumprir a função em questão;
3) Treinamento específico do produto que enfoca os perigos relacionados ao elemento específico do sistema.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
1.7.5.2 Treinamento específico do produto
1.7.5.2 a) O fornecedor deve identificar a necessidade de treinamento de segurança específico do produto e implementar o programa de treinamento de segurança correspondente para todas as partes relevantes.
1.7.5.2 b) O fornecedor deve informar o cliente sobre qualquer treinamento de segurança por ele identificado como necessário para a tripulação de operações de vôo ou pessoal de controle da missão, juntamente com uma definição do tipo de treinamento necessário e seu escopo.
1.7.5.2 c) O fornecedor deve apoiar a implementação do programa de treinamento do cliente para a tripulação de operações de voo ou pessoal de controle da missão
1.7.5.3 Briefings de conscientização geral
1.7.5.3 a) Todo o pessoal que acessa a área onde o produto é processado deve participar previamente do briefing geral de segurança.
1.7.5.4 Treinamento técnico básico
1.7.5.4 a) O fornecedor deve fornecer treinamento técnico básico para todo o pessoal de engenharia e segurança do projeto que trabalha com produtos perigosos.
1.7.5.5 Registros de treinamento
1.7.5.5 a) O fornecedor deve manter registros do pessoal que recebeu treinamento de segurança de acordo com ECSS-Q-ST-20.
1.7.5 Relatório e investigação de incidentes de acidentes
1.7.5 a) O fornecedor deve relatar ao cliente todos os acidentes e incidentes ocorridos durante as atividades do projeto sob o controle do fornecedor ou de seus fornecedores de nível inferior que afetem o elemento do sistema.
1.7.5 b) O fornecedor deve apoiar, mediante solicitação, investigações de acidentes e incidentes relacionados ao projeto que ocorram fora do controle ou das instalações do fornecedor.
1.7.5 c) O fornecedor deve coordenar as atividades de investigação em cooperação com outros departamentos funcionais do fornecedor e fornecedores de nível inferior.
1.7.5 d) O relatório de investigação de acidente ou incidente deverá ser formalmente encerrado pelo fornecedor, mediante aprovação do cliente.
1.7.5 e) Se a conclusão da avaliação for que o incidente de acidente teve um efeito sobre o projeto, ou seja, a segurança do produto ou sua operação, o representante de segurança da organização deve ser informado.
1.7.5 f) No caso a ocorrência de incidentes e acidentes, o relatório de acidente-incidente deve se tornar parte dos dados do projeto e documentado no pacote de dados de segurança.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
1.7.6 Documentação de segurança
1.7.6.1 Geral
1.7.6.1 a) O fornecedor deve manter, como parte da documentação do projeto, todos os dados relacionados à segurança para apoiar as análises e a demonstração de conformidade de segurança.
1.7.6.1 b) O cliente deve ter acesso a esses dados mediante solicitação durante as auditorias, análises de segurança e reuniões realizadas nas instalações do fornecedor de acordo com a ECSS-M-ST-40.
1.7.6.2 Pacote de dados de segurança
1.7.6.2 a) O fornecedor deve enviar um pacote de dados de segurança para apoiar as análises.
1.7.6.2 b) O pacote de dados de segurança deve conter pelo menos a seguinte documentação relacionada à segurança:
1) Relatório de análise de segurança
2) Análise de suporte (se aplicável);
3) Avaliação de risco de segurança (se aplicável);
4) Lista e procedimentos de operações terrestres perigosas;
5) Registro de rastreamento de verificação de segurança
1.7.6.2 c) O conteúdo dos pacotes de dados de segurança para as análises de segurança planejadas de um projeto ou programa deve ser especificado pela Autoridade de Aprovação de Segurança para garantir que eles apoiam os objetivos das análises de segurança para as quais são entregues
1.7.6.2 d) O fornecedor deve usar a *baseline* de configuração real, conforme definido pelo ECSS-M-ST-40, como a *baseline* de projeto e operação que é o assunto do pacote de dados de segurança.
1.7.6.2 e) O fornecedor deve integrar os dados de segurança relacionados aos vários subsistemas ou equipamentos que compõem o sistema no pacote de dados de segurança que é apresentado na revisão.
1.7.6.2 f) Todos os dados de segurança devem ser rastreáveis a partir do pacote de dados de segurança e estar disponíveis para revisão.
1.7.6.3 Desvios e *waivers* de segurança
1.7.6.3.1 Pedido de desvio ou *waiver*
1.7.6.3.1 a) Os requisitos de segurança que não podem ser atendidos devem ser identificados conforme especificado em ECSS-M-ST-40.
1.7.6.3.1 b) Uma solicitação de desvio ou isenção deve ser gerada e rastreada de acordo com os requisitos do ECSS-M-ST-40.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
1.7.6.3.2 Avaliação de desvio ou *waiver*
1.7.6.3.2 a) Todos os RFD / RFW devem ser avaliados a fim de identificar aqueles que impactam a segurança.
1.7.6.3.2 b) Os desvios e renúncias acumulados que afetam a segurança devem ser avaliados para garantir que os efeitos dos desvios individuais não invalidem a lógica usada para a aceitação de outros desvios.
1.7.6.3.3 Aceitação pela autoridade de segurança
1.7.6.3.3 a) Desvios e *waivers* de segurança devem estar sujeitos à aceitação da autoridade de segurança
1.7.6.3.4 Revisão e disposição
1.7.6.3.4 a) Desvios e *waivers* que afetam os requisitos de segurança do projeto ou funções críticas de segurança que o fornecedor considera aceitáveis devem estar sujeitos a revisão e disposição pelo cliente e pela autoridade de segurança.
1.7.6.4 Lições aprendidas de segurança
1.7.6.4 a) As lições aprendidas de segurança devem ser coletadas e utilizadas durante o projeto, na medida em que forem relevantes, considerando:
1) O impacto dos requisitos recentemente impostos;
2) Avaliação de todas as avarias, acidentes, anomalias, desvios e isenções;
3) Eficácia das estratégias de segurança do projeto;
4) Novas ferramentas e métodos de segurança que foram desenvolvidos ou demonstrados;
5) Verificações eficazes versus ineficazes que foram realizadas;
6) Alterações propostas à política de segurança, estratégia ou requisitos técnicos com justificativa.
1.7.6.4 b) As informações sobre as lições de segurança aprendidas devem ser disponibilizadas ao cliente e fornecedores, principalmente aos gerentes de projeto e de segurança, bem como aos engenheiros de projeto e segurança, mediante solicitação para uso em outros projetos.
1.7.6.5 Documentação de itens críticos de segurança
1.7.6.5 a) Os itens críticos de segurança identificados pela análise de segurança devem ser documentados de acordo com ECSS-Q-ST-10-04.
2 Engenharia de Segurança
2.1 Identificação e rastreabilidade de requisitos de segurança
2.1 a) Os requisitos de segurança devem ser identificados e rastreados desde o nível do sistema até o projeto e, em seguida, atribuídos aos níveis inferiores.
2.1 b) Quando especificados pelo projeto, os requisitos de segurança que foram identificados devem ser justificados no projeto e apresentados em documento apropriado.
2.2 Objetivos do projeto de segurança
2.2.1Seleção de projeto.
2.2.1 a) Os recursos de projeto apropriados devem ser selecionados para garantir a segurança.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
2.2.2 Precedência de redução de risco
2.2.2.1 Geral
1.3 a) A seguinte sequência de atividades deve ser aplicada aos perigos identificados, condições perigosas e funções cujas falhas têm consequências perigosas:
1) Eliminação de perigo
2) Minimização de perigos
3) Controle de perigos.
2.2.2.2 Eliminação de perigo
2.2.2.2 a) Perigos e condições perigosas devem, de acordo com as restrições do projeto e objetivos da missão, ser eliminados do projeto e dos conceitos operacionais pela seleção da tecnologia de projeto, arquitetura e características operacionais.
2.2.2.3 Minimização de perigos
2.2.2.3 a) Onde os perigos e as condições perigosas não são eliminados, a gravidade dos eventos e consequências perigosas associados deve, de acordo com as restrições do projeto e objetivos da missão, ser reduzida a um nível aceito por meio da mudança da arquitetura de design, tecnologias e características operacionais, permitindo que substituição desses perigos por outros perigos com menor ameaça potencial.
2.2.2.4 Controle de perigo
2.2.2.4.1 Geral
2.2.2.4.1 a) Riscos que não foram eliminados e foram submetidos à minimização de risco (conforme definido em 6.3.3.3a) devem ser controlados por meio de medidas preventivas ou de mitigação, associadas a cenários de risco, que são introduzidos no projeto e operação do sistema para evitar os eventos ou para interromper sua propagação às consequências.
2.2.2.4.1 b) As seguintes medidas devem ser aplicadas em ordem de precedência:
1) Seleção de projeto
2) Dispositivos de segurança automáticos
3) Dispositivos de aviso
4) Procedimentos especiais.
2.2.2.4.2 Seleção de projeto - Projeto de tolerância a falhas
2.2.2.4.2 a) A tolerância a falhas é o requisito básico de segurança que deve ser usado para controlar a maioria dos perigos.
2.2.2.4.2 b) O projeto deve tolerar um número mínimo de falhas credíveis e / ou erros do operador determinados pela consequência do perigo.
2.2.2.4.2 c) O fornecedor deve estabelecer a lista de falhas a serem consideradas "não confiáveis" para aprovação do cliente o mais cedo possível no desenvolvimento.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
2.2.2.4.3 Seleção de projeto - Projeto para risco mínimo
2.2.2.4.3 a) O perigo que não pode ser controlado pela conformidade com a tolerância a falhas deve ser reduzido a um nível aceito pela conformidade com as propriedades específicas relacionadas à segurança e características do projeto.
2.2.2.4.4 Dispositivos de segurança automáticos
2.2.2.4.4 a) Os riscos que não são eliminados por meio da seleção do projeto devem ser reduzidos e controlados por meio do uso de dispositivos automáticos de segurança como parte do sistema, subsistema ou equipamento.
2.2.2.4.4.b) Os dispositivos de segurança, especificados no padrão, não devem ser dependentes do desempenho humano.
2.2.2.4.5 Dispositivos de alerta
2.2.2.4.5 a) Quando não for prático impedir a existência ou ocorrência de perigos conhecidos ou usar dispositivos automáticos de segurança, devem ser usados dispositivos para a detecção oportuna da condição e a geração de um sinal de alerta.
2.2.2.4.5 b) Isso deve ser acoplado a controles de emergência de ação corretiva para os operadores protegerem ou desligar o subsistema afetado.
2.2.2.4.6 Procedimentos especiais
2.2.2.4.6 a) Quando não for possível reduzir a magnitude de um perigo por meio do projeto, do uso de dispositivos de segurança ou de dispositivos de advertência, procedimentos especiais devem ser desenvolvidos para controlar as condições perigosas para o aumento da segurança.
2.2.2.4.6 b) Os procedimentos especiais devem ser verificados por meio de teste e o treinamento apropriado deve ser fornecido para o pessoal.
2.2.2.4.6 c) A detecção de perigo deve ser implementada se meios alternativos não puderem ser usados.
2.2.2.4.6 d) Para permitir o uso de monitoramento em tempo real, detecção de perigos e sistemas de proteção para controle de perigos, a disponibilidade de tempo de resposta suficiente deve ser verificada e os procedimentos de proteção correspondentes devem ser desenvolvidos e verificados e o pessoal treinado.
2.2.3 Compatibilidade ambiental
2.2.3 a) O projeto do sistema deve atender aos requisitos de segurança nos piores cenários naturais e ambientes induzidos definidos para o projeto.
2.2.3 b) Margens de projeto e desempenho devem ser estabelecidas e aplicadas para combinações de pior caso de ambientes induzidos e naturais e características operacionais.
2.2.4 Serviços externos
2.2.4 a) Perda, mau funcionamento e restauração repentina de serviços externos devem ser definidos como uma entrada para a fase de desenvolvimento.
2.2.4 b) O projeto do sistema deve ser definido de modo que consequências catastróficas ou críticas não sejam induzidas por perda, mau funcionamento e restauração repentina de serviços externos.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
2.2.5 Detecção de perigo - sinalização e proteção
2.2.5 a) Monitoramento de segurança, exibição, alarme e recursos de proteção devem ser incorporados para sistemas espaciais tripulados.
2.2.5 b) Essas capacidades devem fornecer as informações para permitir que a tripulação e os operadores do sistema tomem ações para proteger o pessoal das consequências de falhas nas funções críticas de segurança e da falha nas medidas de controle de perigo.
2.2.5 c) O projeto do sistema deve fornecer a capacidade de detectar falhas que resultem na degradação da tolerância a falhas com relação à detecção de perigo, sinalização e função de segurança.
2.2.5 d) O desempenho dessas funções deve ser verificável durante as fases operacionais de voo e solo.
2.2.5 e) Função de emergência, cuidado e advertência deve detectar e notificar a tripulação e os operadores do sistema sobre situações de emergência, advertência e advertência.
2.2.5 f) Funções e capacidades de proteção devem ser incluídas para fornecer a contenção ou controle de situações de emergência, advertência e cuidado.
2.2.5 g) Provisões devem ser incluídas para o monitoramento da execução da função de segurança.
2.2.5 h) Devem ser fornecidas funções de proteção dedicadas para situações de emergência.
2.2.5 i) O controle de situações de alerta e cuidado deve ser aceitável pela reconfiguração do sistema ou por funções de proteção dedicadas.
2.2.5 j) Uma única falha não deve causar a perda da função de emergência e advertência.
2.2.5 k) Quando a operação de um sistema de proteção introduz um novo perigo, a ativação inadvertida do sistema de proteção deve ser controlada de acordo com os requisitos de tolerância a falhas.
2.2.5 l) Uma única falha não deve causar a perda das funções de emergência e advertência junto com as funções monitoradas.
2.2.5 m) Dados de emergência, aviso e cuidado, anúncio fora do limite e comandos de segurança devem ter prioridade sobre outras funções de processamento de dados e comando.
2.2.5 n) Quando sistemas ou elementos são integrados ou acoplados a outros sistemas ou elementos, a função de emergência, aviso, cuidado e proteção deve permitir que as áreas de responsabilidade de controle monitorem e exibam os parâmetros aplicáveis e controlem as funções de proteção relacionadas.
2.2.5 o) As informações de status dos parâmetros de emergência, advertência e cuidado devem estar disponíveis e exibidas nos centros de controle de lançamento e de controle de missão em "tempo quase real" durante as fases operacionais.
2.2.5 p) Deve ser possível para a tripulação verificar e monitorar em "tempo real" o status de emergência, parâmetros de alerta e cautela de sistemas ou elementos sem tripulação antes de atracar com sistemas tripulados.

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
2.2.6 Mitigação de detritos espaciais
2.2.6 a) O projeto e as características operacionais do sistema espacial devem ser tais que a geração de detritos espaciais seja minimizada de acordo com as restrições do projeto e objetivos da missão, e em conformidade com a regulamentação aplicável de mitigação de detritos espaciais.
2.2.7 Reentrada atmosférica
2.2.7 a) O veículo espacial deve ser projetado e operado (manobras de eliminação pós-missão) de modo que, quando aplicável, o risco de um evento catastrófico não exceda o nível de risco aceitável especificado pela regulamentação aplicável.
2.2.8 Segurança das missões de retorno à Terra
2.2.8 a) A contaminação biológica (incluindo constituintes orgânicos) resultante da introdução de matéria extraterrestre deve ser evitada.
2.2.8 b) A introdução de matéria extraterrestre não deve afetar as condições ambientais na Terra.
2.2.8 c) Matérias extraterrestres devem ser tratadas como substâncias perigosas até prova em contrário.
2.2.8 d) Deve ser fornecida uma função de contenção para as substâncias perigosas da espaçonave, que evita a liberação em caso de acidentes até a recuperação ou chegada a uma instalação de contenção dedicada.
2.2.8 e) Se a contenção não puder ser verificada, as substâncias perigosas (e qualquer parte do sistema espacial que tenha sido potencialmente exposta) não devem ser devolvidas à Terra (a menos que esterilizadas no espaço).
2.2.9 Segurança de missões de vôo espacial humano
2.2.9 a) Uma capacidade de abortar missão deve ser fornecida.
2.2.9 b) As funções de proteção e céu seguro devem ser fornecidas.
2.2.9 c) As funções de escape e resgate devem ser fornecidas.
2.2.9 d) A capacidade de reconfigurar o sistema para restaurar a capacidade funcional das funções críticas de segurança em caso de falhas ou acidentes deve ser fornecida.
2.2.9 e) A capacidade de monitorar, detectar e avaliar os perigos e efeitos de eventos insidiosos lentos com consequências perigosas deve ser detalhada de acordo com as restrições do projeto e os objetivos da missão.
2.2.9 f) O sistema espacial deve fornecer instalações médicas a bordo e capacidade para lidar com tripulantes com deficiência permanente ou falecido.
2.2.10 Acesso
2.2.10 a) O sistema deve ser projetado de modo que qualquer acesso necessário aos elementos do sistema durante o vôo ou operações terrestres possa ser realizado com um nível de risco aceito para o pessoal.

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
2.3 Redução e controle de risco de segurança
2.3.1 Gravidade do evento perigoso e criticidade da função
A gravidade das consequências potenciais de eventos perigosos identificados deve ser categorizada conforme mostrado na Tabela 6-1.
O entendimento dos critérios definidos na Tabela 6-1 deve ser acordado entre o cliente e o fornecedor.
A avaliação dos efeitos ambientais prejudiciais, conforme identificado na Tabela 6-1, não deve ser limitada aos efeitos na Terra, mas também incluir efeitos, por exemplo, no espaço sideral, incluindo a Lua e os planetas, órbita geoestacionária (GEO), órbita baixa da Terra (LEO) bem como a atmosfera da Terra.
Para programas internacionais, um conjunto coerente de gravidade das consequências deve ser estabelecido para as fases operacionais conjuntas.
Essas categorias não devem violar a política e os princípios de segurança definidos na cláusula 4.2.1 para a proteção da vida humana ou os princípios de categorização de acordo com a definição das categorias de gravidade das consequências na Tabela 6-1.
A avaliação de especialistas sobre a determinação de limites para exposições que não criam perigo, aquelas que criam perigos críticos e aquelas que criam perigos catastróficos deve ser realizada pela autoridade responsável, no início do processo de projeto.
Os requisitos e medidas de segurança detalhados devem ser derivados dos níveis de exposição permitidos.
Uma lista abrangente de eventos perigosos deve ser compilada para o sistema espacial e missão.
A lista abrangente de eventos perigosos especificados em 6.4.1i deve ser completada e mantida ao longo do projeto, desenvolvimento e operação do sistema espacial.
A criticidade de uma função implementada no sistema espacial deve ser atribuída de acordo com a gravidade dos eventos perigosos identificados que ela pode causar, seguindo as categorias definidas na Tabela 6-2.
A maior gravidade identificada de eventos perigosos deve definir a criticidade da função.
A criticidade da função deve ser atribuída sem levar em consideração quaisquer disposições compensatórias.
2.3.2 Requisitos de tolerância a falhas
2.3.2.1 Requisitos Básicos
2.3.2.1 a) A tolerância a falhas deve ser o requisito básico de segurança usado para controlar os perigos.
2.3.2.1 b) Nenhuma falha de sistema único ou erro de operador único deve ter consequências críticas ou catastróficas.
2.3.2.1 c) Nenhuma combinação de duas falhas de sistema independentes ou erros do operador deve ter consequências catastróficas.
2.3.2.1 d) As inibições de segurança devem ser independentes, verificáveis, estáveis e permanecer em uma posição segura mesmo em caso de falha de energia.
2.3.2.1 e) Múltiplas falhas, que resultam de mecanismos de falha de causa comum ou modo comum, devem ser analisadas como falhas únicas para determinar a tolerância a falhas.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
2.3.2.2 Separação de redundância
2.3.2.2 a) O projeto do sistema deve:
1) incluir a capacidade de gerenciamento de redundância a bordo de funções críticas de segurança,
2) fornecer tolerância a falhas e informações de status de redundância para as tripulações de voo e de solo, incluindo notificação imediata da tripulação em caso de detecção de falha, troca de redundância ou perda de redundância operacional,
3) incluir detecção de falha, isolamento de falha e comutação de itens redundantes.
2.3.2.2 b) A capacidade deve ser fornecida à tripulação de voo e ao controle da missão para anular a proteção automática e a troca de redundância.
2.3.2.2 c) As funções críticas de segurança alternativas ou redundantes devem ser física e funcionalmente separadas ou protegidas de tal forma que qualquer evento que cause a perda de um caminho não resulte na perda de caminhos alternativos ou redundantes.
2.3.2.3 Propagação de falha
2.3.2.3 a) Falhas de hardware ou erros de software não devem causar falhas adicionais com efeitos perigosos ou se propagar para causar a operação perigosa do hardware de interface.
2.3.3 Projeto para risco mínimo
2.3.3.1 Geral
2.3.3.1 a) Os requisitos técnicos para áreas de projeto para risco mínimo devem ser identificados e aprovados pelas autoridades de aprovação de segurança relevantes
2.3.3.2 Fatores de segurança
2.3.3.2.a) Os fatores de segurança estruturais devem ser definidos e aplicados de acordo com ECSS-E-ST-32-10 ou fator de segurança superior quando aplicável.
2.3.3.2 b) As margens de segurança devem ser baseadas nas piores combinações confiáveis de condições ambientais.
2.3.3.3 Controle de fratura
Para sistemas tripulados, onde a falha estrutural pode ter consequências catastróficas ou críticas, as estruturas, vasos de pressão, fixadores e caminhos de suporte de carga dentro dos mecanismos devem ser projetados de acordo com ECSS-E-ST-32-01.
Para sistemas não tripulados, apenas vasos de pressão devem ser projetados de acordo com ECSS-E-ST-32-01, quando exigido pela autoridade de segurança do local de lançamento.
2.3.3.4 Materiais
2.3.3.4 a) Os materiais devem ser selecionados e controlados de acordo com ECSS-Q-ST-70.
2.3.3.4 b) A seleção do material deve assegurar que os perigos associados às características do material sejam eliminados ou controlados.
2.3.3.4 c) Se o requisito2.3.3.4b. não for viável, o projeto do sistema deve incluir as disposições necessárias para controlar eventos perigosos associados às características do material de acordo com os requisitos desta Norma.

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
2.3.4 Metas probabilísticas de segurança
2.3.4 a) Quando fornecidos, os alvos probabilísticos de segurança devem ser usados para:
1) Identificar e classificar os principais contribuintes de risco,
2) Tomar a decisão de risco aceitável para cada perigo identificado,
3) Apoiar a tomada de disposição para os casos em que a não conformidade com os requisitos qualitativos é identificada.
2.3.4 b) Os alvos de segurança probabilísticos devem estar em conformidade com os requisitos dados pelas autoridades de segurança de lançamento e regulamentos nacionais e internacionais
2.4 Identificação e controle de funções críticas de segurança
2.4.1 Identificação
2.4.1 a) Uma função que, se perdida ou degradada, ou por meio de operação incorreta ou inadvertida, pode resultar em uma consequência perigosa catastrófica ou crítica, deve ser identificada como uma função crítica para a segurança.
2.3.5.1 b) A identificação deve ser feita sem levar em consideração os controles de perigos a serem ou que já foram implementados.
2.4.2 Operação inadvertida
2.4.2 a) A operação inadvertida de uma função crítica de segurança deve ser evitada por
1) Duas inibições independentes, se induzirem consequências críticas, ou
2) Três inibições independentes, se induzir consequências catastróficas.
2.4.3 Informação de status
2.4.3 a) O sistema deve fornecer tolerância a falhas e informações de status de redundância de funções críticas de segurança.
2.4.3 b) O sistema deve fornecer o status de pelo menos duas inibições nas funções que, se operadas inadvertidamente, podem levar a consequências catastróficas, incluindo:
1) Notificação em tempo real em caso de detecção de falha,
2) Anúncio de qualquer perda de redundância operacional,
3) Notificação de troca de redundância, ou
4) Mudanças de status de inibição.
2.4.4 Requisitos de desligamento seguro e tolerância a falhas
2.4..4 a) O projeto deve fornecer a capacidade para o desligamento seguro das funções críticas para a segurança antes das operações de manutenção em vôo ou estar em conformidade com os requisitos de tolerância a falhas durante as operações de manutenção.
2.4.5 Componentes eletrônicos, elétricos, eletromecânicos
2.4.5.a) Componentes eletrônicos, elétricos, eletromecânicos (EEE) usados para suportar funções críticas de segurança em hardware padrão de vôo devem ser selecionados e adquiridos de acordo com os requisitos de programa aplicáveis de ECSS-Q-ST-60.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
2.4.6 Funções de software
2.4.6.1 Criticidade do software
2.4.6 1 a) Os aspectos de segurança associados à função do software devem ser parte integrante dos esforços gerais de segurança do sistema e não devem ser avaliados isoladamente.
2.4.6 1 b) Um produto de software será considerado crítico para a segurança se implementar ou afetar uma ou mais funções das quais pelo menos uma tenha criticidade I ou II, conforme definido na cláusula 2.3.1.
2.4.6.2 Análise de software crítico de segurança
2.4.6.2 a) Durante o ciclo de vida do projeto, a análise de segurança deve ser realizada para:
1) Identificar o software crítico para a segurança e quaisquer recursos comuns compartilhados entre o software crítico para a segurança e o software não crítico para a segurança,
2) Determinar onde e em quais condições o sistema pode desencadear eventos perigosos causados pelo software,
3) Definir métodos de verificação para controles de perigo envolvendo software,
4) Fornecer evidências de verificação da implementação do controle de risco.
2.4.6.3 Atribuição da categoria de criticidade de software
2.4.6.3 a) A criticidade de um produto de software (A, B, C) deve ser atribuída, com base na criticidade atribuída à função mais crítica que implementa e atendendo aos critérios definidos na Tabela 6-3 presente no apêndice da norma em questão e requisitos 2.4.6.3b a 2.4.6.3 g.
2.4.6.3 b) A criticidade dos produtos de software deve ser atribuída considerando o projeto geral do sistema e, em particular, se o hardware, software ou meios operacionais existem, pois existem disposições compensatórias que podem prevenir falhas de sistema causadas por software ou mitigar suas consequências.
2.4.6.3 c) A eficácia das provisões de compensação com o objetivo de reduzir a categoria de criticidade do software a uma categoria inferior do que na ausência de provisões de compensação deve ser demonstrada em todas as condições, excluindo falhas das próprias cláusulas de compensação.
2.4.6.3 d) Em todas as situações, haverá tempo suficiente para que as disposições compensatórias intervenham de forma a prevenir ou mitigar a falha em questão.
2.4.6.3 e) Caso as cláusulas de compensação contenham software, este software deve ser classificado na categoria de criticidade correspondente à maior gravidade das consequências de falha que eles previnem ou mitigam.
2.4.6.3 f) A avaliação probabilística de falhas de software não deve ser usada como um critério para atribuição de categoria de criticidade de software.
2.4.6.3 g) Quaisquer recursos comuns compartilhados por produtos de software de criticidade diferente devem ser identificados e a alocação de criticidade de software confirmada / alterada de acordo.

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
2.4.6.4 Desenvolvimento de software
2.4.6.4 a) Um produto de software de segurança crítica deve ser projetado, implementado, verificado e operado de acordo com os requisitos de engenharia e garantia de produto definidos em ECSS-E-ST-40 e ECSS-Q-ST-80.
2.4.6.4 b) O software crítico de segurança deve ser analisado para a identificação e verificação de controles e inibições de software adequados e validado em conformidade.
2.4.6.4 c) O nível de esforço de garantia do produto de software exigido deve ser determinado de acordo com a criticidade do produto de software.
2.5 Segurança Operacional
2.5.1 Requisitos básicos
2.5.1 a) O envolvimento da segurança na fase operacional deve ser planejado.
2.5.1 b) Responsabilidades, regras e procedimentos de contingência devem ser estabelecidos antes da operação para condições “limite” perigosas que podem ocorrer durante as operações em solo e em vôo.
2.5.1 c) Faixas de operação e limites de desempenho para operação segura devem ser estabelecidos e especificados.
2.5.1 d) O projeto não deve exigir controle ativo contínuo pelo pessoal, a fim de permanecer dentro das faixas operacionais e limites de desempenho estabelecidos.
2.5.1 e) As interfaces homem-máquina devem ser projetadas e as tarefas do pessoal devem ter como escopo reduzir o potencial de eventos perigosos resultantes de erro humano a um nível aceitável.
2.5.1 f) Limites de exposição da tripulação a ambientes naturais e induzidos pelo sistema devem ser estabelecidos e mantidos por características de projeto ou restrições operacionais que cobrem modos operacionais nominais, de contingência e de emergência, a fim de evitar ferimentos na tripulação ou incapacidade de realizar funções críticas de segurança.
2.5.2 Operações de voo e controle de missão
2.5.2.1 Operações do lançador
2.5.2.1 a) Perigos para os humanos, propriedade pública e privada e meio ambiente, resultantes da operação ou mau funcionamento do sistema do lançador, devem ser impedidos pelo cumprimento dos regulamentos da autoridade de segurança do lançamento.
2.5.2.2 Contaminação
2.5.2.2 a) As operações normais ou de aborto não devem resultar na contaminação do meio ambiente da Terra que coloque em risco a saúde humana, as culturas ou os recursos naturais ou que excedam os limites estabelecidos pelos regulamentos nacionais ou internacionais.
2.5.2.3 Regras de voo
2.5.2.3 a) As regras de voo devem ser preparadas para cada missão que delineiam as decisões pré-planejadas em caso de situações fora do nominal e consistentes com os requisitos de segurança.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
2.5.2.4 Controle de comando perigoso
2.5.2.4 a) O controle de comando perigoso deve garantir que todos os comandos perigosos sejam identificados.
2.5.2.4 b) O controle de comando perigoso deve garantir que os modos de falha, associados ao vôo e à operação em solo - incluindo hardware, software e procedimentos - usados no comando a partir de centros de controle ou outro equipamento de solo, sejam incluídos na avaliação de segurança.
2.5.2.4 c) O controle de comando perigoso deve garantir que o projeto do sistema forneça proteção para evitar a aceitação errônea de comandos que podem resultar em consequências catastróficas ou críticas.
2.5.2.4 d) O controle de comando perigoso deve garantir que os comandos, que podem resultar em consequências catastróficas ou perigosas críticas, não sejam executados até que sejam autorizados e verificados.
2.5.2.5 Controle de mudança de operação da missão
2.5.2.5 a) O controle de mudanças na operação da missão deve garantir que todas as mudanças desejadas ou necessárias durante a missão sejam analisadas quanto ao impacto na segurança.
2.5.2.5 b) O controle de mudança de operação da missão deve garantir que a autoridade de aprovação de segurança responsável aprove todas as solicitações de mudança operacional com impacto na segurança.
2.5.2.5 Vigilância de segurança e controle de anomalias
2.5.2.5 a) Os parâmetros de status de segurança devem ser identificados.
2.5.2.5 b) Os parâmetros de status de segurança devem ser monitorados.
2.5.2.5 c) O desvio dos limites especificados deve ser gerenciado.
2.5.2.6 Detritos perigosos, precipitação e controle de impacto
2.5.2.6 a) No caso de desvio da trajetória de lançamento planejada durante a subida, os estágios do veículo lançador devem ser destruídos remotamente ou ter seus motores de propulsão desligados para evitar que os estágios ou detritos caiam fora das áreas de segurança pré-definidas.
2.5.2.6 b) As trajetórias do veículo lançador e do estágio gasto devem ser monitorados para determinar os pontos de impacto do veículo, estágio ou detritos.
2.5.2.6 c) Os propelentes residuais contidos nos estágios suborbitais gastos ou abortados devem ser dispersos com segurança.
2.5.3 Operações terrestres
2.5.3.1 Aplicabilidade
2.5.3.1 a) Os requisitos de segurança da cláusula devem ser aplicados durante as seguintes operações terrestres:
1) Teste de desenvolvimento, qualificação ou aceitação;
2) Operações de montagem, integração ou teste;
3) Lançar operações de site;
4) Operações de manutenção ou recuperação; e
5) Operações de transporte ou manuseio,

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
2.5.3.2 Iniciação
2.5.3.2 a) O fornecedor deve estabelecer procedimentos para realizar análises e inspeções de prontidão de segurança antes da execução de qualquer operação aplicável.
2.5.3.3 Revisão e inspeção
2.5.3.3 a) Para verificar a conformidade com os requisitos de segurança, análises de prontidão e inspeções devem incluir análise e avaliação de segurança de instalações, equipamentos (incl. GSE), artigos de teste, procedimentos operacionais, de teste e contingência, controles de acesso e capacidades de pessoal para cumprir os requisitos de segurança.
2.5.3.4 Operações perigosas
2.5.3.4 a) As operações perigosas devem ser monitoradas quanto à conformidade com os requisitos e procedimentos de segurança e para o possível desenvolvimento de situações perigosas imprevistas.
2.5.3.4 b) Quando necessário, planos ou procedimentos de contingência e emergência devem ser estabelecidos e verificados antes do início da operação.
2.5.3.4 c) O gerente de segurança ou autoridade relevante de segurança deve ter autoridade para interromper qualquer operação que não esteja em conformidade com os requisitos de segurança.
2.5.3.5 Lançamento e local de pouso
2.5.3.5 a) As operações de lançamento, pouso, reversão e missão devem estar sujeitas à análise de risco.
2.5.3.5 b) Para operações terrestres, a análise deve abordar:
1) Potenciais consequências perigosas de erro humano e deficiências processuais;
2) Adequação e manutenção das margens operacionais;
3) Potencial de exposição humana a perigos e efeitos perigosos;
4 Requisitos para treinamento de operadores e tripulantes de voo;
5) Adequação das informações e dados fornecidos pelo hardware de voo, equipamento de suporte de solo (GSE) ou equipamento de teste, conforme apropriado, para apoiar o desempenho das operações de acordo com todos os requisitos de segurança aplicáveis (incluindo todos os regulamentos de segurança).
2.5.3.6 Equipamento de suporte de solo
2.5.3.6 a) Todos os equipamentos de suporte de solo (GSE) devem ser submetidos à análise de risco.
2.5.3.6 b) Todo GSE deve estar em conformidade com os "Requisitos Essenciais de Saúde e Segurança" de todas as "diretrizes da Nova Abordagem" da UE aplicáveis.
2.5.3.6 c) Conformidade com 2.5.3.6b. deve ser mostrado pela adição da marca ‘CE’ ao produto e pela emissão de uma ‘Declaração de Conformidade’.
2.5.3.6 d) A conformidade com quaisquer outras diretivas relacionadas ao produto deve ser demonstrada.

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
3 Requisitos e técnicas de análise de segurança
3.1 Geral
3.1 a) A análise de segurança deve ser realizada de forma sistemática como base para todas as fases aplicáveis e para garantir que os perigos sejam identificados, eliminados ou minimizados e controlados e os riscos de segurança sejam avaliados e reduzidos.
3.1 b) As análises de segurança devem ser iniciadas no início do processo de design e fornecer suporte simultâneo à engenharia do projeto na seleção das opções operacionais e de design menos perigosas que sejam compatíveis com a missão do projeto e as restrições do programa e estejam em conformidade com os requisitos.
3.1 c) Os resultados das análises de segurança também devem ser usados para apoiar a gestão do projeto na avaliação dos riscos gerais, verificação da redução do risco, classificação das fontes de risco, apoio à alocação de recursos do projeto, monitoramento das tendências de risco e aceitação do risco residual.
3.1 d) A análise deve sempre ser feita com referência a uma *baseline* de configuração definida conforme definido pelo ECSS-M-ST-40.
3.2 Avaliação e alocação de requisitos
3.2.1 Requisitos de segurança
3.2.1 a) O fornecedor deve responder e cumprir os requisitos de segurança aplicáveis ao projeto.
3.2.2 Requisitos de segurança adicionais
3.2.2 a) O fornecedor deve identificar requisitos de segurança adicionais, quando aplicável, por meio do uso de lições aprendidas de projetos anteriores e das análises de segurança realizadas durante o projeto.
3.2.3 Definir requisitos de segurança - funções
3.2.3 a) O fornecedor deve definir os requisitos de segurança para as várias funções do sistema.
3.2.4 Definir requisitos de segurança - subsistemas
3.2.4 a) O fornecedor deve definir os requisitos de segurança associados aos vários subsistemas e níveis inferiores.
3.2.5 Justificativa
3.2.5 a) O fornecedor deve justificar ao cliente a proposta de alocação dos requisitos de segurança, o mais tardar no final da fase de definição detalhada.
3.2.6 Especificação funcional e de subsistema
3.2.6 a) O fornecedor deve garantir que os requisitos de segurança da função e do subsistema estejam incluídos nas especificações funcionais e do subsistema relevantes.
3.3 Análises de segurança durante o ciclo de vida do projeto
3.3 a) A análise de segurança deve ser refinada e atualizada de forma iterativa conforme o processo de projeto prossegue, para garantir que os perigos e eventos perigosos sejam avaliados e que o projeto detalhado e os requisitos operacionais relevantes, os controles de risco e as atividades de verificação sejam definidos e implementados

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
3.4 Análises de segurança
3.4.1 Geral
3.4.1 a) O relatório da análise de segurança deve ser estabelecido em conformidade com o DRD do Anexo D da referida norma, a fim de reunir os resultados das análises de segurança, as quais utilizam métodos determinísticos e probabilísticos descritos nas cláusulas 3.4.2 a 3.4.4.
3.4.2 Análise de Perigo
3.4.2 a) A análise de perigos deve ser realizada de forma sistemática, começando na fase de conceito e continuando através da fase operacional, incluindo fim da vida útil e descarte.
3.2.4 b) A análise de risco deve apoiar o processo de redução de risco.
3.2.4 c) A análise de perigo deve identificar e avaliar:
1) Perigos associados ao projeto do sistema, sua operação (tanto em solo quanto em vôo) e o ambiente de operação;
2) Os efeitos perigosos resultantes da propagação física e funcional dos eventos iniciadores;
3) Os eventos perigosos resultantes da falha de funções do sistema e componentes funcionais;
4) Situações críticas de tempo.
3.2.4 d) Os seguintes eventos iniciadores potenciais devem ser considerados:
1) Falha de hardware (aleatória ou dependente do tempo);
2) Erro latente de software;
3) Erro do operador;
4) Inadequações de design, incluindo:
4 a) Margens inadequadas;
4 b) Modos de operação não intencionais causados por circuitos furtivos;
4 c) Inadequações e incompatibilidades materiais;
4 d) Interações hardware-software;
5) Efeitos ambientais naturais e induzidos;
6) Deficiências processuais.
3.2.4 e) A análise de perigo inclui uma análise sistemática das operações do “sistema” e procedimentos operacionais que devem ser executados no design detalhado e nas fases operacionais de um projeto.
3.2.4 f) A análise sistemática da operação do sistema e dos procedimentos operacionais deve ser repetida conforme o projeto e os detalhes operacionais evoluem, incluindo os modos operacionais do sistema e as interfaces homem-máquina.

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
3.4.3 Avaliação de risco de segurança
3.4.3 a) A avaliação de risco de segurança deve:
1) Compreender a identificação, classificação e classificação dos riscos de segurança e seus contribuintes,
2) Basear-se na análise de risco determinística, combinando a gravidade da consequência e a probabilidade de ocorrência
3) Ser usado para facilitar a redução e controle de risco de segurança eficaz e eficiente,
4) Apoiar a gestão de risco do projeto conforme definido no ECSS-M-ST-80,
5) Avaliar o cumprimento das metas de segurança probabilísticas.
3.4.3 b) A avaliação de risco de segurança deve ser iniciada no início do processo de projeto e realizada em etapas progressivas durante a implementação do programa de segurança.
3.4.4 Avaliação e análise de apoio
3.4.4.1 Geral
3.4.4.1 a) Os seguintes métodos de avaliação e análise de apoio devem ser usados conforme necessário (adaptados por projeto) para apoiar a análise de perigos e a avaliação de riscos de segurança.
3.4.4.1 b) As análises de apoio devem ser acordadas com todas as partes relevantes.
3.4.4.2 Análise de tempo de aviso
3.4.4.2 a) A análise do tempo de advertência deve ser realizada durante a fase de definição do conceito e a fase de projeto e desenvolvimento, a fim de avaliar as situações de tempo crítico identificadas na análise de perigo e para apoiar a implementação de dispositivos de detecção e alerta de situações perigosas ou procedimentos de contingência.
3.4.4.2 b) A análise deve determinar o:
1) Intervalo de tempo durante o qual o evento é detectado e a ação de resposta executada;
2) Capacidade de detecção do projeto proposto no que diz respeito à sensibilidade de detecção e tempo de detecção;
3) Tempo resultante disponível para resposta;
4) Adequação do projeto proposto ou procedimentos de contingência, incluindo evacuação de emergência, resgate, reconfiguração do sistema, comutação de redundância e manutenção.
3.4.4.2 c) Os tempos de detecção devem ser determinados a partir do
1) Ocorrência do evento inicial até o momento em que ocorre uma consequência perigosa (tempo de propagação);
2) Ocorrência do evento inicial até o momento da primeira detecção ou anunciação; e
3) Tempo gasto para a ação corretiva ser implementada.

continua

Quadro A.2: Continuação

Requisitos Garantia da Segurança Segundo ECSS
3.4.4.3 Análise de cuidado e aviso
3.4.4.3 a) A análise de cuidado e alerta deve ser realizada durante a fase de definição de conceito e a fase de projeto e desenvolvimento de programas de voo espacial humano, a fim de identificar:
1) Parâmetros de emergência, aviso e cuidado;
2) As funções e capacidades de proteção necessárias;
3) Requisitos de detecção de limite
4) A aplicabilidade das funções individuais de “cuidado e alerta” às diferentes fases da missão.
3.4.4.3 b) A análise de cuidado e aviso deve utilizar os resultados do tempo de aviso e análises de riscos conforme apropriado.
3.4.4.4 Análise de causa comum e falha de modo comum
3.4.4.4.1 Múltiplas falhas
3.4.4.1 a) As falhas múltiplas, que resultam de mecanismos de falha de causa comum ou modo comum, devem ser analisadas como falhas únicas para determinar a tolerância a falhas.
3.4.4.4.2 Identificação de requisitos e escopo
3.4.4.2 a) O fornecedor deve identificar o requisito e o escopo de análises dedicadas de causa comum e modo comum por meio da revisão dos resultados das outras análises de segurança, tais como FTA e análise de risco, e das características do sistema e de seu ambiente.
3.4.4.4.3 Identificação de falhas de causa comum
3.4.4.4.3 a) O fornecedor deve identificar possíveis falhas de causa comum, avaliando os efeitos das causas comuns.
3.4.4.4.3 b) A análise de falha de causa comum deve ser realizada em coordenação com o FTA e a análise de risco.
3.4.4.4.4 Análise de falhas de modo comum
3.4.4.4.4 a) As falhas em modo comum devem ser analisadas por meio da utilização de check-lists (a serem estabelecidas pelo fornecedor) que listam potenciais modos comuns para componentes do sistema durante as fases de fabricação, integração, teste, operação e manutenção.
3.4.4.4.4 b) A análise de modo comum deve ser coordenada com o FMEA / FMECA.
3.4.4.4.5 Integração de resultados
3.4.4.4.5 a) Os resultados da análise de causa comum e de modo comum devem ser integrados aos resultados das análises de segurança no nível do sistema (análise da árvore de falhas, análise de risco).
3.4.4.5 Análise de árvore de falhas
3.4.4.5 a) A análise da árvore de falhas deve ser usada para estabelecer a ligação sistemática entre o perigo no nível do sistema e os eventos perigosos contribuintes e falha do subsistema, equipamento ou peça.
3.4.4.5 b)Uma análise da árvore de falhas, ou seu equivalente, deve ser realizada para verificar os requisitos de tolerância a falhas.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
3.4.4.6 Análise de erro humano
3.4.4.6 a) Sempre que as análises de segurança identificam erros do operador como causa de perigos catastróficos ou críticos, uma análise dedicada deve ser realizada.
3.4.4.6 b) A análise de erro humano deve ser usada para apoiar a análise de segurança para a identificação de tipos de erro humano do operador e seus efeitos e para a definição de contramedidas adequadas para prevenir ou controlar erros humanos do operador.
3.4.4.6 c) A análise de erro humano deve ser desenvolvida desde as fases iniciais do projeto para definir recomendações para o design de hardware e software, desenvolvimento de procedimentos e programa de preparação de treinamento.
3.4.4.7 Efeitos dos Modos de falha e análise de criticidade
3.4.4.7 a) Os resultados dos modos de falha e análise de efeitos (FMEA) ou modos de falha, efeitos e análise de criticidade (FMECA) devem ser usados para apoiar a análise de perigo na avaliação dos efeitos de falhas. FMEA / FMECA e análise de risco são análises complementares.
3.4.4.8 Análise zonal
3.4.4.8 a) A análise zonal deve ser realizada onde a redundância é usada para reduzir a probabilidade de perder uma função ou de ativar inadvertidamente uma função crítica de segurança.
3.4.4.8 b) Os objetivos da análise zonal devem garantir que a instalação do equipamento atenda aos requisitos de segurança adequados em relação a:
1) Regras básicas de instalação e práticas espaciais;
2) Interação entre subsistemas;
3) Implicação de erros do operador;
4) Efeitos de eventos externos.
4 Verificação de segurança
4.1 Geral
4.1 a) Deve haver um sistema que rastreie todos os perigos e riscos relacionados, para relacionar todas as verificações do perigo correspondente exclusivamente a causas e controles inequívocos.
4.1 b) Para técnicas comuns de verificação de características de projeto usadas para controlar riscos, os requisitos de ECSS-E-ST-10 devem ser aplicados.
4.1 c) Para concluir com sucesso o processo de segurança, feedback positivo deve ser fornecido nos resultados de conclusão para todos os itens de verificação associados a um determinado perigo.
4.2 Relatório e revisão de perigos
4.2.1 Sistema de relatório de perigo
4.2.1 a) O fornecedor deve estabelecer um sistema de relatório de perigo para rastrear o status de todos os perigos identificados.
4.2.1 b) O sistema deve ser aplicado para todos os perigos com consequências potencialmente catastróficas ou críticas.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
4.2.1 c) O fornecedor deve relatar e fornecer evidências que:
1) Os controles são definidos e acordados;
2) Métodos de verificação são definidos e acordados;
3) A verificação é concluída.
4.2.1 d) Se a verificação não puder ser concluída, o fornecedor deve estabelecer um Registro de Rastreamento de Verificação de Segurança
4.2.2 Revisão do status de segurança
4.2.2 a) O status das atividades de controle de perigo e redução de risco deve ser analisado em reuniões de progresso de segurança e análises de segurança do projeto para cumprimento das decisões tomadas e obtenção dos resultados pretendidos.
4.2.3 Documentação
4.2.3 a) Toda a documentação de perigo deve ser emitida formalmente para cada revisão de segurança e revisão de projeto principal, conforme especificado na cláusula 1.7.6
4.3 Métodos de verificação de segurança
4.3.1 Engenharia de verificação e planejamento
4.3.1 a) A engenharia de verificação deve selecionar os métodos de verificação que são consistentes:
1) Com os requisitos de verificação documentados no relatório de perigo,
2) Com as regras de segurança da base de lançamento.
4.3.1 b) O planejamento da verificação deve começar de maneira integrada após a seleção do método de controle.
4.3.2 Métodos e relatórios
4.3.2 a) Os métodos de verificação de segurança devem incluir, alternativamente ou em combinação, a revisão do projeto, análise, inspeção e teste.
4.3.2 b) Para todas as verificações de segurança, rastreabilidade deve ser fornecida.
4.3.3 Análise
4.3.3 a) Todas as análises técnicas de segurança e engenharia relevantes realizadas ou atualizadas com a análise em relação à configuração as-built devem ser usadas para verificação.
4.3.3 b) Quando a análise de similaridade é fornecida, para fins de rastreamento, ela deve conter uma cópia (ou uma referência única) da verificação anterior referenciada, procedimento de verificação e requisito válido no momento da primeira verificação.
4.3.4 Inspeções
4.3.4.1 Geral
4.3.4.1 a) As inspeções consideradas necessárias para atender aos requisitos de segurança do sistema devem ser identificadas e incluídas nos manuais e procedimentos do usuário.

continua

Quadro A.2: Continuação.

Requisitos Garantia da Segurança Segundo ECSS
4.3.4.2 Inspeções de Pré-voo
4.3.4.2 a) Todas as inspeções de segurança de pré-voo devem ser avaliadas para inclusão na lista MIP.
4.3.4.2 b) As inspeções de preparação de lançamento devem ser incluídas no procedimento da base de lançamento.
4.3.4.2 c) O encerramento será dado pelo procedimento de autoridade de lançamento aprovada.
4.3.4.2 d) Os procedimentos de acesso tardio devem ser objeto de treinamento e executados por pessoal qualificado.
4.3.4.2 e) O treinamento para a tripulação de voo e equipes de operação de missão deve ser realizado, incluindo instruções de segurança específicas, treinamento e simulação de missão.
4.3.4.2 f) O encerramento deve ser por procedimento aprovado de segurança, sessão de treinamento documentada e simulações.
4.3.4.3 Inspeções a bordo
4.3.4.3 a) As inspeções a bordo devem ser inseridas nos procedimentos de voo e manuais de operação.
4.3.5 Verificação e aprovação
4.3.5 a) O fornecedor deve selecionar e propor à autoridade de aprovação de segurança os métodos de verificação de segurança a serem usados em conformidade com os requisitos de segurança aplicáveis.
4.3.5 b) Os resultados da verificação de segurança devem ser apresentados para aprovação à autoridade homologadora de segurança relevante.
4.4 Verificação de funções críticas de segurança
4.4.1 Validação
4.4.1 a) As funções críticas de segurança devem ser verificadas por meio de testes que incluem a aplicação dos procedimentos operacionais, o “man-in-the-loop” e a verificação da eficácia dos requisitos de tolerância a falhas aplicáveis.
4.4.1 b) Os testes devem incluir a demonstração dos modos operacionais nominais, de contingência e de emergência.
4.4.2 Qualificação
4.4.2 a) As características críticas de segurança de todas as funções críticas de segurança devem ser qualificadas por teste.
4.4.2 b) O teste de qualificação de função crítica para a segurança deve incluir a determinação das margens de desempenho, considerando as combinações do pior caso de ambientes induzidos e naturais e condições operacionais.
4.4.2 c) A qualificação “por similaridade” não deve ser aplicada, exceto após a aprovação do cliente, caso a caso.
4.4.3 Testes de falha
4.4.3 a) Os testes de falha induzida devem ser realizados quando exigido pela análise de segurança para avaliar os efeitos da falha e para demonstrar a conformidade com a tolerância a falha em funções críticas de segurança.

continua

Quadro A.2: Conclusão.

Requisitos Garantia da Segurança Segundo ECSS
4.4.4 Verificação do projeto ou características operacionais
4.4.4 a) A verificação do projeto exclusivo de segurança exigida ou das características operacionais deve fazer parte dos programas de desenvolvimento, qualificação ou teste de aceitação, conforme apropriado.
4.4.5 Teste de verificação de segurança
4.4.5 a) Quando o teste em escala real não é realizado, o método de verificação de segurança equivalente baseado em hardware ou modelos tecnicamente representativos deve ser justificado, aprovado e executado.
4.4.5 b) Para a verificação de controles de perigo em perigos catastróficos, onde o equipamento não-vôo substitui parte do equipamento de vôo para testar uma função de vôo, a verificação deve ser realizada de forma independente por um terceiro que não estava envolvido no projeto e qualificação do modelo de vôo (FM)
4.5 Fechamento de perigo
4.5.1 Verificação de garantia de segurança
4.5.1 a) Um registro de rastreamento de verificação de segurança (SVTL) deve ser estabelecido, em conformidade com o DRD no Anexo C da referida norma, para coletar todos os itens de verificação em aberto dos diferentes relatórios de perigo da análise de segurança.
4.5.1 b) Em tempo de aceitação pelo cliente e na preparação da transferência para o próximo estágio de integração do sistema, o gerente de segurança deve verificar se:
1) Fechamentos de perigo realizados até o momento pelo engenheiro responsável ainda são válidos;
2) As verificações refletem o status de execução ou modificação do hardware;
3) Todas as verificações em aberto neste momento são aceitáveis para transferência para o próximo estágio de integração do sistema;
4) Todas as verificações abertas são inseridas no registro de rastreamento de verificação (SVTL);
5) O registro de rastreamento de verificação é mantido para refletir o status atual.
4.5.1 c) Se a verificação de segurança restringir quaisquer operações em solo, o gerente de segurança deve notificar o painel de revisão de segurança.
4.5.2 Verificação de fechamento de perigo
4.5.2 a) O gerente de segurança deve garantir que cada perigo considerado para fechamento tenha a aprovação da autoridade de aprovação de segurança, verificando que:
1) Os perigos não eliminados são controlados de acordo com os requisitos aplicáveis e as atividades de verificação associadas são concluídas com sucesso ou, quando aplicável,
2) Desvios ou dispensas de requisitos são concedidos pela autoridade de homologação de segurança.
4.6 Declaração de conformidade do equipamento de solo
4.6 a) Todos os equipamentos de aterramento que se enquadram no escopo de uma "diretiva de nova abordagem" aplicável devem ter a marca "CE" e ser fornecidos com uma "Declaração de conformidade" de apoio e um manual do usuário detalhando todos os avisos de segurança.

Fonte: Adaptado de ECSS (2017a).

APÊNDICE B

Quadro B.1: Requisitos de segurança referentes à organização de segurança.

Requisitos aplicáveis à organização	Grande	Médio	Pequeno	Nano
1 Programa de segurança de sistema				
1.1 Escopo				
1.1.1) O escopo e conteúdo do programa de segurança visam estabelecer um sistema de gestão de segurança para implementar os itens previstos nesta tabela de acordo com os requisitos do projeto espacial.				
1.1.1.a) O fornecedor deve estabelecer e manter um programa de segurança de sistema.	A	A	A	NA
1.1.1.b) O fornecedor deve garantir que todos os regulamentos e leis de segurança nacionais ou internacionais aplicáveis sejam identificados.	A	A	A	NA
1.1.1.c) Os requisitos do programa de segurança do sistema contidos nesta tabela devem ser aplicados.	A	A	A	NA
1.1.2) Adaptações não podem diminuir o grau de proteção do pessoal, de equipamento ou material de voo, de equipamento de apoio no solo, do público em geral, de propriedade pública e privada e do meio ambiente contra os riscos associados aos sistemas espaciais.	A	A	A	A
1.2 Plano do programa de segurança				
1.2.1 Definição				
O plano deve definir:				
1.2.1.a) as tarefas do programa de segurança a serem implementadas;	A	A	A	NA
1.2.1.b) o pessoal ou fornecedor responsável pela execução das tarefas;	A	A	A	NA
1.2.1.c) o cronograma de tarefas do programa de segurança relacionadas aos marcos do projeto;	A	A	A	A
1.2.1.d) interface da atividade do programa de segurança com a engenharia do projeto e com outras atividades de garantia do produto;	A	A	A	NA
1.2.1.e) como o fornecedor realiza as tarefas e verifica se foram concluídas satisfatoriamente (ex.: procedimentos internos).	A	A	A	NA
1.2.2 Conformidade				
1.2.2.a) O plano deve garantir que os requisitos e regulamentos de segurança aplicáveis a quaisquer outras instalações e serviços que sejam utilizados durante o curso do projeto sejam identificados.	A	A	A	A

continua

Quadro B.1: Conclusão.

Requisitos aplicáveis à organização	Grande	Médio	Pequeno	Nano
1.3 Organização de segurança				
1.3.1 Representante de Segurança				
1.3.1.a) Cada fornecedor deve nomear um representante de segurança, qualificado por treinamento ou experiência, para desempenhar as funções de segurança do sistema, de acordo com a legislação brasileira.	A	A	A	NA
1.3.2 Independência				
1.3.2.a) O representante de segurança deve ter acesso direto para reportar com o gerente de projeto e à alta gerência e ser independente da linha hierárquica dentro do projeto.	A	A	A	NA
1.4.3 Auditorias de Segurança				
1.4.3.a) O fornecedor deve realizar auditorias ou revisões de segurança para verificar a conformidade com a política e os requisitos de segurança do projeto.	A	A	A	NA
1.4.3.b) As auditorias de segurança devem estar de acordo com os procedimentos estabelecidos.	A	A	A	NA
1.4.3.c) O cliente deve ser informado do cronograma de auditoria.	A	A	A	NA
1.4.4 Aprovação de Relatórios				
1.4.4.a) O fornecedor deve permitir que os relatórios do projeto que tratam de questões relacionadas à certificação de segurança sejam emitidos com a assinatura apenas do representante de segurança.	A	A	A	NA
1.4.5 Representação em Conselhos				
1.4.5.a) A segurança deve estar representada em reuniões de controle de configuração (CCBs), reuniões de controle de não conformidade (NRBs), reuniões de prontidão de teste (TRBs) e em qualificações e revisões de aceitação, onde os requisitos de segurança e funções críticas de segurança estão envolvidos.	A	A	A	NA
1.6.2.5 Teste Detalhado de Definição, Produção e Qualificação - Fases C / D				
1.6.2.5.d) O centro de testes espaciais deve estabelecer um programa de segurança para garantir a segurança de todo o pessoal do centro de testes, incluindo o cliente e visitantes, o espécime em teste, as instalações e infraestrutura associada, de acordo com a norma ECSS-Q-ST-20-07C.	A	A	A	A

Fonte: Produção da autora.

Quadro B.2 - Requisitos de segurança referentes à projeto.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
1.5 Gestão de riscos de segurança				
1.5.1 Riscos de Segurança				
1.5.1 a) A base para a gestão de riscos deve ser o processo de quatro etapas e nove tarefas, como apresentado na ECSS-M-ST-80C	A	A	A	A
1.5.1 b) Os cenários de risco devem ser identificados de forma estruturada para todos os domínios usando como fontes de informação:	A	A	A	A
1) Análises anteriores, lições aprendidas e dados históricos;				
2) Entrevistas com especialistas e dados de experiência;				
3) Extrapolação de dados;				
4) Simulações, dados de teste e modelos;				
5) Análise detalhada de segurança e confiabilidade (consulte ECSS - Q - ST - 30 e ECSS - Q - ST - 40);				
6) Análise de todas as estruturas e níveis de decomposição do trabalho;				
7) Comparação de metas e planos;				
8) Análise de recursos;				
9) Análise de fornecedores;				
10) Análise das mudanças propostas;				
11) Resultado dos testes;				
12) Relatórios de não conformidade;				
13) consideração do cronograma;				
14) Criticidade da tecnologia e disponibilidade de soluções de backup.				
1.5.1 c) Os cenários de risco devem ser avaliados aplicando o método e esquema de pontuação definidos na política de gestão de risco.	A	A	A	A
1.5.1 d) Os cenários de risco devem ser analisados quanto à sua aceitabilidade.	A	A	A	A
1.5.1 e) Os riscos devem ser reduzidos de acordo com a política de gestão de riscos aplicando métodos que visem reduzir as probabilidades ou severidade dos cenários de risco, ou reduzir as incertezas aplicando medidas como:	A	A	A	A
1) Modificação de requisitos ou acordo comercial;				
2) Mudança de design, *baseline* ou estrutura do projeto;				
3) Introdução de tolerância a falhas de acordo com os documentos ECSS - Q - ST - ST;				
4) Aquisição de recursos adicionais ou redirecionamento de recursos;				
5) Aumento do teste ou análise.				

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
1.5 Gestão de riscos de segurança				
1.5.1 f) As opções para aceitação dos riscos resolvidos, aceitáveis e gerais devem ser definidas quando apropriado e apresentadas ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para eliminação.	A	A	A	A
1.5.1 g) Os riscos não resolvidos devem ser apresentados ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para posterior disposição.	A	A	A	A
1.5.1 h) Os riscos residuais ao final de um ciclo de gestão de risco devem ser submetidos ao nível de gerenciamento apropriado, conforme definido no plano de gestão de risco, para aceitação.	A	A	A	A
1.5.1 j) Os riscos devem ser monitorados, comunicados e os resultados devem ser exibidos em conformidade com o relatório de avaliação de risco apresentado no padrão.	A	A	A	A
1.5.1.k) Riscos à vida humana, ao hardware de voo, à missão e ao meio ambiente devem ser gerenciados durante todo o projeto, executando-se as seguintes atividades:	A	A	A	A
1) atribuição de requisitos de segurança;				
2) identificação de perigos;				
3) avaliação de perigos;				
4) prevenção, redução e controle de perigos; e				
5) encerramento do perigo, incluindo aceitação de risco residual.				
1.5.2 Avaliação dos perigos				
1.5.2.a) Todas as avaliações dos perigos devem considerar principalmente o potencial de risco e categorizar todos os perigos de acordo com a categoria de gravidade apropriada.	A	A	A	A
1.5.2.b) Controles correspondentes devem ser propostos.	A	A	A	A
1.5.2.c) O projeto inicial deve ser escolhido de tal forma que o potencial de risco e sua consequente gravidade sejam minimizados.	A	A	A	A
1.5.2.d) A probabilidade de um evento perigoso deve, consequentemente, ser levada em conta sempre que os métodos de redução da gravidade das consequências de perigo sejam considerados, isoladamente, como insuficientes para reduzir adequadamente o risco.	A	A	A	A

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
1.5 Gestão de riscos de segurança				
1.5.2.e) A probabilidade de ocorrência deve ser reduzida considerando-se todas as áreas de projeto para risco mínimo, aumentando-se a confiabilidade dos dispositivos de segurança, fornecendo-se dispositivos de aviso, ou usando-se controles de procedimento e treinamento.	A	A	A	A
1.6 Fases do projeto e ciclo de revisão de segurança				
1.6.1 Reuniões de Progresso				
1.6.1.a) O fornecedor deve realizar reuniões regulares de progresso de segurança para revisar o status das atividades do programa de segurança, conforme exigido pelos itens contidos nesta tabela.	A	A	A	D
1.6.1.b) As reuniões devem ser assistidas pelos especialistas relevantes do cliente e fornecedor.	A	A	A	D
1.6.2 Análises do Projeto				
1.6.2.1 Geral				
1.6.2.1.a) O fornecedor deve apresentar um status de segurança do projeto conforme exigido pelo cliente.	A	A	A	D
1.6.2.1.b) Um pacote de dados de segurança deve ser preparado para cada revisão de projeto.	A	A	A	D
1.6.2.1.c) O status de segurança do projeto deve ser apresentado durante as revisões do projeto (por exemplo: PDR, CDR, AR)	A	A	A	D
1.6.2.2 Análise da Missão / Identificação de Necessidades - Fase 0				
1.6.2.2.a) O fornecedor deve preparar uma análise de segurança para dar suporte à identificação de fontes de risco de segurança, bem como a realização de análises preliminares de *trade-off* entre os conceitos de sistemas alternativos.	A	A	A	A
1.6.2.2.b) Durante a Fase 0, o fornecedor deve demonstrar que:	A	A	A	A
1) Os requisitos de segurança e as lições aprendidas de projetos anteriores foram analisados e foi dado apoio ao projeto e para ao *trade-off* do conceito de operações;				
2) Os principais requisitos de segurança do sistema foram identificados.				

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos **1.6 Fases do projeto e ciclo de revisão de segurança**	Grande	Médio	Pequeno	Nano
1.6.2.3 Viabilidade - Fase A				
1.6.2.3.a) A análise de segurança deve apoiar análises de *trade-off* para se chegar ao conceito que tenha um risco de segurança aceitável, considerando-se as restrições do projeto e da missão.	A	A	A	D
1.6.2.3.b) A tecnologia de projeto selecionada e o conceito operacional a ser implementado devem ser selecionados com base nos dados de análise para a arquitetura de sistema mais segura, a fim de eliminar ou reduzir os riscos a níveis aceitáveis.	A	A	A	D
1.6.2.4 Definição Preliminar - Fase B				
1.6.2.4.a) A análise de segurança deve apoiar uma otimização contínua e mais detalhada da segurança do projeto e das operações do sistema, bem como a identificação dos requisitos técnicos de segurança e sua aplicabilidade.	A	A	A	D
1.6.2.4.b) A análise também deve fornecer dados para a avaliação de riscos de segurança em apoio à avaliação de riscos de segurança, identificação de contribuintes de risco no projeto e no conceito operacional.	A	A	A	D
1.6.2.5 Teste Detalhado de Definição, Produção e Qualificação - Fases C / D				
1.6.2.5.a) A análise de segurança deve apoiar o projeto detalhado, produção, qualificação e teste.	A	A	A	A
1.6.2.5.b) A análise de segurança deve também apoiar a otimização da segurança operacional, a avaliação da implementação de requisitos de segurança, a verificação da redução de riscos e a aceitação de riscos.	A	A	A	A
1.6.2.5.c) A análise das operações também deve apoiar a identificação de requisitos de planejamento e treinamento de resposta a emergências e contingências, bem como o desenvolvimento de procedimentos.	A	A	A	A
1.6.2.5.e) Tarefas críticas envolvendo alto nível de risco devem ser executadas após aprovação prévia do representante de segurança do INPE.	A	A	A	A

continua

Quadro B.2: Continuação

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
1.6.2.6 Utilização - Fase E				
1.6.2.6.a) A análise de segurança deve avaliar o projeto e as mudanças operacionais por impacto na segurança, assegurando que as margens de segurança sejam mantidas e que as operações sejam conduzidas dentro do risco aceito.	A	A	A	D
1.6.2.6.b) A análise deve também apoiar a avaliação de anomalias operacionais por impacto na segurança e a avaliação contínua das tendências de risco.	A	A	A	D
1.6.3 Pacote de Dados de Segurança				
1.6.3.a) O fornecedor deve preparar e entregar o pacote de dados de segurança.	A	A	A	A
1.6.3.b) O conteúdo do pacote de dados de segurança deve ser definido para cada projeto ou programa pela autoridade de segurança do projeto.	A	A	A	A
1.7 Certificação de segurança				
1.7.a) Todos os projetos devem certificar a segurança dos hardwares de voo e sistemas de solo como tendo atingido um nível aceitável de risco em conformidade com os requisitos de segurança específicos do projeto.	A	A	A	A
1.7.b) Deve ser de responsabilidade da organização do projeto fornecer à autoridade de certificação todas as informações relacionadas à segurança necessárias para permitir que a declaração de conformidade com a segurança seja aceita e entendida.	A	A	A	A
1.8 Treinamento de segurança				
1.8.1 Treinamento				
1.8.1.a) Todo treinamento relacionado à segurança de qualquer equipe que trabalhe - permanentemente ou ocasionalmente - com produtos e / ou atividades que possam ter propriedades perigosas deve ter três aspectos principais:	A	A	A	A
1) *briefings* de conscientização geral sobre medidas de segurança a serem tomadas em um determinado local ou ambiente de trabalho;				
2) treinamento técnico básico em técnicas e habilidades de segurança exigidas (por exemplo, inspeção, teste, manutenção ou integração), que são obrigatórias para cumprir a função de trabalho sob consideração; e				
3) treinamento específico do produto que enfoque os riscos relacionados ao produto específico.				

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
1.8 Treinamento de segurança				
1.8.2 Participação				
1.8.2.a) A participação no *briefing* geral de conscientização deve ser obrigatória para todo o pessoal que tiver acesso à área onde o produto espacial é processado.	A	A	A	A
1.8.3 Registros				
1.8.3.a) Devem ser mantidos registros do pessoal que recebeu treinamento.	A	A	A	A
1.9 Acidentes / inquérito e investigação de incidentes				
1.9.a) O fornecedor deve relatar à entidade responsável todos os acidentes e incidentes que afetem o produto espacial e que ocorrerem durante as atividades do projeto, sob o controle do fornecedor ou de seus subfornecedores.	A	A	A	A
1.10 Documentação de segurança				
1.10.1 Geral				
1.10.1.a) O fornecedor deve manter dados relacionados à segurança para dar suporte a revisões e certificação de segurança.	A	A	A	A
1.10.2 Revisão de fornecedor				
1.10.2.a) O fornecedor deve revisar a documentação do projeto, incluindo especificações, desenhos, análises, procedimentos e relatórios, relatórios de não conformidade, relatórios de falha, *waivers* e alterações na documentação, a fim de verificar ou avaliar o impacto em:	A	A	A	A
1) implementação de requisitos de segurança e controles de riscos e perigos;				
2) incorporação de controles de risco e perigo no projeto ou no programa de verificação;				
3) conclusão das atividades de verificação;				
4) concepção e segurança operacional do sistema; e				
5) validade das análises de segurança realizadas e documentadas.				

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
1.10 Documentação de segurança				
1.10.3 Desvios e *Waivers* de segurança				
1.10.3.a) O fornecedor deve identificar todos os desvios e *waivers* que afetem os requisitos aplicáveis de segurança do projeto.	A	A	A	A
1.10.3.b) O representante de segurança do fornecedor para o projeto deve rever esses desvios e *waivers* para garantir que os possíveis impactos na segurança sejam totalmente analisados.	A	A	A	A
1.10.3.c) Deve ser fornecida justificativa adequada para qualquer desvio considerado aceitável pelo fornecedor.	A	A	A	A
1.10.4 Arquivo de lições aprendidas				
5.10.4.a) As lições de segurança aprendidas devem considerar, no mínimo:	A	A	A	A
1) o impacto de requisitos recém impostos;				
2) avaliação de todas as avarias, acidentes, anomalias, desvios e desistências;				
3) eficácia das estratégias de segurança do projeto;				
4) novas ferramentas e métodos de segurança que foram desenvolvidos ou demonstrados;				
5) verificações efetivas e ineficazes que foram realizadas; e				
6) mudanças propostas para a política de segurança, estratégia ou requisitos técnicos com justificativa.				
2 Engenharia de segurança				
2.1 Princípios da segurança do projeto				
2.1.1 Consideração da Vida Humana				
2.1.1.a) A preservação da segurança do pessoal deve ser a prioridade mais importante no desenvolvimento e operação de sistemas espaciais.	A	A	A	A

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
2.1.2 Detecção de Perigo - Sinalização				
2.1.2.a) Os recursos de monitoramento, exibição, alarme e segurança devem ser incorporados para assegurar que o hardware de voo, o pessoal e as instalações estejam em condições seguras (por exemplo: alarmes de incêndio, som / luz de emergência, etc.).	A	A	A	A
2.1.2.b) Estas capacidades devem fornecer as informações necessárias para permitir que o pessoal realize ações que sejam necessárias para protegê-las das consequências de falhas em funções críticas de segurança e a falha de medidas de controle de risco.	A	A	A	A
2.1.3 Redução e Controle de Risco de Segurança				
2.1.3.1 Avaliação de Gravidade de Consequência				
2.1.3.1.a) A gravidade dos eventos perigosos identificados deve ser categorizada.	A	A	A	A
2.2 Requisitos de tolerância de falha				
2.2.1 Requisitos Básicos				
2.2.1.a) A tolerância a falhas é um dos requisitos básicos de segurança usados para controlar os perigos. O projeto do sistema deve atender aos seguintes requisitos de tolerância a falhas:				
b) Nenhuma falha individual ou erro do operador terá consequências críticas (ou catastróficas).	A	A	A	A
c) Nenhuma combinação de:	A	A	A	A
1) duas falhas, ou				
2) dois erros do operador ou				
3) uma falha e um erro do operador podem ter consequências catastróficas.				

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
2.2.2 Projeto para risco mínimo				
2.2.2.a) Os riscos relacionados ao risco mínimo para as áreas do projeto (por exemplo, mecanismos, estruturas, vasos de pressão, linhas e conexões pressurizadas, dispositivos pirotécnicos, compatibilidade de materiais e inflamabilidade dos materiais) devem ser controlados pelas propriedades e características relacionadas à segurança do projeto; como margem ou fatores de segurança.	A	A	A	A
2.2.2.b) Os requisitos de tolerância a falhas devem ser somente aplicados ao processo de *design* conforme necessário para garantir que falhas confirmadas que possam afetar o projeto não invalidem as propriedades relacionadas à segurança.	A	A	A	A
2.2.2.c) As instalações do centro de testes espaciais devem estar de acordo com a norma ECSS-Q-ST-20-07C	A	A	A	A
2.2.2 Projeto para risco mínimo				
2.3 Identificação e controle de funções críticas de segurança				
2.3.a) Uma função do sistema que, se perdida ou degradada, ou por operação incorreta ou inadvertida, resultaria em uma consequência perigosa catastrófica ou crítica, deve ser identificada como função crítica de segurança. EXEMPLO: Uma série de eventos operacionais que podem resultar em perigo se ocorrerem inadvertidamente ou se forem operados fora de ordem.	A	A	A	A
3 Segurança operacional				
3.1 Operações em solo				
3.1.1 Revisão e Inspeção				
3.1.1.a) As revisões e inspeções de prontidão devem incluir revisão de segurança e avaliação de instalações, equipamentos, artigos de teste, procedimentos de operação, teste e contingência, controles de acesso e recursos de pessoal para conformidade com os requisitos de segurança.	A	A	A	A

continua

Quadro B.2: Continuação.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
3.1.2 Requisitos de equipamento de suporte de solo (GSE)				
3.1.2.a) O equipamento de suporte de solo (GSE) deve estar sujeito a análise de risco.	A	A	A	A
3.1.2.b) Para operações terrestres, a análise deve abordar:	A	A	A	A
1) potenciais consequências perigosas de erro humano e falha de processos;				
2) adequação e manutenção das margens operacionais;				
3) potencial de exposição humana a perigos e efeitos perigosos;				
4) requisitos para treinamento de operadores em solo; e				
5) adequação das informações e dados fornecidos pelo equipamento de voo, equipamento de suporte de solo (GSE) ou equipamento de teste para apoiar no desempenho das operações de acordo com os requisitos de segurança aplicáveis.				
4 Requisitos e técnicas de análise de segurança				
4.1 Análise de segurança				
4.1.1 Geral				
4.1.1.a) A análise de segurança deve ser refinada e atualizada de forma iterativa à medida em que o projeto avançar, de modo a garantir que os perigos e eventos perigosos sejam avaliados e que os requisitos operacionais e de projeto detalhados relevantes, controles de risco e atividades de verificação, sejam definidos e implementados.	A	A	A	A
5 Verificação de segurança				
5.1 Rastreamento de perigos				
5.1.1 Relatórios de Perigos identificados				
5.1.1.a) O fornecedor deve estabelecer um sistema para registrar os perigos assim como procedimentos para rastrear o status de todos os perigos identificados.	A	A	A	A
5.1.1.b) O sistema deve ser aplicado para todos os perigos com consequências catastróficas e críticas.	A	A	A	A
5.1.1.c) As informações relacionadas com princípios, processo, implementação e requisitos da análise de perigos devem ser descritas conforme orientações contidas na norma ECSS-Q-ST-40-02C.	A	A	A	A

continua

Quadro B.2 – Conclusão.

Requisitos aplicáveis a projetos	Grande	Médio	Pequeno	Nano
5.2 Qualificação				
5.2.a) As características de todas as funções críticas de segurança devem ser totalmente qualificadas por meio de testes.	A	A	A	A
5.2.b) O teste de qualificação da função crítica de segurança deve incluir a determinação das margens de desempenho, considerando-se as combinações de pior caso de ambientes naturais e induzidos, e condições de operação.	A	A	A	A
5.2.c) Qualificação “por similaridade” deve ser aplicada somente após a aprovação do cliente, caso a caso.	A	A	A	A
5.3 Encerramento de um perigo				
5.3.1 Verificação da garantia de segurança				
5.3.1.a) Na preparação para o envio do equipamento de voo para o local de lançamento, a garantia de segurança deve verificar se:	A	A	A	A
1) Ressalvas feitas pelo engenheiro responsável ainda são válidas;				
2) Não houve descuidos;				
3) As verificações refletem o status *as-built* /*as-modified* do hardware de voo;				
4) Todas os itens pendentes neste momento são aceitáveis para envio ao local de lançamento;				
5) Todas as verificações abertas foram inseridas no registro de rastreamento de verificação de segurança (SVTL), de acordo com a norma ECSS-Q-ST-40C, que agora se torna um documento ativo.				
5.3.2 Autoridade de Aprovação de Segurança				
5.3.2.a) O fechamento de cada perigo requer aprovação da autoridade responsável pela segurança. Os perigos só podem ser considerados prontos para encerramento quando:	A	A	A	A
1) forem eliminados;				
2) tiverem sido minimizados e controlados de acordo com o requisito aplicável e as atividades de verificação associadas tenham sido concluídas com sucesso; ou				
3) a autoridade responsável pela segurança tiver concedido um desvio ou *waiver*.				

Fonte: Produção da autora.