



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

**Avaliação de Riscos Cibernéticos aplicado ao
processo de Consciência Situacional do Centro de
Defesa Cibernética do Comando da Aeronáutica**

Cleber Mitchell de Lima

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Orientadora

Prof.a Dr.a Simone Borges Simão Monteiro

Brasília
2022

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

ML732a Mitchell de Lima, Cleber
Avaliação de Riscos Cibernéticos aplicado ao processo de
Consciência Situacional do Centro de Defesa Cibernética do
Comando da Aeronáutica / Cleber Mitchell de Lima;
orientador Prof.a Dr.a Simone Borges Simão Monteiro. --
Brasília, 2022.
219 p.

Dissertação (Mestrado - Mestrado Profissional em
Computação Aplicada) -- Universidade de Brasília, 2022.

1. Segurança Cibernética. 2. Defesa Cibernética. 3.
Consciência Situacional. 4. Gestão de Riscos. I. Borges
Simão Monteiro, Prof.a Dr.a Simone, orient. II. Título.



Universidade de Brasília

Instituto de Ciências Exatas
Departamento de Ciência da Computação

**Avaliação de Riscos Cibernéticos aplicado ao
processo de Consciência Situacional do Centro de
Defesa Cibernética do Comando da Aeronáutica**

Cleber Mitchell de Lima

Dissertação apresentada como requisito parcial para conclusão do
Mestrado Profissional em Computação Aplicada

Prof.a Dr.a Simone Borges Simão Monteiro (Orientadora)
PPCA/UnB

Prof.a Dr.a Viviane Vasconcellos Ferreira Grubisic Prof. Dr. Edison Ishikawa
Membro Externo Membro Interno

Prof. Dr. Marcelo Ladeira
Coordenador do Programa de Pós-graduação em Computação Aplicada

Brasília, 24 de fevereiro de 2022

Dedicatória

Dedico este trabalho de mestrado à minha esposa e à minha filha, pois sem estas pessoas em minha mente e ao meu lado, eu não chegaria ao final deste desafio. Dedico, em segundo lugar àqueles que saem todos os dias de suas casas com o propósito de ensinar, que tiram seu sustento oferecendo conhecimento, coragem e incentivo aos que querem aprender, e sobretudo àqueles que não abrem mão deste compromisso, pois está arraigado indelevelmente em suas almas.

Agradecimentos

Nenhum homem é uma ilha, conforme dito por John Donne, há muitos séculos. Somos um conjunto de experiências e interdependências que nos levam mais longe e nos permitem ser o que somos. Cada obra que fazemos é fruto de conhecimento, ímpeto, força, mas sobretudo do apoio e colaboração de outros seres humanos.

Sempre temos muito a agradecer, primeiramente baseado em minhas crenças mais profundas a Deus, que me mantém nos trilhos da humildade, da humanidade e da fé. Aos meus pais que me ensinaram o valor do trabalho, do estudo e da família. À minha esposa, que surgiu em minha jornada como e com uma promessa que dali em diante, eu teria uma aliada, uma cúmplice, que não me deixaria ser menos do que preciso ser, por mais difícil que seja a estrada, companhia constante em meus sonhos e realizações. À minha filha que, ao chegar, me mostrou o sentido de não ser mais único, mas tornar-me um modelo e porto seguro, uma responsabilidade e uma honra. Aos meus professores, em especial à minha orientadora, pelo apoio e direcionamento seguros, os quais há muito chamo de amigos, pois também enveredei pela seara insana de trilhar esta jornada da educação. Aos meus alunos, filhos que considero como meus, e dos quais sinto orgulho ao ver seus progressos. À Força Aérea Brasileira, pelos mais de 40 anos de serviço compartilhados, pelo apoio e auxílio, representados pelas pessoas que a compõem, em especial aos meus chefes e companheiros de jornada, sem os quais, nada deste trabalho teria sido possível. Aos amigos que nunca faltaram, e que muito incentivaram. Aos colegas do PPCA, mais novos amigos, aos quais agradeço muito a companhia, o compartilhamento dos conhecimentos e preocupações e os tão importantes "empurrões" pois a jornada é árdua, porém, vamos muito mais longe acompanhados, segundo um antigo provérbio popular africano.

E, finalmente, estranhamente, agradeço às dificuldades, aos momentos não felizes, às dores e às frustrações, pois nos indicam nossas fraquezas, nossas necessidades de reforço e nos fazem mais fortes, humildes, quebrando nossas arrogâncias e vaidades, notavelmente em um trabalho de pesquisa como este, que busca analisar as vulnerabilidades do mundo digital cibernético e as fragilidades e malícias de alguns comportamentos humanos.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES), por meio do Acesso ao Portal de Periódicos.

Resumo

Este trabalho resulta do estudo sobre segurança cibernética (SC) e de suas implicações práticas, a partir do entendimento das necessidades apresentadas pelo governo brasileiro, por meio do Ministério da Defesa (MD), de dotar o país com processos de segurança (SC) e defesa cibernéticas (DC). As dificuldades de implementação de processos de SC e de DC apresentadas pelos órgãos governamentais são multidisciplinares, aumentando a complexidade da empreitada solicitada aos setores de DC das Forças Armadas Singulares (FA). Em função destes fatores, o foco da pesquisa limitou-se ao desenvolvimento de um processo de avaliação de riscos cibernéticos, componente de um macroprocesso de aquisição de consciência situacional cibernética (CSC). O resultado deste processo é a criação de um índice de riscos cibernéticos (IRC), indicador representativo do maior nível de risco cibernético a que os ativos sob responsabilidade dos centros de defesa cibernética das FA e do MD podem estar sujeitos, apresentado de forma quantitativa. O MD encarregou o Comando da Aeronáutica (COMAER) do estabelecimento de um indicador multifatorial do nível de alerta de comprometimento (NAC) do seu espaço cibernético de interesse, às ameaças identificadas e medidas, cujo IRC compõe o elo central do processo de obtenção do NAC. Esta pesquisa aplicada, baseia-se em estudo de caso, com componentes qualitativos para seu embasamento e compõe-se por procedimentos técnicos, como análise documental, entrevistas (não-estruturadas, semiestruturadas e estruturadas) e brainstormings como ferramentas básicas para obtenção dos conhecimentos e validações dos resultados. O processo de pesquisa permitiu compreender as implicações envolvidas, como a identificação e compreensão do significado da segurança cibernética, sua especialização em defesa cibernética e os impactos na organização em estudo, em sua finalidade institucional. O principal resultado esperado e obtido foi o de definir as linhas gerais do processo de avaliação de riscos cibernéticos (ARCiber) com seu conseqüente IRC. O reconhecimento foi evidenciado pela implementação do ARCiber na organização como efeito direto do estudo e da validação por esta pesquisa.

Palavras-chave: Segurança Cibernética, Defesa Cibernética, Consciência Situacional, Gestão de Riscos

Abstract

This work results from the study on cyber security (CS) and its practical implications, from the understanding of the needs presented by the Brazilian government, through the Ministry of Defense (MD), to provide the country with cybersecurity processes (CS) and cyber defense (DC). The issues of implementing CS and CD processes presented by government agencies are multidisciplinary, increasing the complexity of the contract requested from the CS sectors of the Single Armed Forces (FA). Due to these factors, the focus of the research was limited to the development of a cybernetic risk assessment process, a component of a cybernetic situational awareness (CSC) macro process. The result of this process is the creation of a cyber risk index (IRC), an indicator representing the highest level of cyber risk to which the assets under the responsibility of the cyber defense centers of the FA and MD may be subject, presented in a quantitative manner. The MD tasked the Air Force Command (COMAER) with the establishment of a multifactorial indicator of the compromise alert level (NAC) of its cyberspace of interest, the threats identified and measures, whose IRC forms the central link in the process of obtaining the NAC. This applied research is based on a case study, with qualitative components for its foundation and is composed of technical procedures, such as document analysis, interviews (unstructured, semi-structured and structured) and brainstorming as basic tools for obtaining knowledge and validations of results. The research process allowed us to understand the implications involved, such as the identification and understanding of the meaning of cyber security, its specialization in cyber defense and the impacts on the organization under study, in its institutional purpose. The main result expected and obtained was to define the general lines of the cyber risk assessment process (ARCiber) with its consequent IRC. The recognition was evidenced by the implementation of ARCiber in the organization as a direct effect of the study and validation by this research.

Keywords: Cybersecurity, Cyber Defense, Situational Awareness, Risk Management

Sumário

1	Introdução	1
1.1	Contextualização do Problema	1
1.2	Justificativa do Tema	2
1.3	Objetivos	4
1.3.1	Objetivo Geral	4
1.3.2	Objetivos Específicos	4
1.4	Contribuição Esperada	5
1.5	Estrutura do trabalho	5
2	Revisão do Estado da Arte	7
2.1	Descrição do TEMAC	7
2.1.1	Preparação da pesquisa	8
2.1.2	Apresentação e inter-relação dos dados	12
2.1.3	Detalhamento, modelo integrador e validação por evidências	20
3	Referencial Teórico	25
3.1	Segurança da Informação	25
3.2	Segurança Cibernética	26
3.2.1	Defesa e Guerra cibernéticas para o contexto do Governo Brasileiro.	30
3.3	Gestão de Riscos (GR)	31
3.3.1	Gestão de Riscos Cibernéticos (GRCiber)	36
3.4	Processo de Aquisição de Consciência Situacional Cibernética (CSC)	39
3.4.1	Compreensão da importância dos processos de CSC	39
3.4.2	Análise dos processos de CSC	41
4	Metodologia da Pesquisa	48
4.1	Classificação da pesquisa	48
4.2	Estrutura da pesquisa	50

5	Resultados	71
5.1	Análise do Contexto de Defesa Cibernética	71
5.1.1	Legislações e iniciativas norteadoras do tema segurança cibernética	72
5.1.2	Ações realizadas pelo Governo Federal para a implantação da segurança cibernética	76
5.2	Entendimento do processo de CSC do NuCDCAer	77
5.2.1	Identificação da saída do processo – NAC	77
5.2.2	Análise dos índices componentes do NAC	79
5.2.3	Exame dos procedimentos de cálculo do NAC	82
5.3	Estabelecimento do processo de Avaliação de Riscos Cibernéticos para o NuCDCAer	83
5.3.1	Seleção do modelo de gestão de riscos cibernéticos	83
5.3.2	Desenho do processo de Avaliação do Risco Cibernético para o NuCDCAer	91
5.4	Geração do processo de obtenção do IRC	96
5.5	Criação da ferramenta computacional para cálculo do IRC	113
5.5.1	Estruturação da ferramenta de cálculo do IRC	113
5.5.2	Desenvolvimento da ferramenta de cálculo	115
5.6	Validação da ferramenta computacional e do método de cálculo do IRC	125
5.6.1	Emprego da ferramenta computacional e definição do processo de validação	125
5.6.2	Execução da investigação para validação	126
6	Conclusão	132
6.1	Resultados obtidos	132
6.2	Limitações da pesquisa	134
6.3	Sugestões para aprofundamento e pesquisas correlatas	134
	Referências	135
	Apêndice	144
A	Entrevista estruturada para qualificação dos profissionais do NuCDCAer	145
B	Entrevista semiestruturada para Levantamento dos Processos das Seções do NuCDCAer	152
C	Entrevista semiestruturada para entendimento na criação do IRC	154

D	Resultado da entrevista semiestruturada para análise dos grupos de controle e controles para avaliação dos riscos	160
E	Resumo e análise da entrevista estruturada sobre a validação da planilha de cálculo do IRC sob o método DELPHI para a etapa 6	168
F	Artigos publicados durante o período do PPCA	199

Lista de Figuras

2.1	Modelo TEMAC	8
2.2	Países que mais publicaram sobre o tema	12
2.3	Artigos e Citações ano a ano.	13
2.4	Mapa de calor dos autores mais citados	17
2.5	Mapa de calor de palavras-chave	19
2.6	Mapa de calor de cocitações	20
2.7	Mapa de calor de acoplamento bibliográfico (<i>Coupling</i>)	21
3.1	Relacionamento entre segurança cibernética e outras seguranças	27
3.2	Conceitos e relações de segurança	28
3.3	Triângulo do Risco	32
3.4	O processo de gestão de riscos	33
3.5	Diagrama de processos da gestão de riscos pela ISO 27005:2019	35
3.6	Processo de avaliação de risco cibernético	37
3.7	Avaliação de risco cibernético malicioso e não malicioso.	38
3.8	Processo de Aquisição de Consciência Situacional Cibernética	42
3.9	Aprofundamento do Processo de Aquisição de CSC	46
4.1	Classificação da pesquisa	49
4.2	Estrutura da pesquisa	51
4.3	qualificação dos profissionais entrevistados	59
5.1	Níveis de Decisão no EC	74
5.2	Processos de Aquisição de CSC	80
5.3	Processo de Avaliação de Riscos Cibernéticos	84
5.4	Subprocessos de identificação de riscos cibernéticos maliciosos e não maliciosos	89
5.5	Diagrama do Processo de Avaliação de Riscos Cibernéticos do NuCDCAer	91
5.6	Nuvem de palavras que primeiro vêm à mente dos entrevistados em SC/DC	99
5.7	Diagrama do Processo de Avaliação de Riscos Cibernéticos do NuCDCAer	114

5.8	Planilha 1 – Cadastro do Contexto e relatório de IRC	117
5.9	Planilha 2 – Análise de vulnerabilidades pelos controles	118
5.10	Planilha 3 – Tabelas de valores de base para os controles	119
5.11	Produtos ou Serviços (ativo agregador)	120
5.12	Dispositivos (ativos componentes)	121
5.13	Controles para avaliação do ambiente dos ativos(questionário)	122
5.14	Cadastro de Processos de Negócio	123
5.15	Registro de Riscos (avaliação dos riscos de serviços ou produtos)	124
5.16	Modelo conceitual de fluxo do método Delphi para esta pesquisa	126

Lista de Tabelas

2.1	Pesquisas por palavras-chave sem limitações de tempo e área de pesquisa	10
2.2	Pesquisas por palavras-chave com limitação temporal	10
2.3	Pesquisas por palavras-chave com limitação temporal e por área	11
2.4	Aplicação dos critérios de inclusão e exclusão	11
2.5	Identificação das revistas mais relevantes	12
2.6	Autores que mais publicaram sobre o tema	14
2.7	Identificação dos 15 autores e artigos mais citados	16
2.8	Quantidade de trabalhos dentro das áreas de pesquisa	18
2.9	Artigos selecionados para o estudo	23
5.1	Níveis de Alerta Cibernético	78
5.2	Funções e categorias do NIST CSF	101
5.3	Agrupamentos de controles e controles para avaliação de riscos	102
5.4	Definição da Eficácia dos Controles	110
5.5	Valores e condições de criticidade dos ativos ou serviços estratégicos	112
5.6	Resultado da validação da ferramenta via método Delphi	129

Lista de Abreviaturas e Siglas

APF Administração Pública Federal.

ARCiber Avaliação de Riscos Cibernéticos.

BPM Business Processes Management.

BPMN Business Process Model and Notation.

C2 Sistema de Comando e Controle.

CCA-BR Centro de Computação da Aeronáutica de Brasília.

CDCAer Centro de Defesa Cibernética do Comando da Aeronáutica.

CDCiber Centro de Defesa Cibernética.

COMAER Comando da Aeronáutica.

ComDCiber Comando de Defesa Cibernética.

COMGAP Comando Geral de Apoio.

CS Consciência situacional.

CSC Consciência situacional cibernética.

CTIR Centro de Tratamento e Resposta a incidentes de rede.

CVSS Common Vulnerability Scoring System.

DC Defesa Cibernética.

DTI Diretoria de Tecnologia da Informação.

EC Espaço Cibernético.

END Decreto Nº 6.703 – Estratégia Nacional de Defesa.

ENSC Estratégia Nacional de Segurança Cibernética.

ETIR Equipe de Tratamento e Resposta a incidentes de rede.

FA Forças Armadas individuais (Marinha, Exército e Aeronáutica).

FAB Força Aérea Brasileira.

FAC Fator de Ameaça Cibernética.

GC Guerra Cibernética.

GR Gestão de Riscos.

GRCiber Gestão de Riscos Cibernéticos.

GRSI Gestão de Riscos em Segurança da Informação.

IAC Índice de Ameaças Cibernéticas.

ICI Infraestrutura crítica da informação.

IFA Projeto de Integração em Defesa Cibernética das Forças Armadas.

IIC Índice de Incidentes Cibernéticos.

IRC Índice de Riscos Cibernéticos.

LGPD Lei 13.709/2020 - Lei Geral de proteção de Dados Pessoais.

MD Ministério da Defesa do Brasil.

NAC Nível de Alerta Cibernético.

NuCDCAer Núcleo do Centro de Defesa Cibernética do Comando da Aeronáutica.

SC Segurança Cibernética.

SDSI Subdivisão de Segurança da Informação.

SGSI Seção de Gestão de Segurança da Informação.

SI Segurança da Informação.

SIC Segurança da Informação e Comunicações.

SMDC Sistema Militar de defesa Cibernética.

TI Tecnologia da Informação.

TIC Tecnologia da Informação e Comunicações.

USAF United States Air Force.

Capítulo 1

Introdução

1.1 Contextualização do Problema

O Ministério da Defesa do Brasil (MD) identificou a necessidade de estruturação da Defesa Cibernética (DC) como forma de dotá-lo com elementos executivos e, em caso de aumento do grau de agressão ou do nível de ameaça cibernética, evoluir para uma possível Guerra Cibernética (GC), viabilizados por centros de defesa cibernética nas forças armadas singulares (Exército, Marinha, Força Aérea). Este esforço conjunto visa aumentar a resiliência do Espaço Cibernético (EC) brasileiro e alinhar-se à Política e Estratégia Nacional de Defesa [1], documento de ordenação da defesa nacional, em vigor.

O primeiro passo para a concretização do projeto foi a criação do Comando de Defesa Cibernética (ComDCiber), órgão hospedado no Comando do Exército, mas gerido pelo MD.

O Núcleo de Defesa Cibernética do Comando da Aeronáutica (NuCDCAer) é um órgão recém-criado, e o primeiro dos centros a iniciar suas operações, a partir de uma força singular, por meio da alteração de função de outra organização, o Centro de Computação da Aeronáutica de Brasília (CCA-BR), motivo pelo qual as duas letras iniciais (Nu) da sigla refletem sua situação de estágio de estruturação, que ao terminar, adotará simplesmente a sigla CDCAer.

O elemento central de qualquer ação em segurança cibernética é representado por processos de aquisição de consciência situacional cibernética (CSC), mais conhecido na língua inglesa como *cyber situation awareness*.

Consciência situacional (CS), segundo Endsley [2], é estabelecida como uma dinâmica humana na tomada de decisões em uma grande variedade de domínios do conhecimento. A CS, segundo Endsley compreende três passos: a percepção, a compreensão e a projeção. Estes passos levam à dedução de que consciência situacional estabelece uma análise e avaliação de uma situação presente que pode ter desdobramentos futuros, ou seja, procura

criar uma projeção sobre momento atual, como uma tentativa de predição de eventos possíveis ou plausíveis a curto, médio ou longo prazos. Para o projeto de defesa cibernética brasileira, a CSC é o elo primordial, composta por processos que fornecem as informações que cumprem os passos identificados por Endsley.

Os macroprocessos componentes da CSC para o projeto do NuCDCAer são três: a) processo que captura os dados do tráfego de redes e identifica incidentes reais ou potenciais, denominado Gestão de Incidentes de Rede; b) processo que busca descobrir ameaças potenciais sob diversas fontes, e sob análise da inteligência, oferecer informações sobre ameaças cibernéticas, denominado Inteligência de Ameaças Cibernéticas; c) o processo que é o objeto desta pesquisa, o qual condensa e analisa riscos aos ativos, auxilia os demais subprocessos na avaliação dos riscos cibernéticos e busca oferecer um tratamento quantitativo a estes riscos, denominado Gestão de Riscos Cibernéticos.

Cabe ressaltar que, apesar de o processo referir-se a gestão de riscos, não significa ser esta a única ou a principal atividade da organização. Esta limitação de visão se deve ao escopo da pesquisa, limitada ao processo de avaliação dos riscos, que, de acordo com a ABNT NBR ISO/IEC 27005 [3] compreende a identificação, a análise e a avaliação dos riscos. Este processo tem a finalidade de produzir um índice, reflexo do projeto de atividade mais importante neste momento, a integração de esforços entre as forças armadas para a gestão dos riscos cibernéticos, obedecendo a destinação do tipo da organização, conforme será visto a seguir.

Logo o problema principal de pesquisa é: Como desenvolver um processo de avaliação de riscos cibernéticos, que produza um Índice de Riscos Cibernéticos (IRC) para processos de Defesa Cibernética a fim de indicar o nível de risco que o Espaço Cibernético (EC) de interesse está submetido?

O IRC poderá influenciar, dentro de uma perspectiva quantitativa, a identificação do nível de comprometimento do espaço cibernético analisado, auxiliando a composição de um índice estratégico denominado Nível de Alerta Cibernético (NAC), a ser usado para as ações efetivas de defesa cibernética.

Este foco norteará a seguir, nas próximas seções, a justificativa para o estudo do tema, bem como os objetivos a serem alcançados, a revisão da literatura disponível e a metodologia a ser adotada.

1.2 Justificativa do Tema

Segundo o relatório da empresa Sonicwall, sobre cyber ataques [4], desde 2017, o mundo vem experimentando um incremento de até 102% no volume de malwares ao ano, observados mês a mês. Este fato, apesar de não se evidenciar, em 2020, o mesmo nível

de crescimento, incluiu um aumento considerável, tanto no número de ataques virtuais quanto na sofisticação. O motivo observado decorre em função da crise gerada pela pandemia de COVID-19 e em função do isolamento social necessário para sua contenção, conforme o mais novo relatório da mesma instituição [5].

Ataques virtuais, apresentados sob diversos tipos, seja no tráfego da rede, seja nos dados dos dispositivos de armazenamento domésticos e empresariais, privados ou públicos, há constante ameaça de olhares indiscretos. Portanto, há como inferir que não gerir os riscos do EC configura uma atividade que pode trazer prejuízos às finanças e à imagem das instituições, bem como ao país.

A Estratégia Nacional de Segurança Cibernética (ENSC) [6] diagnosticou o problema com dados objetivos que justificam ações em segurança cibernética. Este documento compilou dados que evidenciam serem conectados via Internet até 100% dos órgãos federais, 98% das empresas, 74,9% dos domicílios. Concluiu-se que o Brasil ocupa o 2º lugar entre os países com maior prejuízo com ataques cibernéticos, fato explicitado pela estatística da ENSC com somente 11% dos órgãos federais possuindo bom nível de governança em TI.

Segundo a Política e Estratégia Nacional de Defesa (END) [1], o Brasil possui três setores estratégicos para a defesa nacional, os setores espacial, o nuclear e o cibernético. Especificamente para o setor cibernético necessita haver capacitações destinadas aos espectros dos usos industriais, educativos e militares, com prioridade às tecnologias de comunicação, e aos contingentes das forças armadas, de forma a ampliar e assegurar sua atuação em rede.

Algumas prioridades da END para o setor cibernético são:

- Fortalecer o Centro de Defesa Cibernética (CDCiber) do Ministério da Defesa (MD), objetivando evoluir para um Centro de Defesa Cibernética das Forças Armadas, cujo desenvolvimento é de interesse dos setores de DC.
- Estabelecer um processo de obtenção de CS sobre os riscos do EC do Brasil;
- aprimorar a segurança da informação e comunicações (SIC) das forças armadas;
- fomentar a pesquisa científica voltada para o setor cibernético;
- desenvolver tecnologias que permitam o planejamento e a execução da DC, contribuindo para a segurança cibernética nacional; e
- estruturar a produção de conhecimento oriundo da fonte cibernética.

Confirmando as necessidades de contribuição de todas as partes constituintes da sociedade, o Decreto 10.222/2020 (não paginado) [6] que institui a Estratégia Nacional de

Segurança Cibernética, em seu eixo temático de pesquisa, desenvolvimento e inovação, item 2.2, sugere:

A aproximação dos programas de mestrado e doutorado não só em computação aplicada, mas em outras áreas do conhecimento, pode ser uma via eficaz para formação, aprimoramento e qualificação de pessoal interessado no tema, além de geração de conhecimento. Brasil (2020, não paginado) [6]

Segundo a descrição do Projeto de Implantação e Consolidação da Estrutura de Desenvolvimento Conjunto de Defesa Cibernética, cujo inteiro teor não pode ser divulgado, é importante ressaltar que este projeto depende da consolidação da capacidade operativa de gestão de riscos. Isto porque só é possível gerar uma verdadeira consciência situacional sobre o espaço cibernético a partir da compreensão sobre seus ativos críticos, os riscos a que estão submetidos e os impactos de seu eventual comprometimento para a missão de cada Força Singular e do CDCiber. Sem este conhecimento, as informações sobre os incidentes de rede não serão de grande valia para os responsáveis pelo ciclo de tratamento no âmbito do ComDCiber. Além do mais, sem esta capacidade operativa, haverá carência de meios objetivos para o estabelecimento do nível de alerta cibernético.

Há, concomitantemente, necessidade de se estabelecerem requisitos para criação ou aquisição de ferramentas objetivas de procedimentos de identificação, análise e avaliação de riscos cibernéticos com foco em resultados quantitativos e geração de painéis (*dashboards*) de informação do nível de comprometimento do Espaço Cibernético (EC) do país.

1.3 Objetivos

Esta seção contém os objetivos geral e específicos que guiarão a pesquisa.

1.3.1 Objetivo Geral

O objetivo geral desta pesquisa é estruturar um processo de avaliação de riscos capaz de mensurar o valor do risco cibernético para o macroprocesso de aquisição de consciência situacional cibernética da Seção de Gestão de Segurança da Informação (SGSI) do Núcleo de Defesa Cibernética do Comando da Aeronáutica (NuCDCAer).

1.3.2 Objetivos Específicos

Para que seja possível atingir este objetivo geral, será necessário que alguns objetivos específicos sejam alcançados, a saber:

1. Caracterizar Defesa Cibernética e sua relevância para o NuCDCAer;
2. Investigar o processo de aquisição de Consciência Situacional Cibernética (CSC);
3. Definir processo de avaliação de riscos focado em cenários de riscos cibernéticos, guiado pelo processo de gestão de CSC;
4. Propor um índice de riscos cibernéticos (IRC) a partir da aplicação do processo de avaliação de riscos desenvolvido;
5. Desenvolver uma ferramenta computacional para a implementação do processo de avaliação de riscos; e
6. Avaliar a ferramenta computacional desenvolvida em seus aspectos metodológicos.

1.4 Contribuição Esperada

O cenário econômico do país, aliado aos efeitos da pandemia de COVID19 intensificou as ameaças cibernéticas, reduziu o orçamento de defesa e expôs fragilidades de gestão da segurança interna.

O maior benefício esperado refere-se ao uso imediato deste processo, para avaliação prática de riscos que diariamente ameaçam a segurança do espaço cibernético sob a responsabilidade do NuCDCAer.

A Doutrina Militar de Defesa Cibernética [7] considera que o Brasil, uma nação que se impõe como soberana, necessita possuir capacidades de contraposição às ameaças externas, ou mesmo internas, cujos efeitos se podem sentir nos noticiários diários versando sobre supostos ataques cibernéticos às estruturas dos países, empresas e até mesmo das pessoas que possuem informações disponíveis no espaço cibernético.

O relatório de 2021 da empresa SonicWall [5] configura-se como uma evidência deste combate diário entre interesses diversos e dos prejuízos decorrentes dos incidentes cibernéticos nele registrados.

1.5 Estrutura do trabalho

Este trabalho foi estruturado em seis capítulos, sendo este primeiro o de Introdução. Para facilitar o entendimento desta pesquisa os demais capítulos estão organizados como descrito a seguir: O Capítulo 2 traz uma revisão do estado da arte sobre o tema e suas implicações nas pesquisas atuais, bem como oferece um olhar no passado para compreender o momento que o tema passou a ser pesquisado, com a quantidade de trabalhos e de

citações ao longo dos anos, por meio da Teoria do Enfoque Meta Analítico – TEMAC. O Capítulo 3 efetua uma revisão geral sobre o tema de pesquisa, com o embasamento teórico sobre os assuntos que compõem o tema. O Capítulo 4 apresenta o processo proposto para a execução da pesquisa, com a classificação e organização das etapas executadas da pesquisa. O Capítulo 5 demonstra os resultados obtidos, diretamente ligados às etapas da pesquisa. O Capítulo 6 oferece uma conclusão com o resumo dos resultados obtidos, uma visão das limitações da pesquisa e sugestões para aprofundamento do tema e possíveis pesquisas correlatas.

Capítulo 2

Revisão do Estado da Arte

Os próximos tópicos deste capítulo referem-se ao estudo do estado da arte da pesquisa em si a respeito de sua atualidade e qualidade, obtido via Teoria do Enfoque Meta Analítico Consolidado – TEMAC.

Lakatos e Marconi [8] refletem que uma pesquisa científica é precedida pela escolha do tema, representado pelo problema a ser resolvido, elaboração do plano de trabalho e após, a identificação de possíveis fontes de informação para aprofundamento no tema. Para esta pesquisa lançou-se mão de revisão bibliográfica e documental, primeiro passo na delimitação do tema e ajuste dos objetivos, mas sensível a interferências por falta de qualidade ou confiabilidade das fontes. Com a finalidade de facilitar esta busca na consecução da revisão bibliográfica, Mariano e Rocha [9] apresentaram um método sistemático denominado pelos autores como “Teoria do enfoque meta-analítico consolidado”, identificado pela sua sigla “TEMAC”. Este método busca possibilitar um levantamento sobre discussões científicas acerca do tema, identificando a relevância, quantidade e direção das pesquisas para obtenção de uma base de dados qualificada para a realização da pesquisa.

2.1 Descrição do TEMAC

O modelo usado para o desenvolvimento do referencial bibliográfico deste trabalho está embasado na aplicação do TEMAC, o qual está fundamentado em três passos básicos para identificação da origem e qualidade da literatura pesquisada, por meio de análise via leis da bibliometria, conforme a Figura 2.1.

Este método é dividido em três partes, a preparação da pesquisa, a apresentação e inter-relação dos dados e o detalhamento, modelo integrador e validação por evidências, os quais serão explicitados nos próximos tópicos.

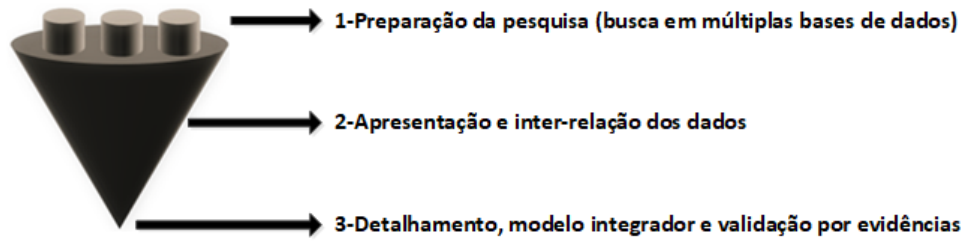


Figura 2.1: Modelo TEMAC
 Fonte: Mariano e Rocha [9]

2.1.1 Preparação da pesquisa

Nesta etapa busca-se delimitar os limites da pesquisa como as áreas do conhecimento; o lapso temporal de produções analisadas; as bases de dados científicas utilizadas e o conjunto de palavras-chave que habilitou a busca por trabalhos científicos dentro do mesmo tema geral.

A pesquisa teve como foco o gerenciamento de riscos e obtenção de consciência situacional cibernética, buscadas, respectivamente, nas bases de dados ISI-Web of Science e Scopus.

Uso de palavras-chave

A busca se deu em função das temáticas gerenciamento de riscos (*Cyber* risk management*), avaliação de riscos (*Cyber* risk assessment*), análise de riscos (*Cyber* risk analysis*), defesa cibernética (*Cyber* defen?e [defense or defence]*), guerra cibernética (*Cyber* warfare*) e consciência situacional cibernética (*Cyber* situational awareness*), para cercar o tema principal sob todo o ecossistema de aspectos em forma de chaves de busca, acrescido. A Tabela 2.1 referencia este aspecto. Cabe ressaltar o uso dos caracteres coringa de busca (*) e (?) para que as diferenças de termos e de grafias possam ser incorporadas para análise, e não serem desnecessariamente filtradas, sendo o asterisco (*) o caractere que substitui um ou vários caracteres alfanuméricos em sua localização e o caractere de interrogação (?) aquele que substitui um e somente um caractere alfanumérico onde for representado. As bases de dados Web of Science e Scopus aceitam este recurso de filtro em suas strings de busca.

Espaço-tempo da pesquisa

A pesquisa foi, inicialmente, delimitada pelo maior tempo possível, disponível nas plataformas de buscas de bases de dados, entre 1945 e 2021, de forma a compreender o surgimento e evolução do tema. A avaliação final se deu com redução do intervalo de

busca a 7 anos (2014-2021), como exibido na Tabela 2.2, segundo as recomendações de Mariano e Rocha (2017), que sugerem um espaço temporal de 5 a 10 anos.

Áreas do conhecimento pesquisadas

Os dados da busca encontram-se descritos na Tabela 2.3, englobando a áreas de conhecimento “Ciência da Computação” e “Engenharia” como mais relevantes para o tema, porém sem estabelecer um intervalo fechado nestas áreas, para compreensão de assuntos acessórios, caso algum artigo relevante se enquadre em alguma categoria com pouco representatividade, mas alta relevância sobre o tema.

Critérios de inclusão e exclusão

Após a busca inicial e delimitação temporal e de áreas pesquisadas, se faz necessário uma delimitação levada em consideração pelo tema da pesquisa em si, sob a ótica de critérios que possibilitem a inclusão de uma referência bibliográfica como fonte da pesquisa, de outros que identifiquem motivos de exclusão de um trabalho por não atingir os objetivos desejados para a pesquisa e de um terceiro que estabeleça o procedimento de uso dos critérios em relação aos filtros criados, conforme Tabela 2.4. Para tal adotou-se os seguintes critérios:

- Critérios de inclusão
 - Abordar o tema segurança cibernética de acordo com a norma ABNT NBR ISO/IEC 27032:2015;
 - Gestão de riscos;
 - Gestão de riscos em uma perspectiva de riscos cibernéticos;
 - Abordar processos de consciência situacional de uma forma generalizada com preferência para as abordagens dentro da área cibernética;
 - Possuir foco em processos de gestão em segurança cibernética;
 - Estar de acordo com os objetivos da pesquisa;
 - Possuir boa quantidade de citações;
 - Caso não possua citações ou sejam em pouca quantidade, ser recente e relevante ao tema de pesquisa (ainda não citados, mas com potencial, ou utilidade identificada).
- Critérios de exclusão
 - Trabalhos fora do contexto de inclusão;

- Abordagens fora da ciência da computação e das engenharias, exceto se servir de embasamento a teorias buscadas;
- Temas relativos à construção de dispositivos técnicos e de aspectos intrínsecos a telecomunicações;
- Técnica para seleção:
 - Leitura dos resumos em busca de critérios de exclusão;
 - Leitura do texto completo em busca dos critérios que indiquem estar alinhados aos objetivos da pesquisa.

Estabelecimento dos filtros de pesquisa iniciais

Cada figura representa uma pesquisa por palavras-chave na base ISI – Web of Science (WoS) e Scopus, e foram divididas segundo os critérios:

Primeiro: Isento de qualquer limitação temporal (somente a das bases de dados), conforme Tabela 2.1.

Tabela 2.1: Pesquisas por palavras-chave sem limitações de tempo e área de pesquisa

Tipo do campo de busca	Palavras-chave e operadores de pesquisa	Período da busca	Áreas pesquisadas	Total de publicações encontradas	Base de Dados
TITLE-ABS-KEY (<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 5px; margin-right: 10px;"> "cyber* risk management" OR "cyber*risk assessment" OR "cyber*risk analysis" OR "cyber* defen?e" OR "cyber* warfare" </div> <div style="margin-right: 10px;">AND</div> <div style="border: 1px solid black; padding: 5px;"> "cyber* Situational Awareness" </div> </div>	"Sem filtros, pelo máximo disponível da base de dados"	"Sem filtros"	781	ISI Web of Science (WoS)
				31	Scopus

Segundo: Após inserida limitação temporal, conforme Tabela 2.2.

Tabela 2.2: Pesquisas por palavras-chave com limitação temporal

Tipo do campo de busca	Palavras-chave e operadores de pesquisa	Período da busca	Áreas pesquisadas	Total de publicações encontradas	Base de Dados
TITLE-ABS-KEY (<div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 5px; margin-right: 10px;"> "cyber* risk management" OR "cyber*risk assessment" OR "cyber*risk analysis" OR "cyber* defen?e" OR "cyber* warfare" </div> <div style="margin-right: 10px;">AND</div> <div style="border: 1px solid black; padding: 5px;"> "cyber* Situational Awareness" </div> </div>	AND LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014)	"Sem filtros"	643	ISI Web of Science (WoS)
		25		Scopus	

Terceiro: Incluída limitação de áreas de pesquisa aos filtros já utilizados, conforme Tabela 2.3.

Tabela 2.3: Pesquisas por palavras-chave com limitação temporal e por área

Tipo do campo de busca	Palavras-chave e operadores de pesquisa	Período da busca	Áreas pesquisadas	Total de publicações encontradas	Base de Dados	
TITLE-ABS-KEY ("Cyber* risk management" OR "Cyber*risk assessment" OR "Cyber*risk analysis" OR "cyber* defen?e" OR "cyber* warfare"	AND "Cyber* Situational Awareness"	AND LIMIT-TO (PUBYEAR , 2020) OR LIMIT-TO (PUBYEAR , 2019) OR LIMIT-TO (PUBYEAR , 2018) OR LIMIT-TO (PUBYEAR , 2017) OR LIMIT-TO (PUBYEAR , 2016) OR LIMIT-TO (PUBYEAR , 2015) OR LIMIT-TO (PUBYEAR , 2014)	AND LIMIT-TO (SUBJAREA, "COMP") OR LIMIT-TO (SUBJAREA, "ENGI")	360	ISI Web of Science (WoS)
					24	Scopus

Quarto: Usada aplicação dos critérios de inclusão e exclusão, conforme Tabela 2.4.

Tabela 2.4: Aplicação dos critérios de inclusão e exclusão

Limitações adicionais	Total de publicações encontradas	Base de Dados
"Aplicação dos critérios de inclusão e exclusão"	60	WoS e Scopus

A partir deste ponto foi removida a necessidade de separação por base de dados, em virtude de os resumos e palavras-chave serem agrupados para aumentar a eficiência do processo. Para aplicação dos critérios de inclusão e exclusão foi observado o resumo (de forma preliminar) e/ou palavras-chave dos 384 artigos, sendo interpretado algum aspecto de exclusão, reduziu-se o número de trabalhos a serem lidos para 161. Após observação mais minuciosa dos trabalhos reservados, foi observada a quantidade de citações e uma avaliação mais minuciosa do resumo dos artigos, tendo sido reduzido o número de trabalhos com significância para 60 artigos, compondo uma base de leitura factível de análise aprofundada.

Vale ressaltar que esta quantidade não compreende o universo total de fontes de pesquisa que podem compor a pesquisa final, em virtude de haver materiais de análise documental (leis e decretos, resoluções, portarias normativas etc.) além de normativos diversos e outros artigos eventualmente encontrados, com relevância ao estudo, permanecendo este total selecionado como um guia de tendências e de fonte de subsídios gerais à pesquisa.

2.1.2 Apresentação e inter-relação dos dados

Revistas mais relevantes

Tendo em vista a base de dados ISI Web of Science anteriormente citada, foi possível elencar na seção (JCR) as revistas com maior fator de impacto dentro das áreas de Computer Science e Engineering.

Tabela 2.5: Identificação das revistas mais relevantes

Posição	Nome da Revista	Fator de impacto	Citações
1	IEEE Communications Surveys and Tutorials	23.700	18,995
2	Information Fusion	13.669	6,409
3	Journal of Statistical Software	13.642	25,372
4	IEEE WIRELESS COMMUNICATIONS	11.391	8,140
5	IEEE TRANSACTIONS ON EVOLUTIONARY COMPUTATION	11.169	15,581
6	MEDICAL IMAGE ANALYSIS	11.148	9,028
7	IEEE Transactions on Cybernetics	11.079	17,681
8	Journal of Industrial Information Integration	10.615	592
9	IEEE Internet of Things Journal	9.936	12,832
10	IEEE Transactions on Systems Man Cybernetics-Systems	9.309	12,083

Fonte: ISI Web Of Science

Deste modo, foram listadas as 10 revistas mais relevantes, conforme a Tabela 2.5.

Países que mais publicaram sobre o tema



Figura 2.2: Países que mais publicaram sobre o tema

Fonte: ISI Web Of Science

Pode-se observar pela Figura 2.2 que o tema é mais efetivamente publicado por países como Estados Unidos, Inglaterra e China, com a predominância em larga escala do idioma inglês.

O Brasil foi representado na pesquisa com três publicações, ocupando a 24ª colocação neste levantamento específico. Os artigos brasileiros, apesar de apontarem o tema, não receberam citações e não trouxeram contribuição direta à pesquisa, por não estarem alinhados aos critérios de inclusão e exclusão.

Identificação da evolução do tema e de citações ano a ano

Para a classificação do tema, foi ampliada a pesquisa para o máximo prazo disponível no Web of Science (1945-2021) e no Scopus (2002-2021), verificando-se que o tema começou a ganhar mais importância a partir de 2013, quando a curva de crescimento de publicações pela Figura 2.3(a) e consequentemente de citações, pela Figura 2.3(b), foi quase exponencial.

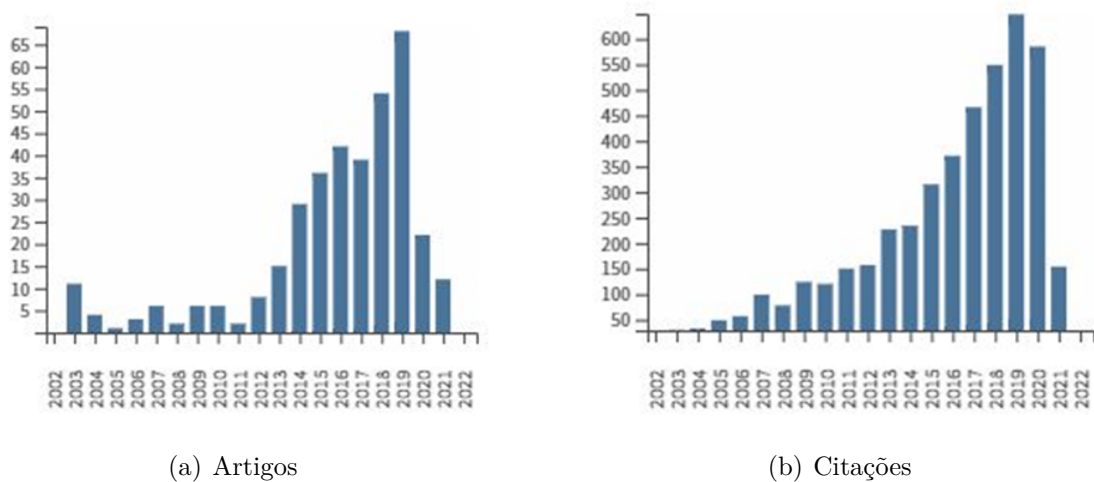


Figura 2.3: Artigos e Citações ano a ano.

Fonte: ISI Web Of Science e Scopus

Cabe ressaltar que o artigo mais citado dentro do tema de pesquisa já totaliza mais de 7000 citações, escrito em 1995 por Endsley M.R. [2], sobre a teoria da consciência situacional (CS) e a capacidade decisória humana, dentro do ambiente da aviação militar na Força Aérea dos Estados Unidos (USAF), e por Franke ([10], que compilou uma revisão de literatura sobre consciência situacional cibernética (CSC), especificando o tema, mas não abrindo mão da citação de Endsley em diversos artigos que a pesquisadora participou sobre o tema.

Autores que mais publicaram

Neste t3pico pode-se notar que h3 uma correla33o parcial entre os autores que mais publicaram e os que mais foram citados, o que pode ser interpretado que uma grande produ33o n3o significa, necessariamente, um grande reconhecimento cient3fico. N3o h3, concomitantemente uma rela33o expl3cita entre os autores que t3m seus trabalhos publicados em mais de uma base de dados de publica333es, como pode ser observado na Tabela 2.6 e os mais citados, conforme a Tabela 2.7.

Tabela 2.6: Autores que mais publicaram sobre o tema

Web of Science (WoS)		Scopus	
Endsley, MR	65	Endsley, M.R.	107
Al-shaer, E	13	Liu, P.	19
Xu, S.	11	Al-Shaer, E.	17
Skopik, F	10	Aubuchon-Endsley, N.L.	17
Janicke, H	9	Atighetchi, M.	15
Kaber, DB	9	Connors, E.S.	15
Leenen, L	9	Xu, S.	15
Zhu, QY	9	Skopik, F.	14
Jajodia, S	8	Jajodia, S.	13
Mehetre, BM	8	Gonzalez, C.	12
Atighetchi, M	7	Zhu, Q.	12
Franke, U	7	Endsley, M.P.	11
Liu, P	7	Jacobson, D.	11
Husak, M	6	Janicke, H.	11
Knox, Bj	6	Kaber, D.B.	11
Kotenko, I	6	Rursch, J.A.	11
Kott, A	6	Fulghum, D.A.	10
Ottis, R	6	Strater, L.D.	10
Reith, M	6	Bolstad, C.A.	9
Rursch, JA	6	Franke, U.	9
Sutterlin, S	6	Kott, A.	9
Van Vuuren, JJ	6	Ottis, R.	9
Bolstad, Ca	5	Pal, P.	9
Chen, Jt	5	Riley, J.M.	9
Fiedler, R	5	Yang, S.J.	9
Ganesan, R	5	Betser, J.	8
Grobler, M	5	Campbell, W.B.	8
Helkala, K	5	Carvalho, M.	8
Holm, H	5	Mehetre, B.M.	8
Irwin, B	5	Nithipatikom, K.	8
Lu, WL	5	Rajivan, P.	8

Fonte: ISI Web Of Science e Scopus

Esta compara33o permite visualizar que autores como Endsley [2], Franke [10], n3o s3o aparecem na lista de mais publicados como na lista de mais citados, sendo outros como Barford [11], Webb [12] e Tadda [13] que apesar de n3o serem os mais publicados, s3o

bastante citados em outros trabalhos, revelando a importância de suas pesquisas e de serem citados neste trabalho.

Identificação dos autores e artigos mais citados

Prosseguindo com a análise, notou-se que os artigos com maior número de citações foram os que mais contribuição trouxeram ao tema pesquisado, conforme exposto pela Tabela 2.7. Segundo Mariano e Rocha [9], a finalidade desta fase é a de identificar que autores têm a liderança quantitativa de publicações sobre o tema.

Tabela 2.7: Identificação dos 15 autores e artigos mais citados

Título	Autores	Ano	Citações ISI WoS	Citações Scopus
Toward a theory of situation awareness in dynamic systems	Endsley, M.R.	1995	3010	4481
Cyber situational awareness - A systematic review of the literature	Franke, U., Brynielsson, J.	2014	92	146
Cyber situational awareness: from geographical alerts to high-level management	Barford, P., Dacier, M., Dietrich, T.G., Wang, C., Yen, J.	2010	81	82
A situation awareness model for information security risk management	Webb, J., Ahmad, A., Maynard, S.B., Shanks, G.	2014	52	76
Final reflections: Situation awareness models and measures	Endsley, M.R.	2015	39	23
Overview of cyber situation awareness	Tadda, G.P., Salerno, J.S.	2010	33	53
Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks	Holm, Hannes, Ekstedt, Mathias, Andersson, Dennis	2012	34	54
High level information fusion for tracking and projection of multistage cyber attacks	Yang, SJ, Stotz, A, Holsopple, J, Sudit, M, Kuhl, M	2009	30	55
Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies	Paté-Cornell, M.-E., Kuypers, M., Smith, M., Keller, P.	2018	27	36
Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection	Öğüt, H., Raghunathan, S., Me-non, N.	2011	27	38
Framework and principles for active cyber defense	Denning, D.E.	2014	24	30
Lessons Learned From Complex Hands-on Defence Exercises in a Cyber Range	Vykopal, J, Vizvary, M, Oslejsek, R, Celeda, P, Tovarnak, D	2017	19	29
An integrated cyber security risk management approach for a cyber-physical system	Kure, H.I., Islam, S., Razzaque, M.A.	2018	16	18
Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management	Ganin, A.A., Quach, P., Panwar, M., Marchese, D., Linkov, I.	2020	16	25
Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study	Granasen, M, Andersson, D	2016	15	20

Fonte: ISI Web Of Science e Scopus

Para reforçar a análise foi gerado o mapa de calor de citações, Figura 2.4, via software VOSviewer, confirmando os autores já presentes na lista textual.

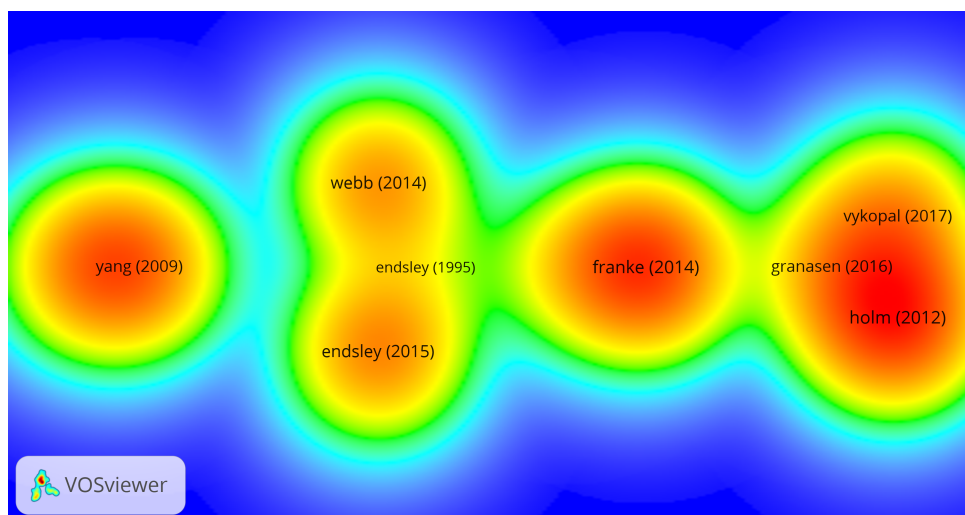


Figura 2.4: Mapa de calor dos autores mais citados

Fonte: VOSviewer Software [14], com dados de ISI Web of Science e Scopus

O mapa de calor de citações revela quatro grupos básicos (clusters) de autores, aparecendo Endsley (1995, 2015) em uma cor um tanto mais clara, provavelmente pela distribuição temporal das citações de seu trabalho mais utilizado nas pesquisas, com Franke (2014) e Yang (2009) em clusters isolados. Porém a importância de seus trabalhos possui peso na escolha do rumo da pesquisa, onde encontra-se no primeiro cluster, o trabalho de Yang (2009) [15] focando em ataques cibernéticos em redes de computadores, e a necessidade de fusão de sensores de dados para corresponder ao incremento de complexidade dos ataques, expandindo a capacidade humana de resposta a estes eventos. No segundo cluster há dois autores, sendo Endsley (1995, 2015) [2] [16] em seus artigos de 1995, com mais de 7000 citações e a revisão da própria autora em 2015 que foca no aspecto cognitivo da aquisição de consciência situacional, trabalhos acompanhados por Webb (2014) [12] cujo trabalho foca em desenvolver um sistema de gerenciamento de riscos de segurança da informação baseado em consciência situacional, cujo foco dado utiliza o modelo de Endsley (2015) para estabelecer um trabalho para serviços de inteligência dos Estados Unidos. No terceiro cluster encontra-se Franke (2014) [10] com o importante foco em uma revisão sistemática acerca do tema consciência situacional cibernética com a revisão de 102 artigos. Finalmente no quarto cluster aparecem 3 autores Holm (2012) [17], Granasen (2009) [18] e Vykopal (2017) [19] focados no estabelecimento de exercícios coordenados com foco em cibersegurança e medição de efetividade, demonstrando a urgência que a situação dos últimos tempos exige, com o aumento substancial e amplo dos ataques cibernéticos, com o primeiro com assunto diretamente importante a esta pesquisa, a classificação de severidade de vulnerabilidades de segurança cibernética pelo padrão internacional *Common*

Vulnerability Scoring System (CVSS) [20] a ser utilizado durante o uso da metodologia de avaliação de riscos, neste trabalho.

Identificação da quantidade de trabalhos dentro das áreas de pesquisa

As áreas de pesquisa após os filtros aplicados revelaram a grande concentração do assunto em ciência da computação, seguida de engenharia, conforme demonstrado pela Tabela 2.8, a qual revela o valor numérico dos trabalhos pelas áreas de pesquisa, ressaltando-se que o número de registros, se somado, ultrapassa o total de trabalhos encontrados, em função de alguns trabalhos estarem classificados em mais de uma área.

Tabela 2.8: Quantidade de trabalhos dentro das áreas de pesquisa

Áreas de pesquisa	Registros	% de 384
Computer science	361	97.043
Engineering	100	26.882
Telecommunications	36	9.677
Education educational research	12	3.226
Psychology	5	1.344
Behavioral sciences	4	1.075

Fonte: ISI Web Of Science e Scopus

As áreas de ciências humanas revelam o interesse no tema tanto para gestão de riscos (normalmente não cibernéticos) quanto de conhecimentos acerca de consciência situacional, pois é assunto pertinente no mercado de trabalho, em estudos comportamentais e na área de educação, sendo tema em crescimento, conforme os artigos observados, apesar de não se enquadrarem exatamente no tema de pesquisa.

Análise de palavras-chave

Nesta fase trata-se a identificação das palavras-chave utilizadas nos artigos encontrados. Segundo Mariano et al. [21] as palavras-chave são importante indicativo a respeito da evolução do tema e das linhas de pesquisa. As palavras-chave foram obtidas nas buscas pelas bases de dados WoS e Scopus, exportadas para uma planilha Excel e após, foi utilizada a ferramenta VOSviewer que revela as palavras-chave mais evidenciadas em um mapa, Figura 2.5, para uma melhor visualização em termos de concentração de uso das palavras nos artigos.

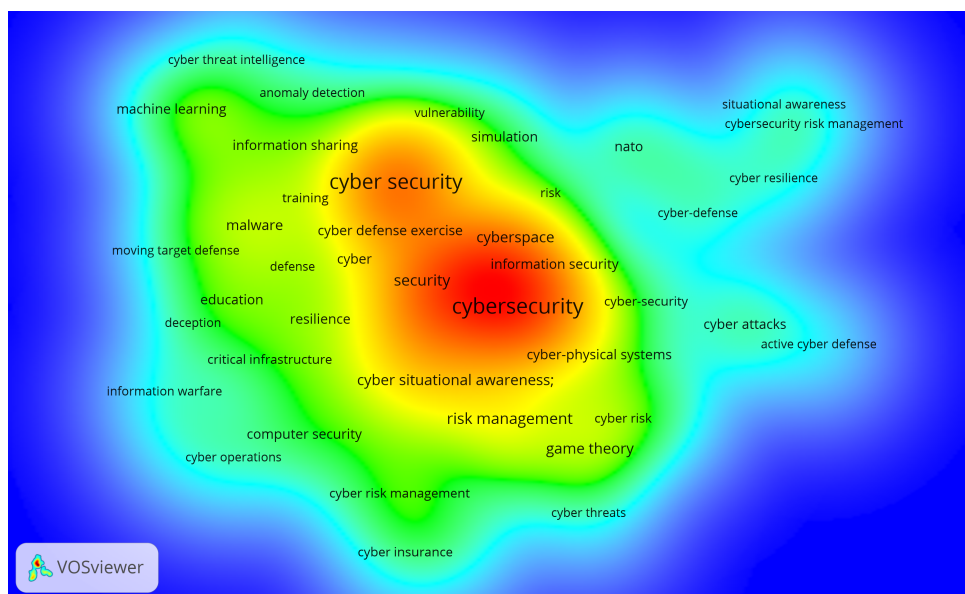


Figura 2.5: Mapa de calor de palavras-chave

Fonte: VOSviewer Software [14] com dados de ISI Web of Science e Scopus

Analisando as principais palavras-chave encontradas, tem-se que as palavras-chave mais citadas formam o tema central da pesquisa. Defesa cibernética baseada em gestão de riscos cibernéticos, apoiada por uma consciência situacional cibernética. Nota-se além disto que próximo ao núcleo do cluster encontram-se palavras-chave importantes como compartilhamento de informações, exercícios em defesa cibernética, o ciberespaço, resiliência, gerenciamento dos riscos, treinamento, entre outras cujos temas serviram para complementar o discurso de defesa da importância desta pesquisa para o NuCDCAer como organização e o quê isto pode impactar positivamente na missão final deste centro. Estes temas correlatos puderam oferecer novos olhares, como a diferença entre tipos de riscos durante o estudo de gerenciamento de riscos; a importância do controle do espaço cibernético ou ciberespaço por meio da consciência situacional cibernética e também da necessidade de se estabelecerem jogos ou exercícios cibernéticos constantes para metrificar a capacidade de detecção e resposta, apesar deste tema fugir ao tema central da pesquisa, mas sendo correlato, reforça a importância dos estudos e da formalização do conhecimento obtido pela pesquisa e pelos resultados dos possíveis exercícios.

Por meio destas análises pôde-se observar a importância da análise bibliométrica antes de se efetuar a pesquisa, em função do ganho possível de qualidade e profundidade do trabalho.

2.1.3 Detalhamento, modelo integrador e validação por evidências

Dentro do método estabelecido pelo TEMAC, nesta fase encontram-se importantes análises acerca das contribuições e abordagens autorais por meio de *coupling* com as frentes de pesquisa e a análise de *co-citation* que oferece as principais abordagens no tema com citações conjuntas agrupadas em *clusters*, bem como os artigos mais citados na pesquisa.

Cocitações

De acordo com Mariano e Rocha [9], uma boa referência para a verificação dos artigos que mais têm citações em comum, ou seja, são citados juntos, é o recurso de Cocitação (*Co-citation*), com a finalidade de identificar semelhanças entre trabalhos de pesquisa.

O mapa de calor das cocitações, Figura 2.6, apresenta algumas concentrações, o que evidencia a abrangência do tema em análise, que se referencia com aspectos como consciência situacional, em enfoques humano e cibernético, gerenciamento de riscos geral e cibernético, além de defesa e guerra cibernéticas, que juntos formam a base da pesquisa representada.

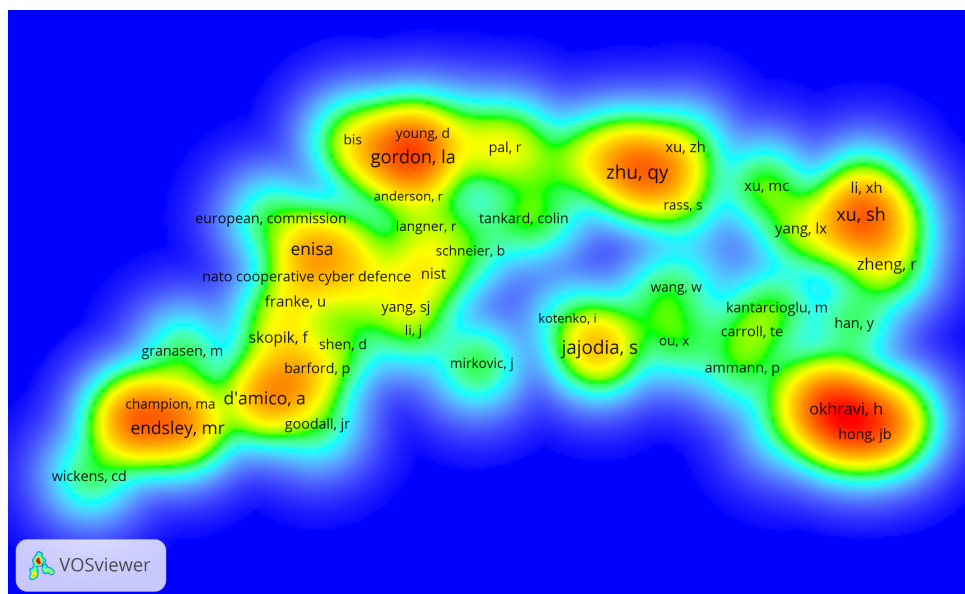


Figura 2.6: Mapa de calor de cocitações

Fonte: VOSviewer Software [14] com dados de ISI Web of Science e Scopus

O mapa de calor indica 5 *clusters* principais, que, apesar de não estarem diretamente conectados (semelhanças entre si) indicam grupos de abordagens identificadas pelas chaves de busca utilizadas com finalidade útil para a pesquisa.

O primeiro *cluster*, representado pelos trabalhos de Endsley [16] e Champion [22] abordam o princípio da consciência situacional e o limite decisório em situações de risco tendo por base o elemento humano, na aviação militar (*USAF*) para Endsley e para equipes de tratamento e resposta a incidentes de rede (ETIR) segundo Champion. O segundo *cluster*, com Gordon [23] e Anderson [24], tratam de aspectos econômicos da segurança da informação, contendo o trabalho de Young [25], que foca em risco cibernético de infraestruturas críticas, mas sob a ótica de investimentos em seguros, o que o habilita a estar neste *cluster*. O terceiro *cluster* composto pelos trabalhos de Zhu [26] e Xu [27], revela trabalhos de pesquisadores chineses com base em gerenciamento de riscos cibernéticos em dispositivos físicos conectados em redes corporativas. O quarto foca em procedimentos de defesa cibernética ativa contra ataques, de forma preventiva e reativa, com o uso de modelos matemáticos diversos. O quinto *cluster*, com Okhravi [28] e Hong [29], demonstra trabalhos que objetivam também defesa cibernética, porém com foco em estratégias gamificadas e baseadas em domínios para sistemas dinâmicos.

***Coupling* (Acoplamento bibliográfico)**

Segundo Mariano e Rocha [9], semelhante à análise de Cocitação, o *Coupling* oferece informações sobre grupos de artigos com similaridades, entretanto tendo por base a premissa de que artigos que possuem mesmas citações tendem a conter pontos comuns. O *coupling* ou acoplamento bibliográfico representa os *fronts* de pesquisa, ou seja, os artigos que possuem referências em comum, revelando abordagens em fortalecimento.

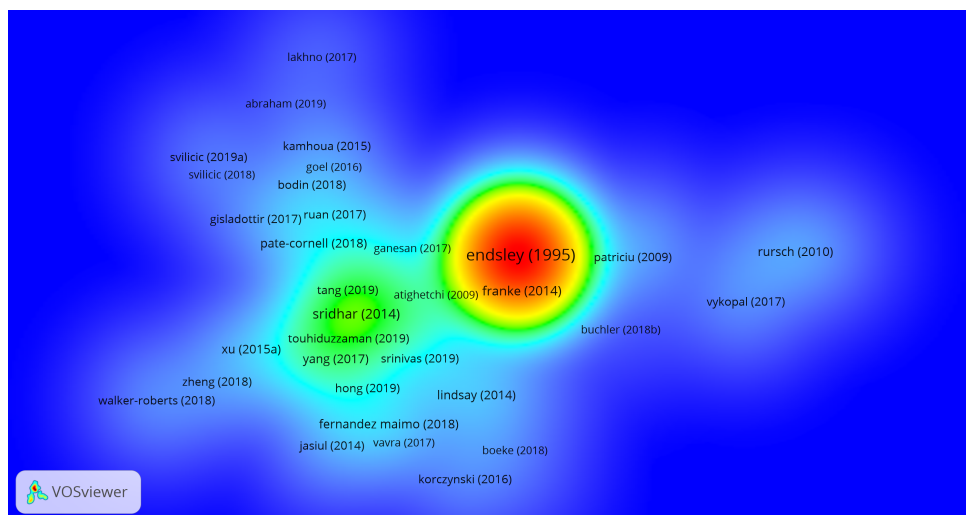


Figura 2.7: Mapa de calor de acoplamento bibliográfico (*Coupling*)

Fonte: VOSviewer Software [14] com dados de ISI Web of Science e Scopus

Os trabalhos de Endsley [2] e Franke [10] possuem forte relação, pois o último autor revela um trabalho de revisão sistemática, onde Endsley ocupa lugar de destaque em função dos diversos trabalhos publicados e citados no trabalho de Franke, bem como citações de seus próprios trabalhos, o que leva a um acoplamento de alto nível, porém sem perder a significância ou a validade.

Há um segundo *cluster*, com um acoplamento menos evidenciado pelo mapa de calor, mas ainda pertencente ao conjunto maior formado pelo primeiro *cluster*, cujos autores Hong[29] e Sridhar [30] ataques cibernéticos (*Cyber Attacks*) devem ser detectados e mitigados por uma camada de proteção cibernética (*Cyber Protection*) formadas por sistemas automáticos. Os trabalhos de Ganesan [31], Srinivas [32] e Tang [33] tratam de forma similar de segurança cibernética (*Cybersecurity*) via tratamento dos dados e processos de gestão e análise para aumento da segurança, seja por definições de padrões e recomendações, por compartilhamento de informações ou pelo tratamento de grandes quantidades de dados via processos de *big data*. Touhiduzzaman [34] e Yang [35] tratam da defesa cibernética via análises que estabelecem métricas para as ameaças cibernéticas via gamificação e/ou modelagem de processos de ataque e defesa, para o entendimento e ação de proteção.

Artigos mais aderentes ao tema estudado

Dentre os artigos mais citados, alguns foram selecionados não somente pela quantidade de citações, o que sugere um padrão de qualidade do autor, mas pela relevância ao tema e pela amplitude e profundidade de suas abordagens, além de artigos que surgiram na análise com temas correlatos, como Holm [17] na análise do CVSS, incorporado à pesquisa antes mesmo de se avaliar, dentro do desenvolvimento da metodologia de avaliação de riscos a necessidade de sua utilização. Autores consagrados como Endsley, que, apesar de seu mais citado artigo ter sido publicado em 1995, soma mais de 7000 citações ao longo das 2 décadas. A autora é referência no tema consciência situacional, em especial no ambiente de alta carga de risco como a aviação militar (*USAF*), compatível com os estudos de consciência situacional cibernética, que não prescindem da atenção humana. Esta relação também se verifica em outros autores como em Franke and Brynielsson [10], Barford et al. [11], Webb et al. [12], entre outros, como demonstrado pela Tabela 2.9, cujas abrangências foram de análise e avaliação de riscos cibernéticos e consciência situacional cibernética por meio de equipes humanas e de sistemas automatizados.

Tabela 2.9: Artigos selecionados para o estudo

Título	Autor(es)	Ano	Linha de Pesquisa	Citações ISI-WoS	Citações Scopus
Toward a theory of situation awareness in dynamic systems	Endsley, M.R.	1995	Risk management, situational awareness	3010	4481
Cyber situational awareness - A systematic review of the literature	Franke, U., Brynielsson, J.	2014	Cyber risk management, cyber situational awareness	92	146
Cyber situational awareness: from geographical alerts to high-level management	Barford, P., Dacier, M., Dietterich, T.G., (...), Wang, C., Yen, J.	2010	Cyber risk management, situational awareness	81	82
A situation awareness model for information security risk management	Webb, J., Ahmad, A., Maynard, S.B., Shanks, G.	2014	Risk management, situational awareness	52	76
Final reflections: Situation awareness models and measures	Endsley, M.R.	2015	Risk management, situational awareness	39	23
Overview of cyber situation awareness	Tadda, G.P., Salerno, J.S.	2010	Cyber risk management, situational awareness	33	53
Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies	Paté-Cornell, M.-E., Kuypers, M., Smith, M., Keller, P.	2018	Cyber risk management, Cyber risk assessment, Cyber risk analysis	27	36
Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection	Ögüt, H., Raghunathan, S., Menon, N.	2011	Cyber Risk management	27	38
Framework and principles for active cyber defense	Denning, D.E.	2014	Cyber Defense	24	30
Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study	Granasen, M., Andersson, D.	2016	Cyber Defense	15	20
Guide for Designing Cyber Security Exercises	Patriciu, V. V.; Furtuna, A. C.	2009	Cyber Security	15	-
An integrated cyber security risk management approach for a cyber-physical system	Kure, H.I., Islam, S., Razzaque, M.A.	2018	Cyber Risk management	16	18

Fonte: ISI Web Of Science e Scopus

Os autores e suas linhas de pesquisa formam o arcabouço teórico para a busca temática deste trabalho. Compõem o referencial teórico e a lógica utilizada para estabelecer os processos de consciência situacional cibernética, objetivando a gestão de riscos cibernéticos, por meio de ações de avaliação dos componentes do risco e de quantificação dos mesmos.

Como forma de enumerar os enfoques de pesquisa encontrados via método TEMAC e garantir o alinhamento da busca com o tema proposto por esta pesquisa, foi feita a análise entre os 812 artigos iniciais (sem filtros) com as palavras-chave básicas da pesquisa, conforme demonstrado na Tabela 2.1. Ao final, após as análises por palavras-chave, quantidade de citações, quantidades de publicações sobre o tema, autores mais citados, autores mais publicados, além das cocitações e do acoplamento bibliográfico chegou-se à conclusão que os temas mais importantes para o prosseguimento da pesquisa deveria estar entre a consciência situacional (cibernética ou geral) com enfoque no processo cognitivo por meio dos trabalhos de Endsley [2] [16], proteção cibernética sobre infraestruturas críticas em especial no trabalho de Young [25], gerenciamento de riscos em dispositivos em redes corporativas, sob as pesquisas de Zhu [26] e Xu [27], defesa cibernética com gamificação ou exercícios cibernéticos sob a ótica de Hong [29], além da pesquisa de Holm [17] que também se focou em exercícios cibernéticos de defesa, mas focou na importância

do estabelecimento de valores padronizados de vulnerabilidade segundo o padrão internacional CVSS. Os resultados da filtragem destes autores em particular, apesar de não terem sido completamente úteis a esta pesquisa revelaram a importância dos temas colaterais ao objetivo principal, guiando a busca e aumentando a profundidade das análises, pois a avaliação de riscos cibernéticos necessita de um arcabouço teórico consistente para estabelecer uma metodologia que possa quantificar os riscos. Estes argumentos se sustentam em virtude de a gestão de riscos, da qual a avaliação de riscos é uma parte importante, ser motivada e estabelecida de uma forma sob medida para cada organização, como revela a norma ABNT NBR ISO/IEC 27005:2019. Portanto, além do 10 artigos citados como importantes pela Tabela 2.9, aliam-se os citados nesta análise em virtude do efeito norteador que a pesquisa TEMAC pôde oferecer.

Capítulo 3

Referencial Teórico

Neste capítulo são apresentados conceitos fundamentais para que a proposta do trabalho seja compreendida não somente em sua extensão, mas nos detalhes complexos que envolvem o tema em análise.

3.1 Segurança da Informação

A Norma ABNT NBR ISO/IEC 27001:2013 [36] - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos — é uma norma internacional cujo foco é o de prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI).

A ABNT NBR ISO/IEC 27001:2013 [36] é dividida em 11 seções e um anexo (Anexo A). As seções de 0 a 3 são introdutórias (não obrigatórias), e as seções de 4 a 10 são obrigatórias, devendo seus requisitos serem implementados se a organização desejar estar em conformidade com a norma. Os controles do Anexo A precisam ser implementados, exceto os estritamente declarados como não aplicáveis na Declaração de Aplicabilidade, cujas justificativas precisam ser apresentadas.

O capítulo 4 corresponde à identificação do contexto da organização, seguindo-se os outros capítulos nos assuntos liderança (responsabilidades da alta direção), planejamento (processo de avaliação do risco, declaração de aplicabilidade, e objetivos do processo de segurança da informação), apoio (disponibilidade de recursos gerais), operação (implementação do SGSI), avaliação do desempenho do SGSI e melhoria do processo. O Anexo A compreende 114 controles em 14 seções.

A ABNT NBR ISO/IEC 27002:2013 [37] difere da ISO 27001 em virtude de ser criada com a finalidade de oferecer recursos de boas práticas ao estabelecimento do SGSI. As duas normas estão perfeitamente alinhadas e fornecem a estrutura básica para a implementação

da gestão da segurança da informação em uma organização. A estrutura da ISO 27002 está em conformidade com os controles do anexo A da ISO 27001, porém com um nível de detalhes e de informações substancialmente maior, cuja finalidade é fornecer orientação para implementação destes controles. Cabe ressaltar que nenhuma das normas explica como preparar o processo de segurança da informação, em virtude de ser uma atividade essencialmente sob medida para cada organização. A estrutura da norma ISO 27002 conta com 19 capítulos, sendo os cinco primeiros introdutórios e os demais oferecendo explicação para os controles seguindo a lógica do anexo A da ISO 27001, com os seguintes assuntos: políticas de segurança da informação (SI), organização da SI, segurança de recursos humanos, gestão de ativos, controles de acesso, criptografia, segurança física e do ambiente, segurança das operações, segurança das comunicações, gestão de sistemas de informação, relacionamento na cadeia de suprimento, gestão de incidentes de SI, gestão da continuidade dos negócios, e conformidade legal.

Observando-se a estrutura das duas normas, compreende-se que não se pode pensar em segurança cibernética sem prescindir da visão holística da segurança deste sistema de gestão compreendido por elas. Os controles apresentados passam por todos os macroprocessos da gestão da segurança em si, compreendendo desde a segurança do espaço físico e dos acessos à organização, da proteção aos importantes ativos humanos aos aspectos mais intrínsecos da segurança da informação, como a criptografia, comunicação de dados, requisitos para desenvolvimento de sistemas seguros e como prosseguir no caso de uma catástrofe. Deve ser compreendido que estes controles dependem de uma correta compreensão do contexto e escopo da organização e dos detalhes dos objetivos e processos nos níveis estratégico, tático e operacional para que os controles possam ser criados e operados de forma precisa.

De posse desta compreensão, importa observar os subdomínios da segurança da informação, mais precisamente o de segurança cibernética, tema amplamente abordado em virtude de as empresas terem migrado parte de seus negócios, ou todo ele para o espaço cibernético. Esta ação pode abrir frentes de desenvolvimento técnico e financeiro, mas aumenta, por muitas vezes desproporcionalmente o nível de risco aceito. Para isto precisa-se compreender as características da segurança cibernética, assunto a seguir.

3.2 Segurança Cibernética

A Norma ABNT NBR ISO/IEC 27032:2015 [38] - Tecnologia da Informação — Técnicas de segurança — Diretrizes para Segurança Cibernética (SC), teve sua publicação inicial em 2015. Possui 13 capítulos, sendo os 5 primeiros destinados à contextualização da

norma em si e os demais voltados à organização da segurança cibernética, além de 3 anexos de A a C.

Os capítulos 6 a 13 referem-se à visão geral de segurança e definem visões e funções para: partes interessadas, ativos no Espaço Cibernético (EC), ameaças no EC, papéis das partes interessadas, diretrizes para as partes interessadas, controles, e, finalmente, coordenação e compartilhamento da informação.

Os anexos A a C englobam, respectivamente: prontidão da SC, recursos adicionais, e exemplos de documentos relacionados, como outras normas ISO e IEC e do ITU-T.

De acordo com a norma ABNT NBR ISO/IEC 27032:2015 [38], O Espaço Cibernético pode ser descrito como um ambiente virtual, o qual não existe em qualquer forma física, mas sim, um ambiente ou espaço complexo resultante do surgimento da Internet, somado às pessoas, organizações e atividades em todo o tipo de dispositivos de tecnologia e redes que estão conectados a ele. A segurança do Espaço Cibernético, ou Segurança Cibernética, é a segurança deste mundo virtual. A norma ABNT NBR ISO/IEC 27032:2015 estabelece que as partes interessadas no Espaço Cibernético têm que desempenhar um papel ativo, além de proteger seus próprios bens, para prevalecer a utilidade do Espaço Cibernético. A segurança cibernética se baseia em outras seguranças e da qual se deriva a defesa cibernética em essência. A segurança cibernética está diretamente ligada à segurança da informação, à segurança das aplicações, redes e da Internet, que, sendo a rede das redes, possui seu próprio ecossistema de funcionamento e riscos inerentes, conforme descreve a Figura 3.1.

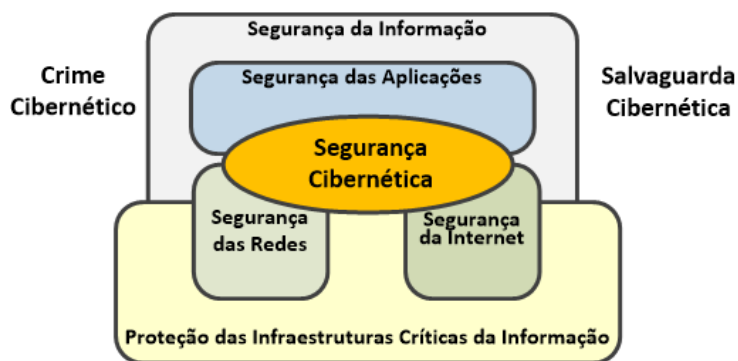


Figura 3.1: Relacionamento entre segurança cibernética e outras seguranças

Fonte: Norma ABNT NBR ISO/IEC 27032:2015 [38]

O tripé da segurança da informação (confidencialidade, integridade e disponibilidade) exerce o mesmo nível de importância na segurança cibernética, e depende da confiabilidade da infraestrutura crítica que a suporta. Como um contexto geral de segurança, tem-se que a segurança refere-se à proteção dos ativos contra ameaças, buscando sempre a

minimização de vulnerabilidades, reforçando barreiras de proteção via estabelecimento de controles e conscientização dos ativos humanos de seus próprios riscos e dos riscos aos elementos constituintes de seu ecossistema. A Figura 3.2 ilustra as relações dos componentes básicos da segurança.

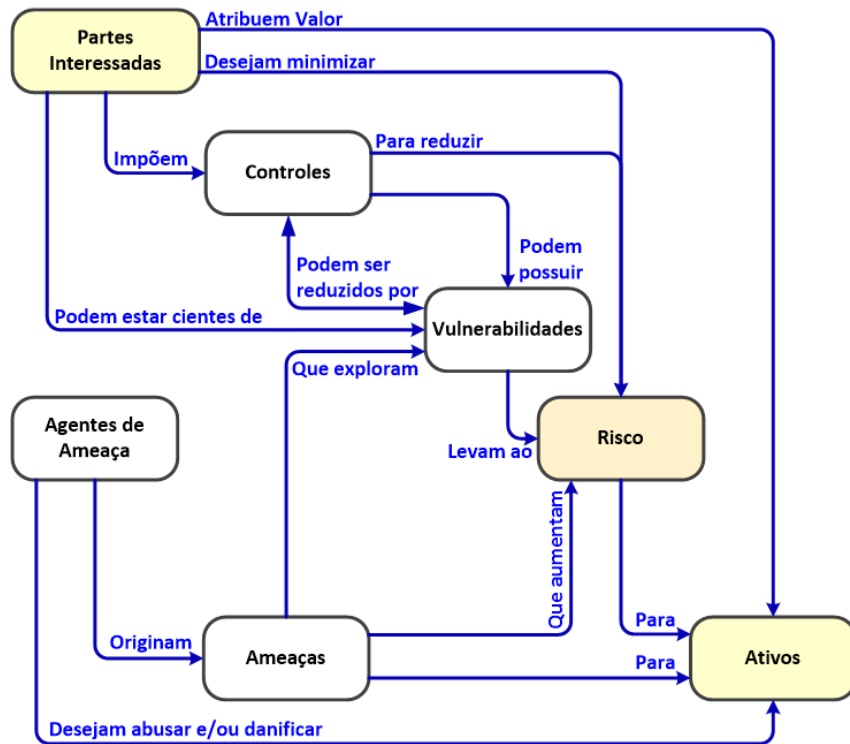


Figura 3.2: Conceitos e relações de segurança
 Fonte: Norma ABNT NBR ISO/IEC 27032:2015 [38]

A segurança cibernética e suas derivadas dependem de uma correta estruturação de: (ABNT NBR ISO/IEC 27032:2015).

- Funções;
- Políticas;
- Métodos;
- Controles técnicos.

Portanto, em relação à norma avaliada [38], há uma análise da atividade de segurança cibernética e estabelecimento do escopo como uma visão de segurança da informação, segurança de redes, segurança da Internet e proteção da infraestrutura crítica de informação (ICI), além de limitar-se ao que ocorre no Espaço Cibernético (EC). A norma

exime-se dos cuidados específicos com este Espaço, com os crimes cibernéticos (que deverão ser abordados por funções e autoridades diversas), bem como a proteção das ICI ou da Internet.

Esta limitação ao EC, incluindo os usuários finais, não se estende aos outros domínios, por mais que pareça lógico que um problema na rede interna facilite um ataque cibernético. A proteção da rede não é tratada pela segurança cibernética, pois não há interação de ameaças cibernéticas e sim um potencial de ocorrência de riscos cibernéticos, devendo a proteção das redes adotar recursos de prevenção gerais, incluindo aqueles que possam advir do espaço cibernético, mas não se limitando a estes.

A SC é atinente à proteção dos ativos contra ameaças cibernéticas, onde ameaças são categorizadas como potencial para a violação de bens protegidos. Convém que todas as categorias de ameaças sejam consideradas, mas no domínio da segurança, maior atenção é dada a ameaças que estão relacionadas com más intenções ou outras atividades humanas no Espaço Cibernético ou originadas nele.

A norma ABNT NBR ISO/IEC 27032:2015 [38] estabelece que as partes interessadas no Espaço Cibernético têm que desempenhar um papel ativo, além de valorar e proteger seus próprios bens, para prevalecer a utilidade do EC. A Figura 3.2 ilustra estes conceitos e relações de alto nível.

Agentes de ameaça reais ou presumidos também podem valorar os ativos e buscar violar os ativos de forma contrária aos interesses legítimos. Haverá percepção destas ameaças como potenciais para a deterioração dos ativos, de forma que o valor dos ativos pode ser reduzido. A deterioração específica da segurança geralmente inclui, mas não está limitada à divulgação prejudicial do ativo para destinatários não autorizados (perda de confidencialidade), danos no ativo por meio da modificação não autorizada (perda de integridade) ou privação de acesso não autorizada ao ativo (perda de disponibilidade).

As partes interessadas estimam os riscos tendo em conta as ameaças que se aplicam a seus ativos. Esta análise pode auxiliar na seleção de controles contra os riscos e reduzi-los a um nível aceitável. Estes controles são impostos para reduzir as vulnerabilidades ou impactos e para atender aos requisitos de segurança (direta ou indiretamente, fornecendo direção a outras partes).

Vulnerabilidades residuais podem permanecer após a imposição de controles. Essas vulnerabilidades podem ser exploradas por agentes de ameaça que representam um nível residual de risco para os ativos, devendo haver recursos para minimizar esse risco, considerando outras restrições.

É necessário que as partes interessadas estejam confiantes de que os controles são adequados para combater as ameaças aos ativos antes de permitirem a exposição de ativos às ameaças especificadas, pois podem não possuir a capacidade para julgar todos

os aspectos e podem, portanto, procurar uma avaliação dos controles usando organizações externas. Para o correto estabelecimento de controles deve haver atenção na diagramação de diretrizes, normas e procedimentos com a finalidade de monitoramento, orientação, gestão dos riscos e da maturidade pessoal e organizacional acerca dos perigos que podem advir do EC [38].

Para uma correta compreensão da abrangência das seguranças, se faz necessário compreender as diferenças entre estas e seus procedimentos de proteção, seja em ambiente de paz, seja em ambiente de conflito entre nações, como será demonstrado pelo próximo tópico.

3.2.1 Defesa e Guerra cibernéticas para o contexto do Governo Brasileiro.

A norma ABNT NBR ISO/IEC 27032:2015 [38] estabelece para a Segurança Cibernética a definição de preservação da confidencialidade, integridade e disponibilidade no Espaço Cibernético, o que não contrasta mas possui diferenças visíveis para as organizações governamentais, cujo foco é a proteção de um ativo mais precioso, a nação e seu conjunto de indivíduos, instituições, espaço físico e cibernético. Logo, a definição constante na Doutrina Militar de Defesa Cibernética [7] é a de assegurar a existência e a continuidade da sociedade da informação de uma nação, com a garantia e a proteção do EC e de seu acervo de informação e de suas infraestruturas críticas. Dentro do escopo definido inicialmente da segurança da nação, surge o conceito de segurança da informação e de suas derivadas, culminando no foco da SC, demonstrado na Figura 3.1, e a partir deste entendimento surgem as necessidades de ação para a consecução dos objetivos de proteção do EC. Segundo a Doutrina Militar de Defesa Cibernética [7], a Defesa Cibernética compreende o conjunto de ações ofensivas, defensivas e exploratórias realizadas no EC, em um contexto estratégico nacional, coordenado pelo Ministério da Defesa e executado pelas suas organizações subordinadas segundo seus níveis de decisão atribuídos, a fim de proteger os sistemas de informações de interesse, bem como obter dados para uso em ações de inteligência para comprometer possíveis sistemas de informações de oponentes, dentro da estratégia de quem detém a informação pode deter o poder.

Alinhado à Doutrina Militar de Defesa Cibernética está o Manual de Campanha sobre Guerra Cibernética [39], cuja finalidade é guiar os procedimentos da Defesa Cibernética quando seus efeitos táticos não são suficientes, gerando um conflito cibernético, com analogias possíveis no ambiente físico ao de uma guerra convencional, porém sem o uso de armas de fogo. Uma guerra cibernética pode acontecer e suas finalidades, além do confronto de objetivos estratégicos e políticos, são bem diferentes, fazendo uso de sistemas

de comando e controle (C2) cibernéticos, cujos operadores são, exclusivamente as forças armadas singulares do Brasil (Marinha, Exército e Força Aérea). O objetivo é proteger o acervo cibernético do país usando dispositivos de Tecnologia da Informação e Comunicação (TIC) com capacidade de C2 para explorar, corromper, degradar ou destruir sistemas análogos do adversário ou inimigo.

As características de uma guerra cibernética são[39]: nenhum sistema computacional é totalmente seguro; alcance global; não limitação de ação por fronteiras geográficas; mutabilidade de técnicas e tecnologias; incerteza sobre as ações executadas; dualidade de ferramentas, que podem ser usadas tanto para ataque quanto para defesa; ser uma função de apoio, por não ser um fim em si mesma, podendo ser auxiliar de ações militares do mundo físico; e assimetria de forças, onde um pequeno grupo de pessoas bem treinadas pode causar danos catastróficos aos objetivos do adversário, incluindo destruição de objetivos no mundo físico, caso haja conexão de equipamentos destes ao EC.

Toda e qualquer ação de avaliação ou de proteção de ativos importantes passa por uma correta gestão dos riscos envolvidos e na SC isto se traduz na gestão de riscos gerais, cujas ameaças podem vir de diversas fontes e nos riscos cibernéticos, cuja origem é a de ameaças advindas de EC. Os próximos tópicos tratarão destes conceitos complementares.

3.3 Gestão de Riscos (GR)

A definição de risco é indicada pela norma ABNT NBR ISO/IEC 31000:2018 [40], como sendo o efeito da incerteza nos objetivos. É um conceito, por vezes, muito abrangente e pouco intuitivo. Segundo Aven [41], o conceito de risco possui duas características principais: valores (ou consequências) e incertezas, e para medi-lo usa-se uma combinação de probabilidade de ocorrência e magnitude ou severidade das consequências.

Portanto, a noção de risco é estabelecida como a relação da probabilidade de ocorrência de uma ameaça explorar uma vulnerabilidade de um ativo (em sua asserção mais abrangente) e causar um impacto negativo a este. Cabe ressaltar que as variáveis ativo, ameaça, vulnerabilidade, probabilidade, impacto e risco possuem uma estreita relação entre si. Segundo REFSDAL e STØLEN [42] as três primeiras permitem compreender o ativo, pelo valor monetário intrínseco (que denota o valor de reposição básico do ativo), e seu valor, por vezes intangível e incalculável, para os objetivos do negócio, denominado criticidade do ativo. Esta observação das necessidades de proteção, permite estimar a probabilidade da ocorrência da exploração, e assim compreender o nível de comprometimento do ativo, calculando-se assim o impacto. O risco é, na verdade, uma análise das interações das probabilidades de ocorrência com os impactos, sendo diretamente proporcionais ao nível de risco imposto ao ativo. A Figura 3.3 ilustra esta relação, denominada

como triângulo do risco em analogia ao conhecido triângulo do fogo, onde segundo Flores et al. [43] se uma das partes for reduzida ou omitida, não há possibilidade de fogo. Para a gestão de riscos, segundo REFSDAL e STØLEN [42] se a vulnerabilidade ou a ameaça forem reduzidas, a probabilidade de ocorrência e/ou o impacto decorrentes também o serão.

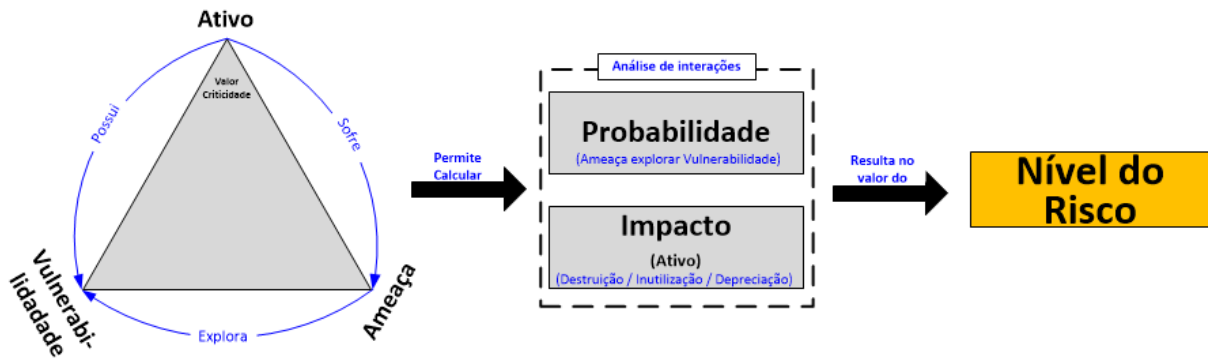


Figura 3.3: Triângulo do Risco

Fonte: Adaptado de REFSDAL e STØLEN [42]

A norma ABNT NBR ISO/IEC 27002 [37] em sua primeira edição, de 2005, previa um capítulo sobre gestão dos riscos, porém, com a criação da norma ABNT NBR ISO/IEC 27005 [3], que especificou os processos de gestão dos riscos em segurança da informação, desobrigou a ISO 27002 do tratamento do assunto. Em sua edição de 2013, a ISO 27002 já não conta com esta previsão de tema.

A norma ABNT NBR ISO/IEC 27005 [3] foi criada em 2008 e sofreu atualizações em 2011 e 2019, tendo sempre seu foco em gestão de riscos (GR) em segurança da informação (SI), de uma forma genérica, com foco nos ativos, sem previsão de gestão de riscos na área cibernética. Possui 12 capítulos, sendo os de 1 a 4 de organização e informação sobre a norma e os demais, de 5 a 12 compondo o processo de gestão de riscos em si. Há ainda 6 anexos, de A a F para composição e explicação de assuntos ligados à gestão dos riscos.

A sequência de abordagem a partir do capítulo 5 segue o roteiro: contextualização da GR, visão geral do processo de GR em SI, definição do contexto de riscos, processo de avaliação dos riscos de SI, tratamento dos riscos, aceitação dos riscos, comunicação e consulta, e monitoramento e análise crítica dos riscos. O Anexo A compõe um informativo sobre o escopo e limites do processo de GRSI; o Anexo B informa sobre a correta identificação e valoração dos ativos e a consequente avaliação dos impactos a estes; os Anexos C e D divulgam, respectivamente, listas de possíveis ameaças e vulnerabilidades;

o Anexo E sugere as abordagens para o processo de avaliação dos riscos; e, finalmente, o anexo F descreve restrições para modificação do risco.

A Figura 3.4 exibe o diagrama com o processo de gestão de riscos de acordo com a norma ABNT NBR ISO/IEC 27005:2019.

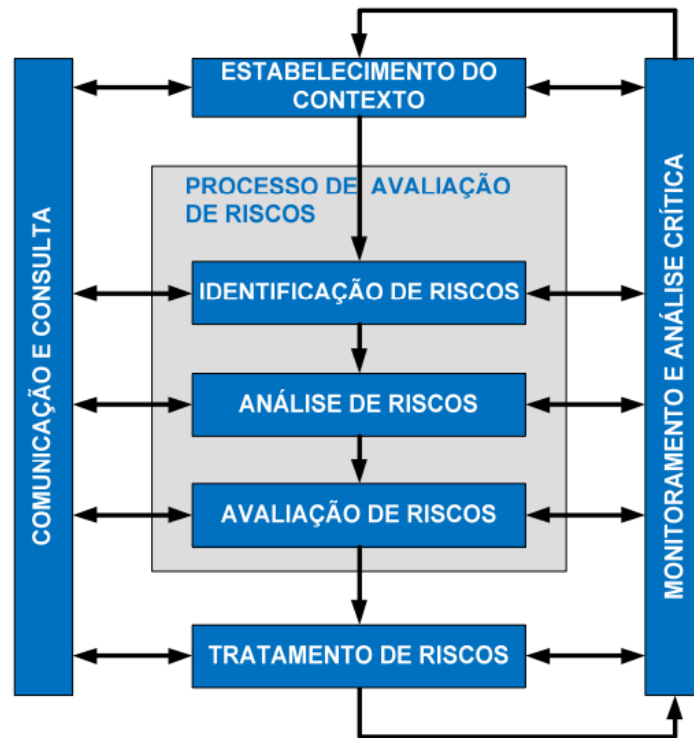


Figura 3.4: O processo de gestão de riscos

Fonte: Norma ABNT NBR ISO/IEC 27005:2019 [3]

Em 2009 foi criada uma nova norma para tratar gestão de riscos de forma genérica, para tratar riscos de todo tipo, para empresas e para a sociedade em geral, a ABNT NBR ISO/IEC 31000, a qual sofreu uma atualização no ano de 2018, sendo a versão mais atual. É acompanhada por mais duas normas que lhe são complementares, a ABNT NBR ISO/TR 31004:2015, como um guia para implementação da ISO 31000 e a ABNT NBR ISO/IEC 31010:2012 que oferece técnicas para o processo de avaliação de riscos de acordo com a atividade operacional cujos riscos serão avaliados.

A norma ABNT NBR ISO/IEC 31000:2018 [40] possui 6 capítulos, sendo os de 1 a 3 referentes à estrutura da norma e definições, e os demais compondo a estrutura de gestão de riscos. O Capítulo 4 trata dos princípios da GR; o capítulo 5 demonstra a estrutura da GR; e, finalmente no capítulo 6 trata-se o processo de GR.

Para esta pesquisa as duas normas possuem lugar de destaque em virtude de a ISO 31000 possuir uma explicação mais detalhada acerca do estabelecimento do contexto de

risco, oferecendo uma qualificação melhor sobre a organização, bem como sua norma auxiliar ISO 31010 oferecer auxílio em técnicas de avaliação dos riscos. A norma ISO 27005 foi utilizada por oferecer uma compreensão mais detalhada sobre o restante do processo e por seus detalhados anexos, permitindo a criação dos diagramas de processo para a gestão dos riscos, os quais serão detalhados no capítulo 5, item 5.4.

As atividades de gestão de riscos (geral e cibernética) podem ser mapeadas para os tópicos da norma ABNT NBR ISO 27005:2019:

- Identificação dos riscos
 - Definições do modelo de negócios, objetivos organizacionais e ativos como determinantes da relevância da Tecnologia da Informação e Comunicações(TIC) nos negócios:
 - * Item 7 – Definição do contexto
 - * Item 8.2.2 – Identificação dos ativos
 - Identificação dos riscos usando uma abordagem top/down
 - * Item 8.2.4 - Identificação dos controles existentes
 - * Item 8.2.5 - Identificação das vulnerabilidades
- Avaliação dos riscos e valoração
 - Quantificação dos riscos de forma qualitativa ou quantitativa:
 - * Item 8.3.4 - Determinação do nível de risco
 - * Item 8.4 - Avaliação de riscos
 - Agregação dos riscos, por meio de um gerenciamento de riscos amplo, pela relação de interdependência entre riscos, e assim determinar riscos relevantes:
 - * Item 8.4 - Avaliação de riscos
- Resposta/Tratamento dos riscos
 - Decisões sobre:
 - * Evitar o risco. Item 9.4 – Ação de evitar o risco
 - * Mitigar ou reduzir o risco. Item 9.2 – Modificação do risco
 - * Transferir ou compartilhar o risco. Item 9.5 – Compartilhamento do risco
 - * Aceitar ou Reter o risco. Item 9.3 – Retenção do risco

Estas relações podem ser referenciadas visualmente pela Figura 3.5.

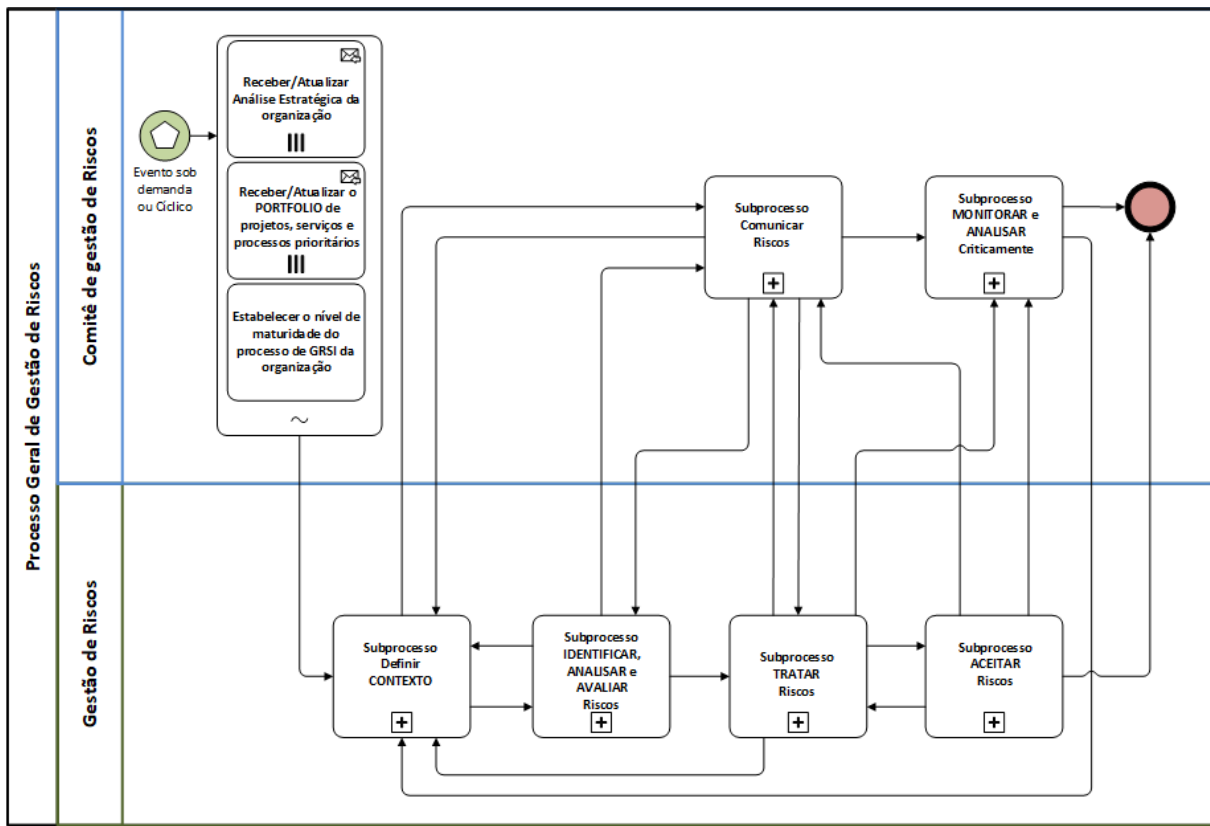


Figura 3.5: Diagrama de processos da gestão de riscos pela ISO 27005:2019

Fonte: Adaptado da Norma ABNT NBR ISO/IEC 27005:2019 [3]

A figura 3.5 representa o processo de gestão de riscos em segurança da informação, de acordo com a norma ABNT NBR ISO/IEC 27005:2019 [3]. Seu processo é composto por uma sequência de atividades e subprocessos, iniciando-se pela identificação dos dados da análise estratégica da organização em análise como subsídio para a primeira fase da gestão de riscos composta pelo processo de definição do contexto, que, de acordo com a norma ABNT NBR ISO/IEC 31000:2018 [40] o contexto¹ de uma organização compreende os fatores internos e externos que podem interferir de forma direta ou indireta na identificação, análise ou avaliação dos riscos, em função do tipo de negócio desta organização. Após a identificação do contexto há o processo de identificação, análise e avaliação dos riscos

¹A norma ABNT NBR ISO/IEC 31000:2018 foi utilizada por pormenorizar melhor esta fase, pois tanto a ABNT NBR ISO/IEC 27005:2019 quanto a ABNT NBR ISO/IEC 31000:2018 tratam de gestão de riscos, a primeira sobre segurança da informação e a segunda desenvolvida para riscos gerais. Possuem a mesma visão do gerenciamento dos riscos, mas cada uma tem seus textos com maior ou menor nível de explicação em alguns processos.

ABNT NBR ISO/IEC 27005:2019 [3] onde serão listados os fatores de risco, analisadas suas interações com o negócio e por fim organizados por nível de risco, antes da fase de tratamento, quando serão adicionados controles para a redução dos níveis dos riscos até o limite do apetite de risco (limite de aceitação) da organização. Esta sequência segue para a aceitação formal dos riscos, pois podem haver riscos residuais e riscos inaceitáveis, em ação dependente dos tomadores de decisão formais da organização, segundo a ABNT NBR ISO/IEC 27005:2019 [3] item 10. Durante todo o processo há a interação dos processos de comunicação dos riscos (transparência) e de monitoramento e análise crítica dos riscos (realimentação do sistema) para a contínua melhoria do processo de gestão. Ainda segundo a ABNT NBR ISO/IEC 27005:2019 [3] a gestão dos riscos deve alinhar-se continuamente com os objetivos do negócio, e para tal a última fase listada é de grande importância pois remete ao final de um ciclo de gestão com realimentação dos dados analisados e com a análise crítica de possíveis mudanças ocorridas, tanto nos objetivos, quanto nos cenários possíveis de riscos, internos ou externos. Como visto, o processo não se encerra definitivamente, mas define ciclos e estabelece controles.

Estas atividades foram limitadas àquelas que compõem a lista de gerenciamento de riscos (gerais) e também de riscos cibernéticos. Há diferenças sutis nos tipos ou naturezas dos riscos, bem como na abordagem da avaliação destes. Conhecer este assunto permite lançar um olhar mais especializado ao tema, portanto deve ser corretamente explicado, e compõe o objetivo do tópico a seguir.

3.3.1 Gestão de Riscos Cibernéticos (GRCiber)

O risco cibernético, segundo REFSDAL e STØLEN [42] é o risco causado por uma ameaça cibernética, estando também definido pela Doutrina Militar de Defesa Cibernética [7] como sendo a probabilidade de ocorrência de um incidente cibernético associado à magnitude do dano por ele provocado.

Há diferença básica de abordagem entre o que preconizam as normas ABNT NBR ISO/IEC 27005:2019 [3] e ABNT NBR ISO/IEC 31000:2018 [40] na gestão de riscos a ativos, aqui denominada de Gestão de Riscos gerais (GR), com foco na análise do ativo, em busca das variáveis do risco, submetendo-as ao processo de identificação, análise, avaliação, tratamento, aceitação, comunicação e monitoramento do risco. Enquanto, a abordagem para o risco cibernético, denominada de Gestão de Riscos Cibernéticos (GRCiber), em função da sutilidade, furtividade, baixa previsibilidade, assimetria de forças em relação aos atores dificulta o estabelecimento de probabilidades de ocorrência, exigindo uma estratégia de definição de cenários pré-formatados para inquirição dos componentes das ocorrências de risco para estabelecer valores quantitativos e padronizados a partir de análises qualitativas.

O primeiro passo na abordagem GRCiber é similar a qualquer avaliação, ou seja, deve-se buscar a identificação do contexto da análise, com a identificação dos aspectos funcionais, técnicos, legais e administrativos da organização analisada, para que haja a correta identificação e valoração dos processos e ativos críticos. Um segundo passo é a identificação do tipo de risco a ser analisado, que pode ter causas maliciosas e não maliciosas, que representam alguma intenção no estabelecimento do risco.

A Figura 3.6 ilustra este processo:

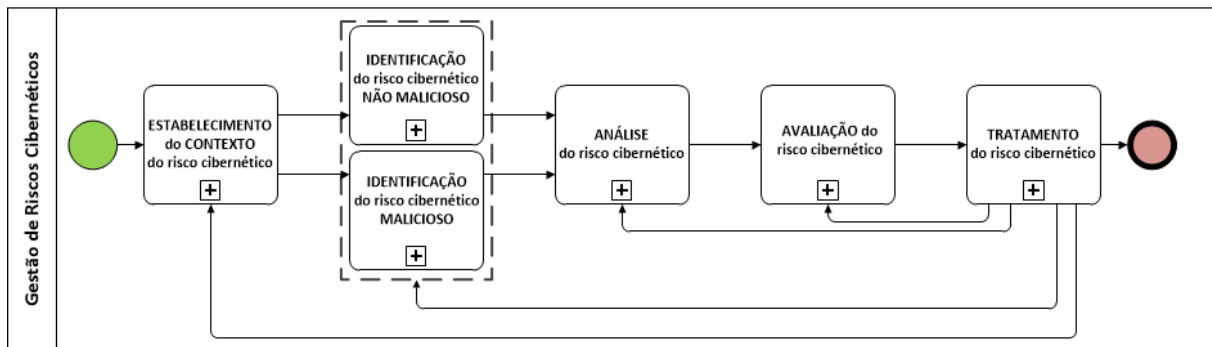


Figura 3.6: Processo de avaliação de risco cibernético

Fonte: Adaptado de REFSDAL e STØLEN [42]

Segundo REFSDAL e STØLEN [42] há dois aspectos que podem ajudar a distinguir os dois tipos de análise de riscos, a análise de riscos cibernéticos e a de riscos em geral. A primeira diz respeito ao ser humano e sua interação com as ameaças, havendo as variáveis de intenção e de motivo, sendo de difícil estimação das probabilidades de ocorrência para os riscos cibernéticos. Um segundo aspecto envolve características dos sistemas cibernéticos em relação a comumente disponibilizarem coleta de logs de uso, monitoramento constante e testagem, facilitando as análises de risco sob a forma de possibilidade de avaliação dos fatos já ocorridos ou de alguma tendência de ataque pelos indícios de tentativas ou de ocorrências de atividades de baixo impacto e visibilidade como escaneamentos ou logins com falhas.

Esta diferenciação modifica a fase de identificação do risco e de sua consequente análise, pois para um risco em que há intenção ou malícia na ocorrência, a busca inicial se dá a partir da busca a fonte da ameaça, para a correta resposta à situação. Para um risco não malicioso, torna-se contraproducente buscar o foco da ameaça, e a meta inicial passa a ser a identificação do próprio incidente em si. A Figura 3.7 oferece entendimento sobre esta sequência.

Em referência às análises de ameaças maliciosas, devido à dificuldade de estimação das probabilidades de ocorrência, REFSDAL e STØLEN explicam que podem ser utilizadas modelagens para descrever características ou requisitos necessários para ultrapassar as barreiras de segurança dos ativos, como nível de habilidades necessárias, recursos, nível de motivação, oportunidade entre outros.

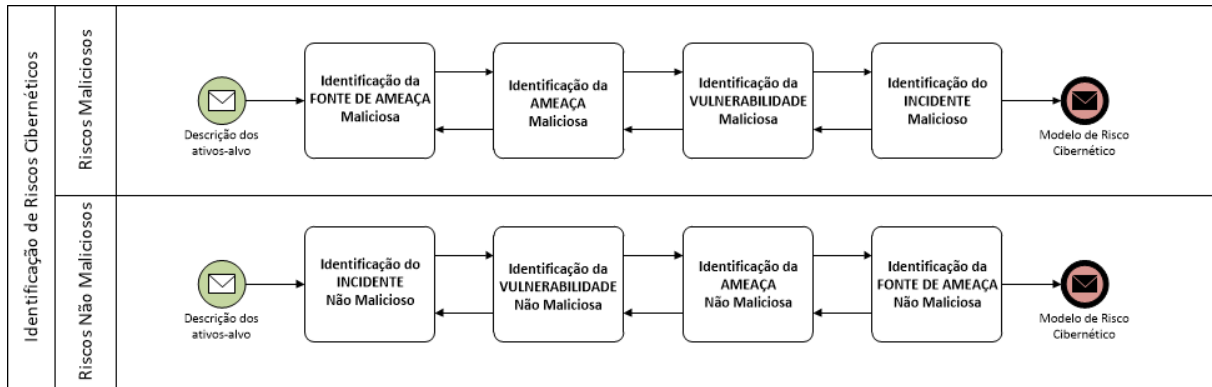


Figura 3.7: Avaliação de risco cibernético malicioso e não malicioso.

Fonte: Adaptado de REFSDAL e STØLEN [42]

Como próximo passo configura-se a sequência de análise e avaliação do risco, para que haja uma quantificação do mesmo e qualificação dos seus impactos já ocorridos ou potenciais, preparando os cenários de resposta e tratamento.

A partir deste ponto, as abordagens de gestão de risco geral e cibernético voltam a sofrer uma aproximação, quando se chega à fase de tratamento, que em GRCiber se foca na proteção ou defesa cibernética, com ações pontuais e normalmente instantâneas de correção proativa ou ligeiramente reativa do risco. Esta abordagem aproxima-se das ações que as equipes de respostas a incidentes de rede devem tomar, ou seja, a resposta aos incidentes cibernéticos possui similaridade com o tratamento de incidentes de redes e recebem tratamento inicial dos centros ou equipes de tratamento e resposta de incidentes de rede (CTIR / ETIR).

Após compreender como se processam as abordagens de gestão de risco, torna-se mais interessante conhecer o processo de gestão de riscos dentro de um contexto de aquisição de consciência situacional cibernética, onde este processo será acrescido de outros para o estabelecimento de visão ampliada dos riscos, como será demonstrado no próximo tópico.

3.4 Processo de Aquisição de Consciência Situacional Cibernética (CSC)

Aquisição de consciência situacional cibernética (CSC) é um complexo e multidisciplinar conjunto de processos que visa determinar de forma proativa o que ocorre com um sistema informacional baseado em computação e em rede para determinar o nível de segurança e os riscos potenciais e/ou já realizados e assim compreender todos os aspectos a serem protegidos.

3.4.1 Compreensão da importância dos processos de CSC

Para o entendimento da relevância do espaço cibernético de interesse e de seus ativos, se faz necessário compreender alguns cenários de ataques no passado para que sirvam de modelo para a criação dos cenários para a organização em estudo e como isto afeta a visibilidade e o convencimento da organização por parte dos órgãos governamentais na escala hierárquica e funcional nas quais está inserido o NuCDCAer e seus processos.

Já foi estudado o ataque de 11 de setembro de 2001 [44], em Nova Iorque, Estados Unidos, quando houve uma coordenação de ações e de informações, mas que se mostraram ações de combate físicos, convencionais, com respostas igualmente físicas. Observou-se que ocorreram falhas de vigilância para a prevenção, e de procedimentos nas atividades de transporte, para as quais havia um histórico de confiança na boa-fé dos passageiros. Este episódio serviu de alerta e de mudança de postura em relação ao crescente cenário de uso de plataformas digitais de comunicação de processos, para os quais, em relação ao Brasil, a Doutrina Militar de Defesa Cibernética [7] alerta para as características dos ataques e da guerra cibernética, que são a assimetria de forças e a furtividade das ações, além de outros menos relacionados neste momento. Para exemplificar, serão utilizados dois eventos em países que sofreram ataques virtuais, para os quais houve grande impacto às operações normais dos cidadãos e dos governos, e igualmente respostas que influenciaram o convencimento das autoridades e a criação de políticas e de financiamento de ações de proteção cibernética.

Segundo Jackson [45] em uma sexta-feira, em 27 de abril de 2007, na Estônia, foi detectado que um grande número de agentes governamentais perderam seus acessos ao correio eletrônico e igualmente aos seus dispositivos de rede. Isto foi somente a ponta de um enorme iceberg que iniciou com a separação da Estônia da antiga URSS em 1990, e da insatisfação de alguns cidadãos e do governo acerca de símbolos soviéticos expostos nas cidades estonianas. Este fato levou à demolição de um monumento, o que provocou discussões e tumultos, inclusive mortais. O resultado foi o ataque por hackers à

infraestrutura de TI da Estônia, como protesto, e indicado pelo governo estoniano como possivelmente uma represália russa ao suposto desrespeito [45], fatos que permaneceram em aberto após a investigação, contribuindo para a confirmação das características de furtividade e dissimulação observadas na Doutrina Militar de Defesa Cibernética.

A análise deste ataque levou, por parte da Estônia, a estabelecer novas estratégias, táticas e parcerias do país com aliados para reaver o controle de seu ambiente cibernético e de aumentar a resiliência a eventos do tipo, revelando a importância da estruturação de políticas de segurança e defesa cibernéticas focadas em padrões consagrados multilateralmente.

Como segundo exemplo, em 23 de dezembro de 2015, segundo o Electricity Information Sharing and Analysis Center (E-ISAC²) [46] e [47], uma empresa regional de eletricidade da Ucrânia sofreu interrupções no fornecimento de energia aos clientes. Detectou-se, posteriormente que havia ocorrido um ataque cibernético em grande escala, atribuído, pelo governo ucraniano, como provocado por serviços de segurança do governo russo, com o qual a Ucrânia estava envolvida em embates políticos e militares.

Portanto, negligenciar processos de CSC pode ser arriscado, caro e expor pessoas, empresas e a sociedade organizada como componente das nações a ações imprevisíveis, principalmente quando há suspeitas de patrocínio de Estados e/ou grupos organizados para estas atividades de ataques a ativos críticos. O atual conflito desencadeado em março de 2022 pela Rússia ao atacar a Ucrânia ainda não pode ser analisado sob todos os seus aspectos teóricos e práticos, mas sugere que os pequenos conflitos de interesses e incidentes anteriores podem ter sido o estopim ou o indicativo que algo mais grave estava por vir.

O estudo sobre Consciência Situacional Cibernética e seus processos revela sua importância por dois fatores: o primeiro diz respeito à necessidade de constante vigilância cibernética, ou seja, o estabelecimento de uma política de aquisição de consciência situacional cibernética eficaz e factível; e em segundo lugar, o estabelecimento de parcerias de compartilhamento de informações de segurança cibernética e de inteligência de ameaças, conforme já descrito neste trabalho, para que não ocorram episódios de ataques cibernéticos de grande monta, ou para que haja resposta tempestiva e oportuna, visando a redução de impactos destes ataques.

Lima e Silva [48] demonstram as implicações internacionais que podem ocorrer em virtude de ataques cibernéticos e a violação de tratados e leis internacionais, o que pode ser observado e estudado pela iniciativa da Organização do Tratado do Atlântico Norte – OTAN (NATO em inglês), por meio do The NATO Cooperative Cyber Defense Centre of

²O E-ISAC é uma organização dos EUA, criada em 1999, cuja missão é a de reduzir o risco de ataques cibernéticos para a indústria do setor elétrico americano

Excellence (CCDCOE) [49], o qual desenvolveu uma ferramenta web, a Cyber Law Toolkit [50], cuja finalidade é fornecer subsídios aos profissionais do direito ou interessados que trabalham na interseção entre a lei internacional e as operações cibernéticas. A ferramenta é composta por 24 cenários hipotéticos com incidentes fictícios inspirados em casos reais para análise dos cenários.

Esta iniciativa demonstra a importância e a relevância do estudo das consequências dos riscos cibernéticos e suas implicações que podem ir muito além do observável diretamente (sem aprofundamento técnico e legal), o que pode aumentar o grau de impacto de ações por vezes aparentemente inocentes.

Para uma melhor interpretação dos processos de CSC, se faz necessário aprofundar um pouco mais análise, sob a ótica de uma autora que vem sendo citada em diversos trabalhos sobre consciência situacional em geral, com derivações em consciência situacional cibernética, tema do próximo tópico.

3.4.2 Análise dos processos de CSC

O estudo dos processos de CSC pode permitir um aumento de conhecimento e maturidade das instituições sobre o espaço cibernético, o qual pode representar virtualmente potenciais de ameaças que podem fugir do espectro cibernético e desencadear em ações cinéticas, com ataques físicos à soberania destas instituições.

Segundo Endsley (1995, p. 6) [2]:

“Consciência situacional é a percepção dos elementos do ambiente com um volume de tempo e espaço, a compreensão de seu significado, e a projeção do seu status em um futuro próximo”.

Endsley [2] ainda faz uma distinção entre dois conceitos muito próximos, o de consciência situacional propriamente dita, que corresponde a um “estado de conhecimento”, ou seja, uma compreensão dos sinais e acontecimentos e o outro conceito é o de avaliação situacional, que compreende os processos de obtenção, aquisição ou manutenção desta mesma consciência situacional, sendo de grande importância em virtude de se compreender que o citado “estado de conhecimento” estaria no domínio de mentes humanas (domínio cognitivo), pois a avaliação situacional pode significar um processo ou conjunto de processos capaz de se autossuportar baseado em técnicas automatizadas.

Aprofundando-se no conceito de consciência situacional [2] sugere-se uma subdivisão da CSC em 3 níveis: o de percepção, compreensão e projeção. Estes níveis podem denotar um progressivo incremento nos níveis de consciência, sendo o primeiro, a percepção básica de dados importantes, como a origem dos dados, os dados em si e de que forma estes dados podem integrar a realidade captada e como se pode agrupá-los para estabelecer

as classificações necessárias para endereçar aos processos corretos de análise. Neste caso do Projeto de Integração em Defesa Cibernética das Forças Armadas (Projeto IFA ³), compreenderá os macroprocessos de Gestão de Incidentes de rede, Gestão de Riscos Cibernéticos e Inteligência de Ameaças, com o objetivo de extrair destes dados o significado padronizado de ameaça cibernética. A Figura 3.8 representa a visão de outros autores, Tadda e Salerno [13], baseados na mesma teoria de Endsley, porém com foco em segurança cibernética, precisamente sobre os níveis de CSC.

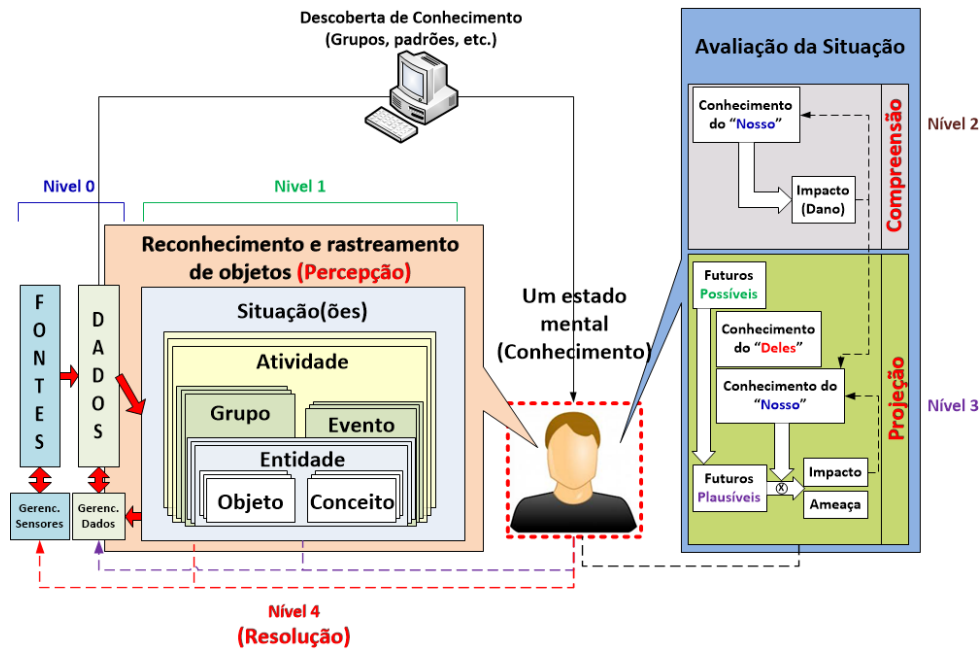


Figura 3.8: Processo de Aquisição de Consciência Situacional Cibernética
Fonte: Adaptado de Tadda e Salerno [13]

Para um melhor entendimento, será feita uma análise desta nova visão da teoria de Endsley, sob a ótica de Tadda e Salerno [13], para a qual é feita uma subdivisão do primeiro nível criando-se adicionalmente um nível 0 representando o processo de obtenção de dados brutos, com a preocupação sobre a origem (fontes) destes dados e como são adquiridos (sensores), bem como do gerenciamento da coleta e dos dados obtidos em si, que no Projeto IFA compreende o processo de filtragem e seleção dos dados em termos de fluxos para o endereçamento aos macroprocessos de análise. Há um acréscimo sobre a teoria de Endsley para um nível além do último (de Projeção), o de Resolução (nível 4) que diz respeito ao que fazer com as informações obtidas e analisadas. O entendimento da CSC

³O Projeto IFA representa a materialização do esforço do NuCDCAer em participar do desenvolvimento conjunto dos processos de gestão de riscos e de consciência situacional cibernéticos para a defesa cibernética nacional.

para o ambiente cibernético ganha novos contornos sob esta teoria e se faz interessante estudá-la por completo.

Segundo Tadda e Salerno [13], o nível 0 faz parte da fase de percepção, mas não encerra o processo completo de interpretação da realidade. Vale ressaltar que esta subdivisão aumentou para 5 os níveis sugeridos por Endsley. O agrupamento dos dados obtidos no nível 0 alimenta o nível 1 (Percepção) [13], que efetivamente fará a padronização e classificação preliminar destes dados, representados por situações no diagrama, podendo sofrer uma organização em atividades, grupos, eventos, entidades, objetos e conceitos, promovendo efetivamente a percepção da situação, compondo um estado mental (o conhecimento), obtido antes de se prosseguir com as análises.

Neste nível 0 (Percepção), para [13], é indispensável para uma correta informação (a criação de uma figura ou fotografia da situação) sobre o ambiente a ser estudado. Este nível é evidenciado de forma mais detalhada na Figura 3.9, que demonstra uma observação do processo de uma forma mais empírica, analisando as atividades sob uma ótica temporal, ou seja, como se o processo estivesse ocorrendo no momento da observação e não somente de forma teórica. Parte-se dos “Elementos Observáveis” e segue-se até às possíveis ameaças detectadas [13]. Os elementos observáveis são avaliados pelo crivo das metas e políticas, de forma a se obter o que os tomadores de decisão podem estar interessados, de uma maneira mais direta, primeiramente levando ao conhecimento (bases de dados) do “nosso” (composta além da análise do estado presente das atividades, aliadas às vulnerabilidades detectadas no processo de análise), porém não descuidando da observação daquilo que possíveis oponentes ou competidores possam fazer ou querer, compondo outra base de dados, a do conhecimento do “deles” (capacidades e intenções a um dado instante presente ou passado para compor uma predição aceitável acerca do oponente ou inimigo), quando os analistas e tomadores de decisão se põem na situação do oponente, para melhor compreender os futuros possíveis, com vistas a obter os futuros plausíveis, verdadeira fonte de informação para os tomadores de decisão, em virtude de trazerem as principais ameaças envolvidas [13].

A partir do terceiro nível (nível 2) o de Compreensão, e o nível 3, de Projeção, observa-se o que se convencionou chamar de “Avaliação da Situação” na qual estuda-se a situação corrente ou inicial e suas implicações futuras, como será explicado a seguir Tadda e Salerno [13].

Tadda e Salerno [13] afirmam que se pode definir avaliação da situação como a compreensão da situação em função do que é definido na Figura 3.9 como o “Conhecimento do Nosso”, ou seja os danos diretos (impactos) que podem ser causados e a projeção da situação atual em um futuro, em termos de um futuro plausível (que realmente pode acontecer) e os potenciais impactos ou ameaças daquelas situações futuras.

Logo, no Nível 2 (Compreensão) exemplificado na Figura 3.8, há uma análise de tudo que foi obtido nos níveis 0 e 1 para a o desenvolvimento de um conhecimento acerca da situação atual. Questionamentos úteis podem ser endereçados para a correta redução das incertezas sobre os dados, segundo Tadda e Salerno [13]. Alguns requisitos podem ser alterados de forma a alterar os requisitos de coleta dos dados (sensores e conjunto resultante dos dados), via gerenciamento humano, após avaliação de viabilidade. Esta parte da atividade de avaliação da situação também pode ser denominada de Avaliação dos Danos, com a identificação de todas as atividades que possam provocar danos, em especial aquelas que necessitarão de algum planejamento de recuperação ou contingência para serem resolvidas. Estas atividades comporão o que pode ser denominado “Conhecimento do Nosso”. Representa importante conhecimento a ser usado pelos tomadores de decisões para o correto cumprimento da missão com o adequado gerenciamento dos ativos importantes.

A área militar é uma grande usuária do conceito de consciência situacional (CS), mas não possui exclusividade do uso deste conceito, útil em diversas atividades especializadas ou comuns, como na simples ação de atravessar uma rua em qualquer cidade. Mica Endsley [2] tem trabalhado com o conceito na *USAF* há muito tempo e seu artigo mais citado considera os fatores humanos como central em CS. De posse deste conhecimento há um trabalho desenvolvido para o Ministério da Defesa dos EUA (DoD) por Alberts et al. [51] que considera que a CS tem um forte domínio cognitivo, que se traduz em para o domínio físico em termos de melhor aproveitamento de recursos e eficácia operacional. Este fator coloca o ser humano como destaque e quando este desenvolve a consciência situacional no campo de batalha, esta é desenvolvida no domínio cognitivo. A interação entre diversos atores humanos, em diferentes locais no campo de batalha, auxiliados por sensores e meios de comunicação permitem que os atores recebam as mesmas informações de forma sincronizada e possam estabelecer uma colaboração com decisões compartilhadas e discutidas, com ganho para todos [51].

Alberts [51] cita ainda que a descoberta de conhecimento via sistemas informacionais dedicados, pode promover auxílio na detecção de relacionamentos ou padrões e significados para estes elementos, cujas medições e avaliações são os pontos fracos do fator cognitivo humano, auxiliando a filtrar as ocorrências significantes, gerando eficácia na CS e decisões melhores.

Por esta razão uma figura humana foi representada no centro do diagrama e suas interações foram informadas, permitindo compreender que a inteligência humana permeia todos os processos, seja na identificação, análise, validação ou retorno de resultados (feedback), segundo Tadda e Salerno [13].

Deve-se ter em mente que um sistema informatizado pode identificar uma atividade

em andamento e por meio de algum tipo de assinatura comportamental (conhecimento prévio), conectá-la a eventos ou objetos, mas não pode estabelecer, necessariamente uma consciência situacional, pois esta supõe a capacidade ou a necessidade de tomada de decisão, o que compete exclusivamente a tomadores de decisão humanos, como para Henriqson [52] em sua pesquisa sobre ambientes complexos e de risco sob decisão humana na aviação, bem como para Marques [53] cuja pesquisa focou em inteligência de imagens e o fator consciência situacional e sua dependência humana nas interpretações.

O Nível 3 (Projeção) representa a análise para uma identificação de eventos futuros, uma predição mediada por evidências coletadas e parcialmente analisadas, segundo Tadda e Salerno [13]. Inicialmente com uma percepção dos impactos atuais que permitirão a criação e o incremento do “Conhecimento do “Nosso”, ou seja, todas as informações de interesse direto e que promovem a “fotografia” do momento corrente, uma análise do significado das atividades identificadas, mas que servirão de subsídio para o estabelecimento de uma visão de futuro.

Ainda por Tadda e Salerno [13], a análise da situação corrente da fase anterior permite uma coleta de informações com a finalidade do desenvolvimento de múltiplos prognósticos de futuro, ou identificados como “Futuros Possíveis”, e para cada um destes, os analistas podem estabelecer as os eventos-chave que podem estar se desenrolando, e que poderão ser usados para ajustar os requisitos de coleta, conforme exibido na Figura 3.9, como base do estabelecimento do nível 4 (Resolução), como uma extensão aos níveis propostos por Endsley. Estas atividades exigem o concurso imprescindível do elemento humano, em virtude de os sistemas não terem a mesma performance quando se trata de julgamento de situações particulares ou de exceção em meio a fatores pouco objetivos ou de incertezas, normalmente não mensuráveis.

O Nível 4 (Resolução) procura fazer uma identificação de um caminho a seguir, de forma a mudar o status da situação corrente, se esta for de risco ou de inadequação de ações anteriormente tomadas ou mesmo a serem efetuadas. Vale ressaltar que este caminho pode não ser o de uma certeza ou de comodidade para o tomador de decisões, mas, sobretudo, o de possibilitar opções viáveis e compreender como elas podem afetar o ambiente em si [13].

Pode-se compreender, segundo Tadda e Salerno [13], que estes níveis ou caminhos a percorrer não precisam ser executados serialmente, mas o podem ser de forma paralela, pois é um processo geral contínuo em todos os níveis.

Segundo Tadda e Salerno [13], a Figura 3.9 estabelece uma visão (ou um fluxo de processos e de produtos finais) a partir de um dado momento (um tempo t), onde se encontra um conjunto de atividades, definido anteriormente como situação corrente, cuja avaliação da situação pode estabelecer significados. As atividades analisadas poderão

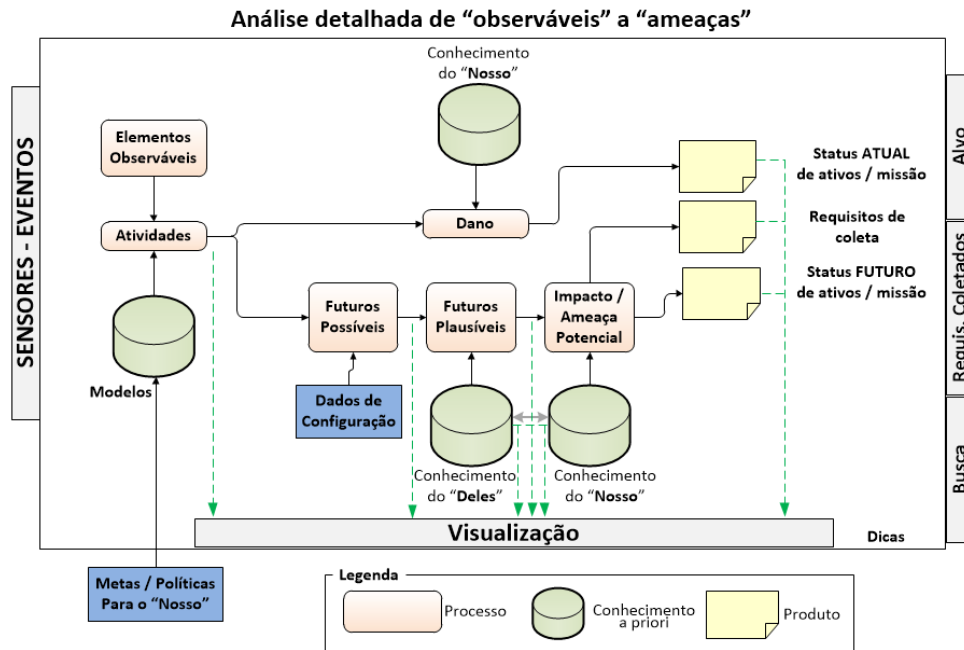


Figura 3.9: Aprofundamento do Processo de Aquisição de CSC
 Fonte: Adaptado de Tadda e Salerno [13]

oferecer dois tipos de análise: a visão do dano possível sendo obtido a partir da base de conhecimento do “Nosso” (conhecimentos a priori), ou seja, a partir dos elementos observáveis, submetidos ao crivo das metas ou políticas e modeladas pela metodologia vigente na organização, e; a visão de futuro (não observada somente pelo tempo em si, mas sob a ótica do próximo passo a dar), tanto os possíveis, obtidos a partir da análise baseada nos dados de configuração (que define o número de estágios ou passos a se observar adiante), quanto os futuros plausíveis, a partir do conhecimento do “Deles” (representado pela análise do oponente/inimigo, suas capacidades e intenções ou objetivos – Outro conhecimento a priori, ou base de conhecimento), para, a partir deste ponto estabelecer uma análise de riscos, que podem trazer à tona os impactos ou ameaças potenciais.

Estes passos, ainda analisando a consciência situacional segundo Tadda e Salerno [13], são compostos pelos 5 níveis e podem produzir 3 tipos básicos de saídas ou produtos: a visão atual da situação, compondo o alvo, ou objetivo de toda a operação de aquisição de consciência situacional; a produção preliminar ou por alteração em função de retroalimentação dos requisitos de coleta, já abordados em função da necessidade do crivo humano para a tomada de decisões bem como na correção ou alteração dos parâmetros dos dados coletados do nível 0, e; da definição de um status futuro dos ativos ou da missão da organização, como requisitos básicos para a tomada de decisões para a redução dos efeitos indesejáveis dos riscos analisados.

Trazendo os conhecimentos obtidos na análise do processo geral de CSC em si, pode-se estruturar como os requisitos de atividades de interesse podem ser mapeados para o domínio de ciberataques, ou mesmo de uma ciberguerra. Este tipo de ação se dá em forma de vários estágios e para cada um há pelo menos uma abordagem.

A utilidade do estudo sobre a consciência situacional cibernética se baseia no fato de que a atividade de análise de riscos cibernéticos necessita de uma visão holística dos riscos como a estabelecida na norma ABNT NBR ISO/IEC 27001:2013, e da compreensão sobre o espaço cibernético contido na norma ABNT NBR ISO/IEC 27032:2015. Notadamente a identificação de que se trata de um processo cognitivo dependente de processos que possam identificar, analisar e avaliar riscos cibernéticos, para os quais a noção de CSC sob as óticas de Endsley e Tadda e Salerno permitem compreender.

A importância do referencial teórico está na utilidade para o pesquisador acerca dos temas pesquisados, para que não falte conhecimento abrangente, nem objetividade das informações. Para uma compreensão de como se construiu a pesquisa, torna-se necessário observar a estrutura e a metodologia da pesquisa, bem como as etapas seguidas, conforme o capítulo a seguir.

Capítulo 4

Metodologia da Pesquisa

Neste capítulo o propósito é descrever o percurso trilhado para compor este estudo, apresentando definições sobre o tipo de pesquisa, o universo espacial, temporal, o objeto e os instrumentos para a aquisição dos dados necessários. A descrição do contexto e escopo, com as inclusões e exclusões do tema e os procedimentos para chegar ao objetivo desejado.

4.1 Classificação da pesquisa

Pesquisa, segundo Jung [54] representa o processo de aquisição de conhecimentos acerca do próprio pesquisador e do mundo em que vive, mas com a característica pragmática de responder a um questionamento, resolver um problema ou satisfazer uma necessidade.

Segundo Wazlawick [55] a Ciência da Computação como campo de pesquisa se classifica como uma ciência empírica por estudar fenômenos que acontecem no mundo real, bem como o enquadramento amplo desta junto às ciências naturais, nos aspectos mais mecânicos ou automáticos e entre as sociais por estabelecer ferramentas de apoio às atividades humanas intrínsecas. Caracteriza-se novamente na aplicação dos estudos, como ciência aplicada e nomotética, especificamente neste campo de atividade, a segurança cibernética como tema mais amplo de estudo, antes de efetuar os cortes para estabelecer o objetivo básico de estabelecer um processo de gestão de riscos cibernéticos. Os resultados, apesar de pertencerem a uma ciência exata, possuem componentes humanos que podem fugir a esta regra, mas estabelecem algum grau de repetitividade suficiente para que se generalize comportamentos e se tenha alguma segurança em previsibilidade. Uma pesquisa pode ser classificada segundo diversos aspectos, a Figura 4.1 representa visualmente esta classificação.

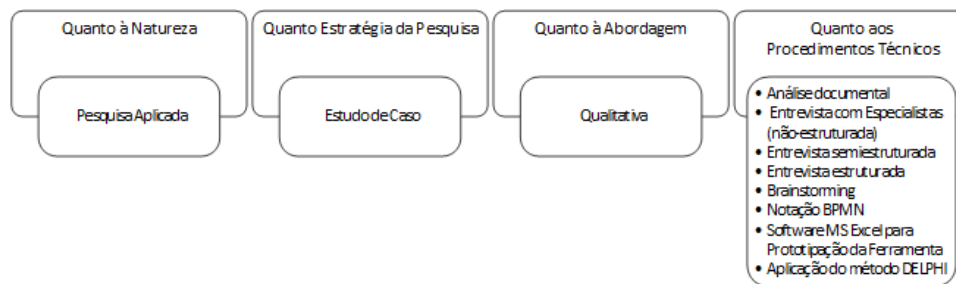


Figura 4.1: Classificação da pesquisa

Fonte: Autoria própria

A própria ideia de uma pesquisa em um programa de mestrado profissional somente se justifica em função de sua utilidade prática (pragmatismo). Neste caso representa a finalidade de estruturar um processo de avaliação de riscos cibernéticos para apoiar o macroprocesso de aquisição de consciência situacional, resultando no fornecimento de um índice que aponte um nível de risco cibernético encontrado em determinado momento para ativos de informação selecionados, segundo Wazlawick [55], representando segundo sua natureza uma pesquisa aplicada.

Usou-se para esta pesquisa uma estratégia de estudo de caso, que, segundo Azevedo e Ensslin [56] é caracterizado por um estudo amplo e profundo de um ou poucos objetos. Sua característica é a de um amplo e detalhado conhecimento. Adotado como procedimento de pesquisas exploratórias, explicando causas e descrevendo comportamentos. Para esta pesquisa, em virtude de ser um trabalho no qual o pesquisador está ativamente envolvido no processo, o estudo de caso revela-se uma ferramenta de obtenção de conhecimento de forma explícita.

Segundo Machado e Cruz [57] uma pesquisa pode ter abordagens qualitativa e quantitativa. A abordagem, nesta pesquisa, apesar de fornecer e incluir valores numéricos, não possui um caráter quantitativo, não abordando tratamento estatístico dos achados, limitando-se a estabelecer valores classificatórios para os riscos cibernéticos, indicando uma classificação de abordagem da pesquisa como qualitativa.

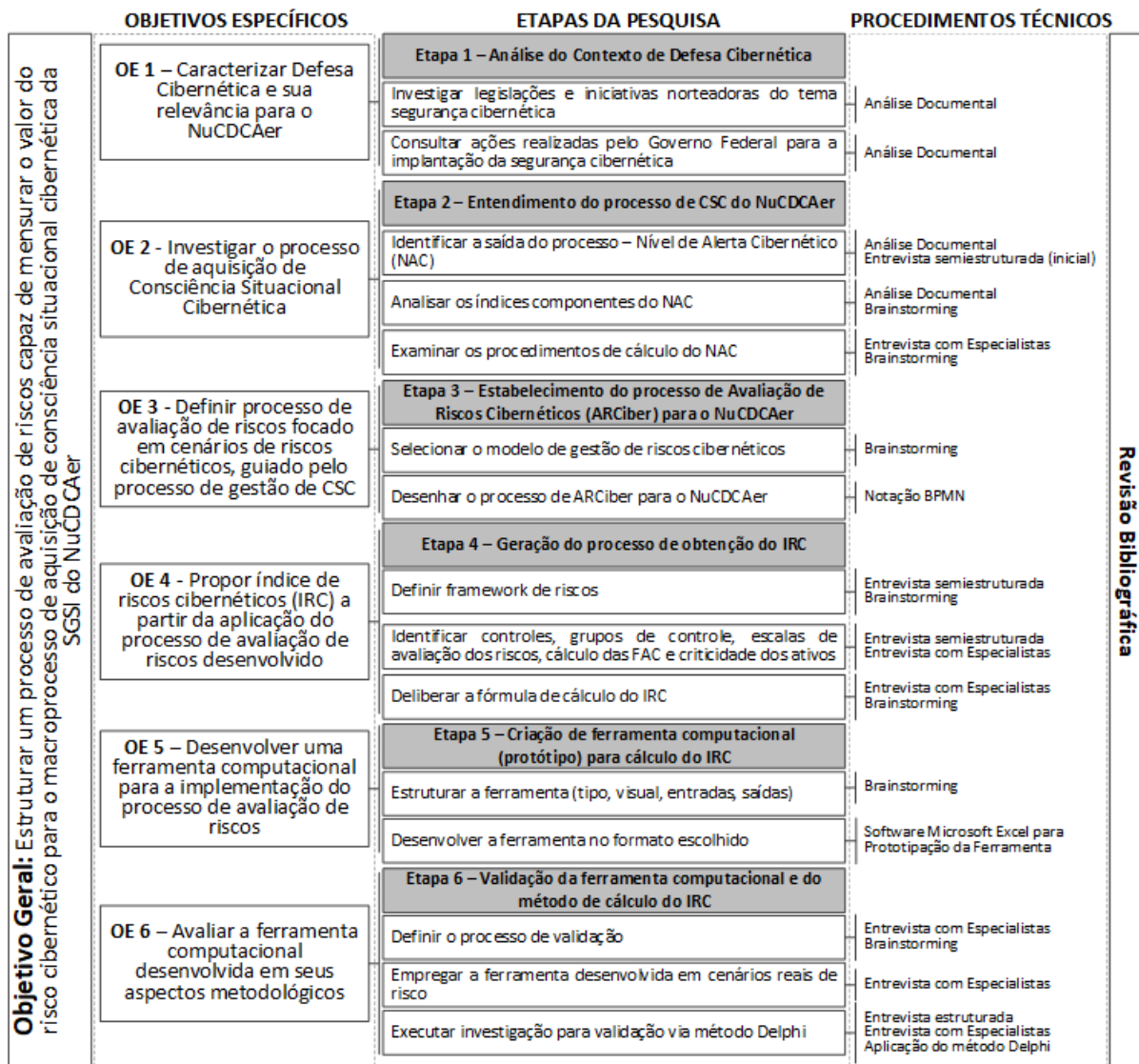
Diversos procedimentos técnicos de pesquisa foram adotados, como a Análise Documental, Reunião com Especialistas, Brainstorming, Entrevistas Semiestruturadas, Notação de Processos BPMN, mas outros ainda serão executados, como Entrevista Estruturada, Software Microsoft Excel para prototipação da ferramenta e Aplicação do método Delphi.

4.2 Estrutura da pesquisa

Uma pesquisa deve ser estruturada de forma a alcançar o objetivo definido, bem como estabelecer os passos ou etapas necessárias para esta consecução, seguindo a trilha dos objetivos específicos, de suas tarefas parciais e dos procedimentos técnicos a serem utilizados para que as etapas sejam cumpridas.

Para uma melhor compreensão faz-se necessário não somente promover um desenho da pesquisa, mas promover uma explicação textual das etapas e dos procedimentos a serem adotados. Ressalta-se que, dentro dos procedimentos técnicos há o de revisão bibliográfica que permeia todas as etapas, razão pela qual não foi individualizado em cada uma e sim definido como um quadro único que atravessa longitudinalmente o gráfico apresentado pela Figura 4.2.

Durante as etapas são desenvolvidos procedimentos técnicos, para os quais se faz necessário compreender alguns parâmetros, como a população do NuCDCAer, que representa a organização-alvo da pesquisa, bem como as amostras utilizadas nos procedimentos específicos.



Revisão Bibliográfica

Figura 4.2: Estrutura da pesquisa

Para a compreensão da extensão da organização, cita-se: Núcleo de Defesa Cibernética do Comando da Aeronáutica (NuCDCAer), subordinada ao Comando de Apoio (COMGAP), diretamente ligada à Diretoria de Tecnologia da Informação (DTI). É uma organização criada em 2020, para suprir as necessidades de um amplo projeto do Ministério da Defesa e das Forças Armadas singulares. É dividida entre Divisão Administrativa (não ligada à área-fim) e a Divisão Técnica (ligada à área-fim), onde trabalha a maior parte do efetivo. Há subdivisões nas áreas de desenvolvimento, suporte e segurança, sendo esta última o foco da pesquisa. A Subdivisão de Segurança da Informação (SDSI).

Os próximos tópicos definem as etapas de consecução da pesquisa ilustradas pela Figura 4.2.

(i) **Etapa 1 – Análise do Contexto de Defesa Cibernética**

A meta, para este passo foi, de acordo com o objetivo específico 1, estabelecer o contexto básico sobre Defesa Cibernética, necessitando, para tal, buscar os motivadores legais e trabalhos técnicos iniciais que nortearam o tema Segurança da Informação, limitando-o em Segurança Cibernética antes de especializá-lo no tema Defesa Cibernética, meta dos órgãos do alto escalão governamental, responsável pela defesa do país, em reconhecimento à importância deste setor de defesa.

(a) Investigar leis e iniciativas norteadoras do tema segurança cibernética

Foi realizado o levantamento documental e bibliográfico sobre a legislação preliminar e os trabalhos iniciais em segurança cibernética, surgidos em reação à tendência internacional no tema, decorrente de eventos registrados, sendo alguns de alto impacto social e financeiro. O tema pesquisado transcende, em parte, à necessidade direta de compreensão do título deste trabalho, pois, inicialmente, deve-se conhecer aspectos de segurança da informação e segurança cibernética para a correta compreensão da teoria e das ações da defesa cibernética. Os conhecimentos componentes necessários estão disponíveis no capítulo 3 (Referencial Teórico) e os eventos motivadores no capítulo 5 (Resultados Preliminares).

(b) Identificar ações do Governo Federal para a implantação da segurança cibernética

Nesta tarefa foi desenvolvido, após a compreensão das legislações e pesquisas iniciais desenvolvidas, demandadas pelos órgãos ou evidenciadas por pesquisas espontâneas, um levantamento das ações iniciais que estes órgãos governamentais desenvolveram como resposta àqueles motivadores.

Ações como criação de equipes, comissões, organizações, normativos, projetos, sugestão de criação de outras legislações ocorreram e ainda ocorrem, à medida que as necessidades são ampliadas, em decorrência de novos eventos.

O procedimento técnico para levantamento das informações foi o de análise documental, em legislações como decretos e portarias ministeriais.

(ii) **Etapa 2 – Entendimento do processo de CSC do NuCDCAer**

Para a compreensão e consecução do objetivo específico 2, identificou-se a necessidade de se aprofundar a abordagem da pesquisa e compreender o processo de

obtenção da Consciência Situacional Cibernética dentro do NuCDCAer, seguindo as recomendações da Doutrina Militar de Defesa Cibernética [7].

O primeiro passo foi compreender a necessidade básica do projeto de CSC do NuCDCAer, dentro do projeto maior, capitaneado pelo Ministério da Defesa que visa replicar a estrutura nos outros órgãos de defesa, como as outras Forças Armadas singulares (Marinha e Exército).

(a) Identificar a saída do processo – Nível de Alerta Cibernético (NAC)

Este projeto almeja a geração de um índice (Nível de Alerta Cibernético – NAC), cujos valores, interpretações, escala e ações a tomar em cada nível estão definidos na Doutrina Militar de Defesa Cibernética [7], que permita quantificar o nível de comprometimento cibernético encontrado no espaço cibernético de interesse de cada órgão via processos de obtenção de consciência situacional cibernética, e em seguida agrupá-los em um órgão central, o Centro de Defesa Cibernética - CDCiber, diretamente subordinado ao Comando de Defesa Cibernética - CDCiber, para servir de subsídio às decisões estratégicas de defesa cibernética.

O problema em si foi dividido em partes menores e estudado, para a composição de um cenário que facilite a compreensão e a criação de soluções técnicas e administrativas e o desenho do processo via notação BPMN, o qual será explicitado na etapa 3.

(b) Analisar os índices componentes do NAC

Para este estudo pormenorizado, foram identificados os processos internos das seções do NuCDCAer, os quais endereçam aos índices de Incidentes Cibernéticos (IIC), de Ameaças Cibernéticas (IAC) e o de Riscos Cibernéticos (IRC), objeto deste trabalho de pesquisa e sob a responsabilidade da SGSI.

(c) Examinar os procedimentos de cálculo do NAC

O próximo passo indica a necessidade de compreensão sobre como funciona o ciclo de informações para geração do NAC (Nível de Alerta Cibernético), definido na Doutrina Militar de Defesa Cibernética [7] como sendo o indicador de comprometimento do espaço cibernético brasileiro e para o qual o esforço de criação do processo de avaliação de riscos para a geração do IRC é endereçado. Além do ciclo de informações, o processo de cálculo do valor quantitativo do índice é levantado e explicitado por uma fórmula matemática definida em consenso com a SDSI.

Objetivando a obtenção destas informações, os procedimentos utilizados foram a análise documental nas pesquisas em legislações, a análise bibliográfica

em artigos e livros, normas ISO, normativos dos órgãos do Governo Federal e em entrevistas com especialistas da área, no Núcleo do Centro de Defesa Cibernética da Aeronáutica (NuCDCAer). Foram realizadas reuniões com os especialistas, onde foram entrevistados 10 integrantes, todos do NuCDCAer ocupando as funções de:

- Chefe da Divisão Técnica (DT)
- Chefe da Subdivisão de Segurança da Informação (SDSI)
- Chefe do Centro de Tratamento de Incidentes de Rede do Comando da Aeronáutica (CTIR.FAB)
- Chefe da Seção de Tecnologia de Defesa (STD)
- Chefe da Seção de Gestão de Segurança da Informação (SGSI)
- Líderes de equipes em Segurança da Informação (CTIR.FAB e STD)

O resultado das entrevistas foi o direcionamento de questões temáticas e sugestão de temas de pesquisa direcionadores, bem como de informações acerca dos processos internos dos setores para obtenção de seus resultados obtidos, com utilidade além desta etapa, como será compreendido na etapa 3.

(iii) **Etapa 3 – Estabelecimento do processo de Avaliação de Riscos Cibernéticos (ARCiber) para o NuCDCAer**

Segundo o objetivo específico 3, é estabelecida a função de criação de um processo de avaliação de riscos, com foco em riscos cibernéticos, cujo produto será o Índice de Riscos Cibernéticos (IRC). O processo deve ser capaz de compor os passos em gestão de riscos estabelecidos na ABNT NBR ISO/IEC 27005:2019 [3], com foco específico em riscos cibernéticos, via identificação de cenários de risco, com escalas padronizadas e uso de *frameworks* de risco.

(a) Escolher modelo inicial de gestão de riscos

Em virtude de não haver qualquer metodologia definida de gestão de riscos, foi necessário identificar um modelo inicial de processos o qual foi encontrado sob a ABNT NBR ISO/IEC 27005:2019 [3], somado aos levantamentos sobre segurança cibernética via norma ABNT NBR ISO/IEC 27032:2015 [38] e REFSDAL e STØLEN [42]. Pôde ser desenhado o processo via notação BPMN segundo BALDAM [58] e ABPMP [59], por meio de buscas nos processos internos das seções do NuCDCAer com a finalidade de resolver os problemas de segurança da forma mais lógica.

(b) Desenhar o processo de ARCiber para o NuCDCAer

Para o desenho deste processo são usados os procedimentos de entrevistas com especialistas, cujos procedimentos da etapa 2 fornecem subsídios para estas atividades, bem como em reuniões de brainstorming na SGSI, seção diretamente ligada ao objetivo desta etapa, além do uso da modelagem de processos via BPMN.

O levantamento para esta etapa ocorreu com pesquisas bibliográficas, artigos, normas, livros e sites especializados, e posteriormente brainstorming com o efetivo da SGSI a fim de estruturar o processo e identificar possíveis *frameworks* de risco, com a finalidade de compor o processo de ARCiber baseado nas melhores e consagradas práticas de segurança cibernética.

(iv) **Etapa 4 – Geração do processo de obtenção do IRC**

Utilizando, diretamente, os conhecimentos obtidos na etapa 3, objetiva-se o cumprimento do objetivo específico 4 como preparação para o desenvolvimento de uma ferramenta. Esta etapa difere da anterior em função do objetivo de estabelecer não os critérios de gestão de riscos cibernéticos, mas estabelecer os requisitos necessários para a geração do IRC.

Para isso foram utilizados os procedimentos de *brainstorming* na SGSI e de duas entrevistas não-estruturadas com especialistas e duas entrevistas semiestruturadas, cuja finalidade é a identificação dos cenários de risco a serem observados e das escalas de avaliação destes cenários, com os pesos a serem adotados entre os mesmos cenários, além da escala de valoração da criticidade do ativo em análise e do tipo de entradas de risco a serem padronizadas.

As entrevistas semiestruturadas foram usadas e diferiram das entrevistas com os especialistas por serem complementares ao *brainstorming* e serem aplicadas em reuniões coletivas.

As entradas de risco correspondem às escolhas dos tipos de relatórios de vulnerabilidades que foram utilizados nas análises, que podem ser obtidos de fontes internas e externas ao NuCDCAer, com parâmetros para comporem os requisitos básicos para o processo de gestão de riscos cibernéticos em seus subprocessos, conforme definido na etapa 3. A finalidade é a de estabelecer o valor de risco de maneira quantitativa, o qual servirá de base para a geração do índice de riscos cibernéticos (IIC).

Finalizando a etapa, foi definida a fórmula de cálculo do IRC a partir dos valores indicados nas análises dos cenários, para uso com a ferramenta a ser desenvolvida.

(v) **Etapa 5 – Criação da ferramenta computacional (protótipo) para cálculo do IRC**

Como parte do objetivo específico 5, trata-se da criação de um protótipo de ferramenta computacional que serviu como teste dos requisitos identificados na etapa 4. Esta parte está a cargo da SGSI, da qual este autor é componente, a qual cumpre as tarefas de definir o tipo de ferramenta mais válido, tendo sido escolhido o formato de planilha em Microsoft Excel 365, pois permite o visual e as funcionalidades de cálculo necessárias, bem como as facilidades de construção sem necessidade de mão-de-obra específica, diferentemente de uma solução de *software* desenvolvida desde o início.

Foi perguntado via entrevista não estruturada com os especialistas da SDSI se esse formato de ferramenta poderia ser usado como ferramenta de uso corrente (calculadora do IRC) e foi estabelecido que o uso com o formato de planilha Microsoft Excel não deveria ser definitivo, mas que a validação dos requisitos é capaz de definir as necessidades básicas para aquisição de uma aplicação comercial ou desenvolvimento de uma aplicação em âmbito interno à organização.

Atualmente, está em curso uma consultoria para avaliar se o processo de avaliação de riscos composto pelo NuCDCAer via SGSI pode ser modelado na plataforma de gerenciamento de governança, riscos e compliance RSA Archer GRC [60], recentemente adquirida, cuja finalidade inicial não é a gestão de riscos cibernéticos, mas foi informada pela consultoria ser suficientemente flexível para receber diversos tipos de abordagens de riscos, inclusive os cibernéticos. Atualmente a consultoria detectou que o processo de ARCiber pode ser integralmente utilizado na plataforma RSA Archer e já o implementou na versão de homologação do software no NuCDCAer.

Cabe ressaltar que a ferramenta RSA Archer compreende uma aplicação comercial, proprietária, a qual possibilita a criação de funcionalidades (processos) dos clientes, sob licenciamento remunerado, de forma interativa. Neste caso recebeu uma aplicação de uso para uma funcionalidade interna que possibilitou a implementação do processo de Avaliação de Riscos Cibernéticos (ARCiber) desenvolvido pela SGSI. Todas as alterações foram efetuadas pela equipe da empresa representante da RSA. A função do efetivo da SGSI (do qual faz parte este pesquisador) foi o de oferecer as características do processo de ARCiber e analisar cada alteração feita, como forma de guiar a implementação, não configurando um redesenho ou alteração intrínseca da aplicação. Os resultados da adição deste recurso foram avaliados e confrontados com a operação básica da ferramenta desenvolvida na SGSI (planilha MS Excel) e foram completamente compatíveis com o desejado no processo de ARCiber.

Em função de sua ação centralizadora de controles de risco, governança e compliance e em função do alto valor dispendido em sua aquisição pode se tornar a opção lógica de viabilização definitiva do processo de avaliação de riscos com a geração do IRC e da conciliação dos dados para o cálculo e do painel de visualização (*dashboard*) para o índice final NAC requisitado pelo MD em um futuro à médio prazo.

Portanto, a ferramenta prototipada pela SGSI é de importância estratégica para a continuação do projeto de processo de avaliação de riscos e geração do IRC. A etapa 6 complementa esta etapa com a validação formal deste artefato (ferramenta de cálculo), a qual será vista a seguir.

(vi) **Etapa 6 – Validação da ferramenta computacional e do método de cálculo do IRC**

Finalmente, para complementar e finalizar o objetivo específico 5, criou-se um procedimento formal para a validação da ferramenta, tanto no aspecto prático, onde é esperado o cumprimento do requisito de estabelecer o IRC, quanto no aspecto de qualidade e validade dos seus cenários, escalas e pesos.

A etapa consiste em entrevistas com os especialistas para apresentar a ferramenta desenvolvida e estabelecer os requisitos dos testes, como quais tipos de dados e avaliações seriam necessárias e quais situações reais poderiam ser utilizadas para o uso prático e real da solução, informando que o uso se dará com dados reais para efetivo teste de confiabilidade do processo.

O objetivo foi o de familiarizar os especialistas com o ambiente e oferecer o contato com os requisitos levantados nas etapas anteriores, com a participação dos mesmos profissionais, evidenciando o compromisso com os esforços demandados e incentivar participações futuras no projeto.

Após a familiarização foram apresentados cenários pré-definidos de análise para uso em situação real da ferramenta (análise de riscos cibernéticos em sistema, serviço ou ativo estratégico à FAB) e consequente coleta de dados e de impressões dos operadores. Esta parte da avaliação ofereceu os subsídios para que os profissionais que participaram do teste pudessem responder aos questionários de validação, por meio de entrevistas estruturadas. Para esta atividade programou-se o uso da amostra da SDSI (30 pessoas), por conveniência, em razão do tema e do grau de sigilo mínimo exigido.

Para o levantamento das impressões sobre o processo foi utilizada a pesquisa por entrevista estruturada com o método DELPHI.

A função básica do método DELPHI utilizado é a premissa de que é possível analisar os critérios e escalas definidos para a ferramenta, bem como avaliar as impressões de uso em situação real para estabelecer um consenso entre os especialistas da SDSI e, desta forma, avaliar a eficácia da ferramenta e promover as alterações necessárias em suas características básicas de cálculo do IRC.

Esta análise permitiu a seleção dos melhores valores para compor a definição dos atributos, escalas e pesos da ferramenta, reduzindo o caráter subjetivo de escolha dos cenários. Os critérios analisados compuseram cenários, escalas, pesos, criticidade do ativo, entrada dos dados, e saída do índice.

Para facilitar o entendimento das técnicas citadas nas etapas, faz-se necessário uma pequena introdução sobre estas nos tópicos a seguir:

(i) População e definição da amostra da pesquisa

O efetivo do NuCDCAer é a população da instituição de origem da pesquisa, divididas por duas divisões, principais: a Divisão Administrativa – DA, e a Divisão Técnica – DT. O efetivo representa o universo dos integrantes da organização em análise, porém, uma grande parte desta população não se envolve com o tema pesquisado, em virtude de estabelecerem processos puramente administrativos e de recursos humanos (RH), cujas especialidades dos elementos atuantes e suas áreas de atuação estão além do objeto da pesquisa.

Há uma outra parcela desta população, que, apesar de serem de especialidades da Tecnologia da Informação (TI), e pertencerem à DT, não se enquadram na pesquisa, em virtude de não atuarem em qualquer área da segurança da informação, incluindo-se estarem distantes, especificamente, da defesa cibernética como área fim de atuação.

A área de Segurança da Informação (SDSI) corresponde à população-alvo da pesquisa e a amostra escolhida para a entrevista compreende 30 pessoas, com profissionais treinados e capacitados para o serviço de segurança da informação e defesa cibernética. Para a qualificação da amostra foi utilizado um questionário com perguntas sobre dados demográficos, educacionais e profissionais básicos, norteados pelo trabalho de Eduardo Wallier [61], cuja pesquisa buscava conhecer as necessidades informacionais de profissionais de segurança cibernética em instituições da Administração Pública Federal (APF). Este questionário revelou que desta amostra de 30 pessoas, 10 delas exercem cargos de liderança ou chefia e por esta razão foram utilizados para as entrevistas semiestruturadas que definiram alguns dados

dos processo de ARCiber e de geração do IRC. As perguntas e os resultados desta avaliação podem ser observados no Apêndice A.

A figura 4.3 representa a qualificação básica dos profissionais entrevistados, e os divide em amostra completa (30 pessoas) e amostra qualificada em cargos de liderança ou de chefia de seções ou equipes.

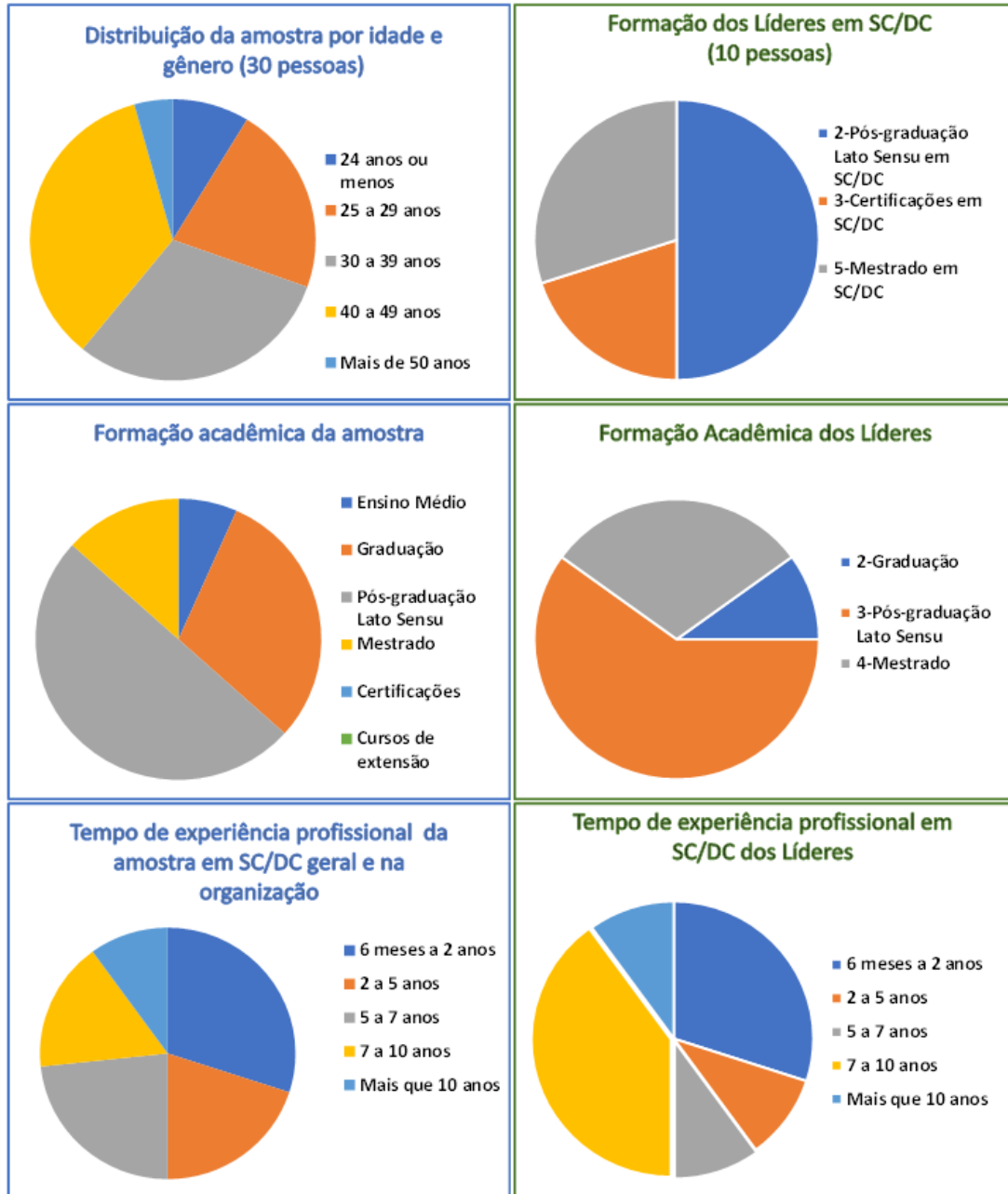


Figura 4.3: qualificação dos profissionais entrevistados

Fonte: Autoria própria

Estes 10 profissionais com cargo ou função de chefia e/ou liderança de seções ou equipes atuam dentro do foco sob análise (Equipes de Gestão de incidentes de Redes, Gestão de Ameaças, Gestão de Vulnerabilidades e Gestão de Riscos). Os outros integrantes são subordinados àqueles e não possuem visão estratégica dos assuntos, porém com participação ativa em etapas posteriores, nos assuntos de natureza tática e operacional, dentro de suas áreas e experiências sobre o tema em pesquisa.

Logo, para a entrevista semiestruturada inicial e as 6 entrevistas com especialistas (cuja função é a de elucidar dúvidas dos processos), as amostras correspondem aos 10 integrantes com cargos de liderança (chefes de equipes), pois têm uma visão dos objetivos com níveis entre o estratégico e o tático.

Para as entrevistas semiestruturadas seguintes (total de 3 entrevistas) e a entrevista estruturada (cuja finalidade será a de avaliar o protótipo da ferramenta de análise e avaliação dos riscos), por tratarem de assuntos operacionais dos processos e estes temas demandarem visão ampla e geral do processo de defesa cibernética, optou-se por entrevistar os 30 (trinta) profissionais selecionados da SGSI.

Os tópicos seguintes demonstrarão as características dos procedimentos técnicos ou de técnicas de pesquisa adotados, suas quantidades empregadas, amostras ou populações utilizadas e questões, temas ou tópicos abordados.

(ii) Entrevista estruturada para qualificação da amostra

Conforme o apêndice A a amostra para esta atividade foi composta com os 30 profissionais escolhidos por conveniência para a amostra da SDSI, relativos ao processo de segurança da informação, com foco mais estrito sobre a segurança ou defesa cibernéticas (SC/DC). O perfil apontado pela qualificação da amostra demonstra predominância de profissionais do sexo feminino com idade média de 30 a 39 anos e masculino com idade média de 40 a 49 anos, com experiência profissional variada, mas com predominância de profissionais (nível de liderança) de 7 a 10 anos e de até 2 anos (nível de execução) na área. A formação acadêmica predominante com foco em SC/DC é a de especialização *lato sensu* com treinamentos adicionais, mas possuindo profissionais com nível de mestrado já obtidos ou em andamento, e um profissional com doutorado em andamento.

As perguntas/assuntos discutidos

Para esta parte foi apresentado o conjunto básico de perguntas que serviu de roteiro para a entrevista estruturada para definição da amostra da pesquisa. O questioná-

rio foi aplicado de forma geral a todo o efetivo da subdivisão, e serviu de estudo da população para todas as outras entrevistas, baseado no trabalho de Viana [61], cujo foco foi o de interpretação das necessidades informacionais dos profissionais de segurança cibernética, em instituições da Administração Pública Federal, coincidentemente necessário para a qualificação dos profissionais do NuCDCAer, foco deste estudo atual. O escopo para esta entrevista foi o de obter informações demográficas e instrucionais dos profissionais do NuCDCAer. Os resultados da caracterização da amostra da população encontra-se no apêndice A.

(iii) Análise documental

O procedimento de pesquisa ou análise documental, de acordo com Lakatos e Marconi [8], utiliza documentação indireta, ou seja, tem por base o uso de dados primários, como legislações diversas e registros de atuação de grupos organizados de pesquisa, motivados pelo poder público, objetivando a criação ou melhoria dos processos necessários cujo tema coincide com o da pesquisa em curso.

A pesquisa pelos documentos foi motivada pelo uso de legislações e manuais do Ministério da Defesa, do Exército Brasileiro e do Comando da Aeronáutica, em virtude de o trabalho de organização ter sido solicitado por documento oficial de demanda, informando o tema. A partir deste ponto, estabeleceu-se uma pesquisa embasadora para ligar os pontos obscuros e aumentar a confiabilidade da busca por informações ligadas ao tema.

(iv) Entrevista não-estruturada (Entrevista com Especialistas)

Segundo Lakatos e Marconi [8] uma entrevista não-estruturada ou despadronizada é a que oferece ao entrevistador autonomia em desenvolver suas questões com mais liberdade. Compõe-se de uma conversa informal acerca de um tema de interesse, normalmente com perguntas abertas com o objetivo de esclarecer alguma dúvida do entrevistador. Esta técnica utilizada dentro desta pesquisa optou por utilizar o que os autores denominam de entrevista focalizada, possuindo um roteiro de tópicos a serem abordados, não possuindo, entretanto, as perguntas definidas. A intenção foi a de complementar as análises documentais e entrevistas semiestruturadas em assuntos que continuaram com dúvidas a esclarecer ou a aprofundar.

Para tal usou-se a terminologia “Entrevista com Especialistas” para redefinir o termo "Entrevista não-estruturada", pois considera-se que não representa a utilidade do procedimento, e em função da praticidade e utilidade deste título, utilização pre-

vista e concretizada em 6 vezes, como nas atividades de descrição da saída do processo gerador do NAC e na análise dos componentes do processo gerador do NAC; para auxílio (compreensão) no desenvolvimento das escalas de avaliação de critérios, pesos, criticidade dos ativos e forma de entrada das vulnerabilidades para uso no processo de cálculo do IRC, bem como na deliberação da fórmula do cálculo do IRC; e nas atividades de validação do protótipo da ferramenta computacional de cálculo do IRC, antes da aplicação do método DELPHI. Nestas entrevistas optou-se por estabelecer tópicos para discussão, de acordo com cada etapa e cada tarefa, não havendo um questionário padronizado, servindo como técnica de redução de dúvidas pontuais, mas com a formalização de prazos para encontros, como forma de não interferir desnecessariamente no trabalho dos profissionais.

Para as entrevistas da etapa 2 (vide Figura 4.2, item 4.2) o foco estabelecido foi o de compreender o processo de cálculo do Nível de Alerta Cibernético (NAC), em uso pelo ComDCiber, constante da Doutrina Militar de Defesa Cibernética [7], o qual, apesar de não fazer parte do escopo desta pesquisa, é importante para integrar os esforços dos setores do NuCDCAer na compreensão e desenvolvimento de seus próprios processos de análise e obtenção dos índices individuais componentes do NAC. Os tópicos foram:

- Compreender os níveis de alerta cibernético;
- Caracterizar cada nível;
- Interpretar os níveis;
- Identificar possibilidade de mudanças de nível; e
- Conhecer as ações de resposta previstas pelo MD.

Para a etapa 4 (vide Figura 4.2, item 4.2) os tópicos da entrevista situam-se nos aspectos, com a amostra populacional correspondente aos 10 componentes de nível estratégico:

- Identificar cenários de risco possíveis ou plausíveis;
- Estabelecer escalas apropriadas para avaliação dos cenários;
- Aplicar ou não valores numéricos de pesos para ponderar os aspectos dos cenários;
- Definir origem, tipos e critérios de valores das criticidades dos ativos a serem analisadas; e
- Classificar tipos de ativos e seus possíveis valores de criticidade.

Para a etapa 6 (vide Figura 4.2, item 4.2) o foco teve suas diferenças em uma informação aos especialistas dos procedimentos que serão adotados. Houve uma troca de informações entre os pesquisadores e os procedimentos adotados com os respondentes, pois versaram sobre a definição do processo de validação em si para o uso real da ferramenta em análises de risco cibernético. A finalidade foi a motivação dos mesmos em responder de maneira fidedigna e crítica ao uso da ferramenta em situação real e do questionário subsequente de entrevista estruturada, que permitiu a análise crítica da ferramenta e do processo de análise como um todo. Para estes procedimentos a amostra foi a dos 30 elementos selecionados em todos os níveis de atuação.

(v) Entrevista semiestruturada

Entrevistas semiestruturadas, são, segundo Lakatos e Marconi [8], correspondentes ao encontro entre duas pessoas com o uso de conversação e reúnem informações pertinentes ao objeto de pesquisa. Possui a vantagem de permitir amplo uso, fácil obtenção de dados difíceis de serem obtidos via análise documental ou bibliográfica, boa precisão, possibilidade de permitir quantificação e análises estatísticas. Possui limitações pela dificuldade ou medo de exposição de alguns entrevistados, influência do entrevistado pelo entrevistador e de disponibilidade dos entrevistados.

Para esta coleta de informações inicial, na etapa 2, foram entrevistados os 10 especialistas com foco estratégico, pertencentes à população-alvo da pesquisa, via entrevista semiestruturada, focalizada, onde foi utilizado questionário básico direcionador e recebidas informações direcionadas pelas perguntas, bem como respostas livres. Foi utilizada a técnica de entrevista pessoal, com formulário impresso e resposta direta durante as entrevistas.

Para tal, preparou-se um questionário com 6 questões abertas, focando nas atribuições básicas de seus setores, segundo os aspectos estratégico e tático. Segundo Vieira (2009, p. 30) [62], questionário é um instrumento de pesquisa, cuja composição estabelece perguntas sobre um tema. Os participantes são denominados respondentes e suas respostas alimentam de dados ou informações a pesquisa. Podem apresentar perguntas fechadas, caso possuam um conjunto de respostas padronizadas a serem escolhidas, ou abertas caso sejam de livre resposta do participante. Segundo Vieira [62] podem estabelecer questões sobre fatos, opiniões, atitudes, preferências, satisfação e podem ser aplicados em formato de autoaplicação, remotamente (telefone, Internet, videoconferência) ou pessoalmente, opção escolhida neste trabalho em função dos respondentes trabalharem no mesmo ambiente físico.

Por possuir um questionário norteador, esta entrevista caracteriza-se como uma entrevista semiestruturada segundo Lakatos e Marconi [8].

As respostas guiaram a estruturação do entendimento dos processos de aquisição de consciência situacional cibernética e dos índices componentes do Nível de Alerta Cibernético – NAC, representativo do grau de consciência situacional, pela composição dos processos e subprocessos identificados nas atividades em que os respondentes são líderes.

Para as respostas que precisaram de organização de informações pelos respondentes, foram estabelecidos prazos de entrega estendidos, individualmente, a fim de obter informações mais completas. O questionário completo encontra-se no apêndice B.

Para esta atividade, os respondentes, cuja amostra corresponderá aos 30 integrantes selecionados da SDSI, receberão, antecipadamente, informações sobre as origens das identificações dos cenários e critérios, como, por exemplo, o uso dos *frameworks* Mitre Att&ck [63], Mitre D3fend [64], The Cyber Security Body of Knowledge - CyBoK [65], NIST Cybersecurity Framework [66] entre outros.

Por meio de entrevistas não-estruturadas anteriores estes *frameworks* compuseram diversas respostas, sugerindo o direcionamento das pesquisas para estas ferramentas de segurança cibernética que começam a estabelecer padrões de referência para a área cibernética.

Para o estabelecimento do processo de avaliação de riscos (ARCiber) e consequentemente do IRC foi efetivada mais uma segunda entrevista semiestruturada, com os profissionais de nível estratégico, para a definição dos parâmetros básicos dos controles e demais dados informacionais que subsidiam o processo de ARCiber, apresentada a seguir, e analisada no item 5.4.2 deste trabalho.

Descrição da entrevista com os especialistas

Na etapa 4 (vide Figura 4.2, item 4.2) esta técnica voltou a ser utilizada, para crítica inicial e sugestão de critérios de análise dos cenários e das escalas de avaliação e evidenciou as seguintes informações: o arcabouço teórico de segurança cibernética utilizado (framework de risco); os tipos ou agrupamentos de controles baseados no framework escolhido a serem utilizados; as escalas de comparação da eficácia dos controles para escolha por parte dos analistas do nível de proteção indicado, bem como da padronização dos valores e itens a serem selecionados para esta análise; da fórmula básica de cálculo para cada controle em relação à vulnerabilidade, de cada vulnerabilidade em relação às demais, de como estes valores serão trabalhados para se chegar ao valor de referência para multiplicação com a criticidade do ativo; da

escala de criticidade dos ativos estratégicos; e como o IRC será revelado ao analista. A especificação da entrevista, seu processo básico e perguntas norteadoras, bem como das ideias levantadas e do resultado dos questionamentos podem ser observadas nos apêndices C e D, porém a estrutura básica da entrevista pode ser vista a seguir.

As partes 1 e 2, além dos blocos A e B da parte 2 da entrevista semiestruturada estão evidenciados no apêndice C. O resultado da análise das respostas dos blocos C e D podem ser observados no apêndice D. As informações da parte 3 pode ser observada no capítulo 5, item 5.4.2, subitem V.

Parte 1: Identificação das dependências e necessidades informacionais e dos elementos do processo de gestão de riscos (níveis de criticidade dos ativos, frameworks, cenários/controles, escalas de avaliação dos controles e dos riscos);

Parte 2: Identificação dos elementos do processo de gestão de riscos (níveis de criticidade dos ativos, frameworks, cenários/controles, escalas de avaliação dos controles e dos riscos);

- Bloco A – Identificação da criticidade estratégica dos ativos para a organização;
- Bloco B – Identificação dos padrões para o processo de avaliação de riscos (frameworks);
- Bloco C – Identificação dos critérios/cenários/controles para avaliação dos riscos cibernéticos;
- Bloco D – Identificação das escalas de avaliação para critérios/cenários/controles.

Parte 3: Estabelecimento das fórmulas de cálculo e dos resultados esperados.

(vi) Entrevista estruturada

Para a validação do protótipo de ferramenta computacional será utilizado o processo de pesquisa estruturada, por meio de questionário estruturado em questões fechadas de diversos tipos, usando escala de Likert [67] e espaço para introdução de comentários às questões, de forma livre, para que o respondente possa estabelecer relações de crítica aos temas abordados.

O questionário utilizado, conforme apêndice E, ofereceu perguntas que analisaram os critérios individuais que compuseram os cenários de análise e avaliação dos riscos cibernéticos, bem como as escalas utilizadas na ferramenta computacional de cálculo. Esta atividade estabeleceu uma crítica ao processo de avaliação e os resultados ofereceram subsídios para análise via método Delphi.

A quantidade dos respondentes foi a da amostra qualificada da SDSI (30 componentes), por conveniência, em razão do tema e do grau de sigilo mínimo exigido durante a análise de situações reais de risco. A técnica da entrevista estruturada foi analisada pelo método Delphi, em função de sua praticidade perante a amostra escolhida e de ser tecnicamente viável para o objetivo da etapa de validação da ferramenta (Etapa 6). A finalidade foi a avaliação da eficácia do método e da qualidade dos critérios (controles) de avaliação dos riscos cibernéticos.

(vii) *Brainstorming*

A técnica de *brainstorming*, segundo a ABNT NBR ISO/IEC 31010:2012 [68] envolve a conversação coletiva entre pessoas com conhecimento sobre o objeto ou assunto estudado com a finalidade de estabelecer linhas de ação diversas, incluindo direcionamento ou mudança de direcionamento da pesquisa acerca de temas de interesse. Normalmente é usado em conjunto com outras técnicas e métodos para complementação da atuação e pesquisa.

Ao longo da pesquisa, este procedimento foi e continuará sendo utilizado para discutir levantamentos de informações, como delimitação e extensão do escopo e definição de etapas e planejamentos diversos, bem como regras para cálculos e processos de validação.

Possui a vantagem de ser flexível, mas limitado pela possível falta de habilidade de algum participante, perda de foco na discussão e dominância excessiva de algum participante em detrimento de outros, segundo Lakatos e Marconi [8].

A população, para as reuniões de *brainstorming*, é a da SGSI, com os 3 (três) integrantes, em virtude de ser a seção que está responsável pela estruturação formal do processo de avaliação de riscos cibernéticos, para o projeto de integração com o ComDCiber.

A técnica foi utilizada extensivamente durante a pesquisa, especialmente na etapa 02, na atividade de examinar os procedimentos de cálculo e dos índices do NAC; etapa 03, atividades de identificação dos cenários de risco e da deliberação da fórmula de cálculo do NAC; na etapa 04, atividade de estruturação da ferramenta de cálculo do IRC; e na etapa 05, na atividade de definição do processo de validação da ferramenta de cálculo do IRC.

(viii) Notação BPMN:

A modelagem de processos de negócios (*Business Process Management – BPM*) representa uma atividade que objetiva a representação de processos por meio gráfico, estabelecendo uma compreensão mais precisa possível do funcionamento de cada processo e de suas interações [59]. Foi usada a técnica de notação dos processos identificados pela linguagem *Business Process Model and Notation* (BPMN), capaz de representar os processos e suas interações com seu uso facilitado por ser inserida em diversas ferramentas de modelagem via sistemas de informações, segundo Baldam [58].

Esta técnica foi utilizada pelos integrantes da SGSI (03 pessoas), com o auxílio (avaliação de conformidade) dos especialistas (os 10 integrantes) já citados, com visão estratégica e cargos de chefia ou liderança, dentro das seções da SDSI.

Seu uso ocorreu na etapa 3, para diagramação dos processos de gestão de riscos (em geral) e cibernéticos, bem como na etapa 4, quando foi criado o diagrama de avaliação de riscos cibernéticos, para o uso da ferramenta computacional do NuCDCAer.

Cabe ressaltar que a organização está em fase final de estruturação, e diversos processos de negócio, incluindo os processos de gestão de riscos em geral, base para o entendimento do subprocesso de avaliação de riscos cibernéticos foi desenhado durante o desenvolvimento deste trabalho. O processo de avaliação de riscos cibernéticos foi igualmente mapeado e desenvolvido durante a pesquisa e foi reconhecido pela chefia do NuCDCAer como um dos ganhos palpáveis do intercâmbio entre as necessidades organizacionais e a metodologia acadêmica.

Para a diagramação dos processos foi utilizada a linguagem BPMN por meio do software Microsoft Visio 2016, com os estênceis para BPMN.

(ix) Software Microsoft Excel para Prototipação da Ferramenta

Segundo Rosemberg et al. [69], prototipação é uma representação limitada ou uma simulação de um design ou ideia, tarefa, e pode ser usada como meio de comunicação para os membros de uma equipe de desenvolvimento. Wazlawick [70] propõe o uso de protótipos para auxiliar na compreensão dos requisitos de um sistema e de sua arquitetura.

Para esta pesquisa, seu uso age em direção ao propósito de Wazlawick, pois é usada como uma técnica de teste para o método da avaliação dos riscos cibernéticos desenvolvido, com a finalidade de testar a efetividade e adicionalmente validar os

controles, pelo uso por meio dos especialistas que efetivamente serão os clientes do método nas atividades diárias da organização.

Estas limitações se situam na dificuldade de automatizar o processo, e de oferecer uma forma mais rápida e prática de avaliar os riscos cibernéticos e de gerar o IRC. Para a prototipação, a ser usada na etapa 5, será utilizada uma pasta de trabalho no formato Excel 365 (extensão .xlxs), escolhida pela simplicidade e capacidade, aliada ao baixo custo. Serão utilizadas diversas planilhas componentes, as quais exibirão os formulários (planilhas) de entrada de dados para as vulnerabilidades a serem valoradas sob a análise dos cenários (critérios ou controles) de risco cibernético definidos segundo os valores das diversas escalas indicadoras dos níveis, planilha com definição de pesos para os critérios, bem como do relatório consolidador e gerador do índice IRC para a análise em curso.

(x) Aplicação do método DELPHI:

Segundo Castilla-Polo [71] o método Delphi se caracteriza em uma utilização sucessiva de um processo de questionamentos a especialistas em determinado assunto visando estabelecer um consenso, tendo sua origem nos anos 60, sendo um método qualitativo baseado em opiniões, sendo o consenso entre os respondentes considerado uma solução confiável para uma definição ou validação de constructos.

Segundo Rocha-Filho [72], o método Delphi define-se como um processo estruturado de comunicação coordenada, cuja finalidade é a obtenção de um consenso de opiniões de um grupo seletivo de pessoas, pressupondo-se que o julgamento coletivo, com bom nível de concordância sobre um determinado tema apresenta um padrão de maior validade sobre os julgamentos individuais.

Oliveira (2008) [73] afirma que o método não requer condições de conhecimentos avançados de matemática ou estatística para a sua implementação, com a heterogeneidade e discrição dos especialistas considerado um ponto vantajoso para o processo, significando que níveis e áreas de conhecimento dos respondentes dos questionários, aliado à individualidade e sigilo de suas opiniões propicia um ambiente de maior interatividade, liberdade e redução de interferências ao processo de obtenção do consenso sobre a matéria em estudo.

Segundo Rocha-Filho [72] o método pode possuir diversos formatos para aplicação, porém deve compreender três premissas definidoras: que o painel possua pessoas selecionadas (especialistas no tema), que haja anonimato entre os respondentes (não contaminação das respostas por persuasão, receios etc.), que seja um processo in-

terativo de retroalimentação controlada (uma ou mais rodadas de respostas, caso necessário, sendo oferecidos *feedbacks* sobre a rodada anterior para cada questionamento).

Quanto à forma de administração dos questionários Rocha-Filho [72] observa que há três modos básicos: o primeiro, da implantação original do Delphi, com o uso e intercâmbio de cartas enviadas; o segundo, face a face dentro de um mesmo ambiente (o que pode dificultar a presença de todos a um mesmo instante); e o terceiro, via ferramentas virtuais de coleta, com uso de plataformas *online* diversas.

Para a aplicação neste trabalho foi usada a terceira forma, pois apesar de os respondentes estarem em um mesmo ambiente, suas disponibilidades não são constantes e a ferramenta virtual permite automações de resultados que facilitam o resultado.

Quanto à amostra necessária para o método, encontra-se em Marques [53], cuja análise oferece uma quantidade mínima de 10 respondentes e de Rocha-Filho [72], cujos argumentos sugerem um mínimo de 7 respondentes. O universo de 30 pessoas da amostra da SDSI supera este valor mínimo das referências, apesar de poderem haver desfalques, em virtude da dinâmica das equipes durante o período da pesquisa.

Este método será usado para o processo de validação da ferramenta computacional de cálculo do IRC, para avaliação dos cenários de risco (aspectos ou controles) e de suas escalas de uso pelo contingente da SDSI, espera-se que a amostra dos 30 componentes (especialistas) em defesa cibernética possa ser completamente utilizada. Cabe ressaltar que a definição dos controles de avaliação dos riscos, por se tratar de processo tático, foi desenvolvido pelos líderes ou chefes de equipes ou seções, que também fazem parte da amostra dos respondentes, em virtude de nem todos terem disponibilidade do uso cotidiano da ferramenta, dentro de suas tarefas específicas, tendo esta fase a finalidade da avaliação prática da ferramenta.

O método compreende, segundo Castilla et al. [71] no envio de um questionário de respostas anônimas, com um texto introdutório com a contextualização dos indicadores a serem avaliados por meio de uma bibliografia escolhida. Segundo Rozados [74] o instrumento de coleta do Delphi é sempre um questionário, que pode ser entre dois tipos: os setoriais, voltados para um ramo técnico específico ou domínio do conhecimento e os generalistas, cujo foco é difuso, procurando estabelecer uma previsão de futuro sem uma especificidade de campo ou área do conhecimento. Para este trabalho, a primeira opção foi a utilizada.

Para o estabelecimento do questionário para o método Delphi, foi escolhida a escala de Likert [67] modificada, com 4 respostas possíveis, não compreendendo resposta neutra em virtude de o questionário ser aplicado para testar um assunto objetivo, de

conhecimento dos respondentes, os quais são profissionais capacitados, como forma de obter respostas analisadas e não opiniões, conforme exemplifica Sonia Vieira em seu livro [62]. Este recurso é corroborado no trabalho de Hill [75], cuja orientação é a de que sempre há algum prejuízo, tanto ao oferecer uma saída neutra para os respondentes, que podem não se comprometer necessariamente com a resposta, partindo pelo "caminho mais cômodo de não se posicionar", quanto ao eliminar a possibilidade de resposta neutra, o que pode gerar uma saída negativa, como forma de "protesto" pela obrigação de estabelecer uma afirmação categórica, negativa ou positiva.

Espera-se que, em virtude do público especializado, não haja comprometimento da finalidade, em virtude de ser um processo coletivo de construção de processos para uma organização que se estrutura durante o seu funcionamento de forma ainda dependente administrativamente de sua organização geradora (o Centro de Computação da Aeronáutica de Brasília).

Rozados [74] afirma que a quantidade mínima de rodadas deve seguir a dificuldade de consenso, no caso de assuntos polêmicos, a capacitação e experiência dos respondentes no tema. Identificou-se ainda em Rozados [74] que uma a duas rodadas é essencial ao método, mas três ou mais rodadas é considerado um evento raro, e comumente ineficaz por desinteressar os respondentes.

O tópico a seguir define a estrutura básica da pesquisa com seus objetivos específicos, etapas e procedimentos técnicos utilizados.

Capítulo 5

Resultados

5.1 Análise do Contexto de Defesa Cibernética

Para que o primeiro objetivo específico seja cumprido, faz-se necessário um estudo das necessidades do NuCDCAer e compreender as exigências de conformidade com leis, decretos e doutrinas militares que os setores de defesa cibernética necessitam cumprir. Tal necessidade se justifica não somente pela obrigatoriedade legal, mas por suas responsabilidades sociais e pelas boas práticas sugeridas por normativos nacionais e internacionais.

Em função destas necessidades importa compreender uma cronologia de eventos que levaram ao surgimento de estudos, leis e decretos que visam fornecer arcabouço legal e normativo para ações que demandam recursos financeiros, humanos e técnicos para criação e manutenção de estruturas de estudo e proteção cibernéticas.

Esta etapa foi caracterizada por dois entendimentos básicos: Estudo das leis e trabalhos que nortearam o tema amplo segurança cibernética; e Entendimento das ações práticas realizadas pelo Governo Federal para a implantação inicial da segurança cibernética. Estas ações estão descritas nas seções a seguir, no formato de uma linha do tempo de atividades realizadas, mas que formam um entendimento conjunto entre as iniciativas legais e práticas efetivamente executadas.

Serão evidenciados os resultados das atividades desenvolvidas, cuja contribuição deste trabalho se dá na composição do estudo de um dos subprocessos componentes da aquisição da consciência situacional cibernética, elemento que pode mensurar o grau instantâneo de risco cibernético do país.

5.1.1 Legislações e iniciativas norteadoras do tema segurança cibernética

Importa observar as iniciativas oficiais para o estabelecimento de um processo que permita a proteção do espaço cibernético brasileiro e todo seu ecossistema.

As necessidades de conhecimento e proteção dos riscos cibernéticos pelos quais o Brasil pode estar sujeito motivaram as diversas ações tomadas em termos de criação de grupos de trabalho e publicação de legislações diversas, e assim forneceram o subsídio necessário para a compreensão das necessidades de conhecimento e controle do espaço cibernético brasileiro.

Em 2008 foi editado o Decreto Nº 6.703 – Estratégia Nacional de Defesa (END) [76] como a primeira reação em nível estratégico que sinalizou a necessidade, além das estratégias naturais de defesa física, em termos militares do país, a reconhecer o setor cibernético como componente importante da defesa nacional. Isso traz visibilidade e foco ao setor e permite a adoção de outras atividades em níveis estratégicos e táticos para que se desenvolva uma mentalidade e uma indústria com a finalidade de subsidiar o tema.

Em 08 de setembro de 2009 foi publicada a portaria nº 45 [77], pelo Gabinete de Segurança Institucional da Presidência da República (GSI-PR) instituindo o Grupo Técnico de Segurança Cibernética (GT SEG CIBER), no âmbito da Câmara de Relações Exteriores e de Defesa Nacional (CREDEN), a qual é um órgão do Conselho de Governo, com o objetivo de propor diretrizes e estratégias de Segurança Cibernética.

O trabalho do GT SEG CIBER, entre outras atividades culminou na publicação do Livro Verde – Segurança Cibernética no Brasil [78]. Este grupo contou com a estrutura de defesa nacional composta pelo GSI-PR, Ministério da Justiça (MJ), Ministério das Relações Exteriores (MRE), Ministério da Defesa (MD) e seus órgãos subordinados, os três Comandos ou Forças Armadas (Marinha, Exército e Força Aérea). Sendo, logo após, em 09 de novembro do mesmo ano publicada a Diretriz do Ministério da Defesa nº 0014/2009 [79], estabelecendo a integração entre os setores militares de defesa, nos mais variados assuntos. A área cibernética foi contemplada com as seguintes informações:

- Não havia (2009) quaisquer tipos de tratados e controles internacionais sobre o tema específico;
- Sugeriu-se a possibilidade de criação de um centro para desenvolvimento de quaisquer tipos de ações cibernéticas (culminando no Comando de Defesa Cibernética – ComDCiber e seu braço tático o Centro de Defesa Cibernética - CDCiber); e
- A possibilidade de composição, deste centro, por militares dos três ramos das Forças Armadas.

O Livro Verde foi o ponto de partida para uma série de atividades e de criação de soluções, pois foi um estudo multidisciplinar elaborado por técnicos das áreas de segurança da informação, defesa, e de políticas públicas em geral, incluindo o delicado contexto das relações exteriores entre nações aliadas ou não. Explicita que a Segurança Cibernética vem sendo caracterizada como importante função estratégica de Estado.

O livro informa sobre a presença do assunto em organismos e fóruns internacionais que suscitam a participação do Brasil, como: pela Organização dos Estados Americanos (OEA) via fóruns como Comitê Interamericano contra o Terrorismo Cibernético (CICTE), Comissão Interamericana de Telecomunicações (CITEL), e, Reunião de Ministros da Justiça ou Procuradores Gerais das Américas (REMJA); pelo International Telecommunication Union (ITU) que estabeleceu áreas de foco em segurança cibernética para os países membros da *Organization for Economic Co-operation and Development* (OECD) como estratégias de combate ao crime cibernético, criação de equipes de resposta a emergências de computação (CERT) e de equipes de resposta a incidentes de segurança informática (CSIRT), além de educação nas áreas, gestão de riscos e suporte às empresas, que dependem cada vez mais da TI, bem como de se registrar e gerenciar o ambiente das infraestruturas críticas do país.

Neste aspecto se nota a importância das atividades de gestão de riscos e de incidentes em redes, itens que se repetem em diversas análises, reforçando suas importâncias, como será visto adiante.

Em 2012 foi atualizada a Estratégia Nacional de Defesa e Criada a Política Nacional de Defesa [1], que, mesmo não sendo específica em segurança cibernética, traça ações de defesa nacional que incluem o assunto, pois define a necessidade de defesa da soberania, do patrimônio nacional e da integridade territorial, que pode ser física ou virtual.

A Doutrina Militar de Defesa Cibernética [7], estabelecida em 2014, explica os conceitos e importância dos termos defesa e guerra cibernéticas como elementos de defesa nacional, definido na Estratégia Nacional de Defesa, porém especializado para o setor cibernético.

A defesa cibernética viabiliza o exercício de Comando e Controle (C2), definido pelo Glossário das Forças Armadas [80] como a estrutura de pessoal, material de recursos que permitem e garantem o desempenho de missões e funções pertinentes à detecção, vigilância, inteligência, auxílio à decisão, entre outros, em cenários de ameaças físicas ou lógicas em nível tático ou estratégico, permitindo ainda simulações para testar efetividade.

No contexto do Ministério da Defesa, a partir das definições da END, de 2008, foram padronizadas as denominações e atuações dos diversos órgãos em seus respectivos níveis dentro do Espaço Cibernético Brasileiro da seguinte forma:

Nível político - Segurança da Informação e Comunicações e Segurança Cibernética - coordenadas pela Presidência da República (PR) e abrangendo a Administração Pública Federal direta e indireta (APF), bem como as infraestruturas críticas da Informação Nacionais;

Nível estratégico - Defesa Cibernética - a cargo do Ministério da Defesa (MD), Estado-Maior Conjunto das Forças Armadas (EMCFA) e Comandos das Forças Armadas, interagindo com a Presidência da República e a Administração Pública Federal; e

Níveis operacional e tático - Guerra Cibernética - denominação restrita ao âmbito interno das Forças Armadas (Denominadas Forças Singulares – FS) , via Comando de Defesa Cibernética (ComD-Ciber), e Força Conjunta de Guerra Cibernética (F Cj G Ciber).

Como forma de melhor entendimento e representação hierárquica, a Figura 5.1 estabelece uma forma visual destes níveis:

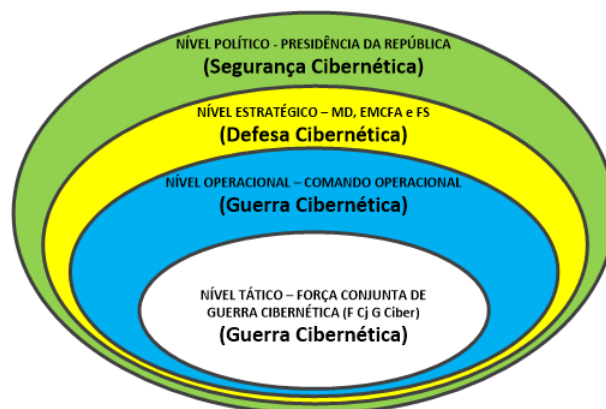


Figura 5.1: Níveis de Decisão no EC
Fonte: Doutrina Militar de Defesa Cibernética [7].

Logo, interpretando-se a Figura 5.1 a defesa cibernética representa um conceito e uma ação a ser tomada em nível estratégico, e a evolução para possível guerra cibernética pertence aos níveis operacional e tático após ordem direta dos níveis superiores (Político e Estratégico).

Segundo a Doutrina Militar de Defesa Cibernética [7] a defesa cibernética pode atuar nas esferas ofensivas, defensivas e exploratórias, dentro do EC, permitindo ações de identificação de ameaças (pela inteligência de fontes cibernéticas), de gestão de incidentes em virtude de sua ação de vigilância e de gestão de riscos por permitir a identificação, análise e avaliação de ameaças e vulnerabilidades com o consequente estabelecimento do nível de risco dentro do espaço cibernético.

A Doutrina Militar de Defesa Cibernética trouxe em seu bojo a criação do Sistema Militar de Defesa Cibernética (SMDC), formalização sistêmica da defesa cibernética brasileira.

A Portaria Normativa nº 2.777/MD/2014 [81] foi publicada com o intuito de garantir a estrutura e responsabilidades da defesa cibernética nacional, com a criação do Comando de Defesa Cibernética (ComDCiber), da Escola Nacional de Defesa Cibernética (ENaD-Ciber), como elemento de educação e de habilitar a dotação orçamentária, de recursos humanos e de infraestrutura física e lógica para a consecução da defesa cibernética nacional.

Em 2015 foi publicada a Política para o Sistema Militar de Comando e Controle - MD31-P-01 [82], cuja finalidade mais importante para este estudo foi a de disponibilizar, para os componentes da Estrutura Militar de Defesa (Etta Mi D), informações que contribuam para a obtenção da Consciência Situacional nos níveis político, estratégico, operacional e tático.

Em 2016 a Controladoria Geral da União (CGU), em conjunto com a Presidência da República (PR) publicou a Instrução Normativa Conjunta nº 1 [83], a qual impõe às entidades do Poder Executivo Federal a implementação de um sistema de gerenciamento dos riscos em todos os níveis de decisão, via controles internos da gestão.

Para continuar a operacionalização das ações necessárias às respostas para os níveis de ameaças cibernéticas, em 2017 o Exército Brasileiro editou o Manual de Campanha para a Guerra Cibernética [39], cuja finalidade precípua é a de estabelecer os conceitos e concepções da Doutrina de Guerra Cibernética do Exército Brasileiro, alinhada com a Doutrina Militar de Defesa Cibernética, em respostas às necessidades levantadas pelo Ministério da Defesa e da necessidade de ação conjunta e integrada das demais Forças Armadas na defesa do espaço cibernético brasileiro.

Em 2018 foram editadas duas grandes legislações que estabeleceram parâmetros além dos já contemplados, visando a proteção de forma holística não só do espaço cibernético do país, como de suas infraestruturas críticas e do ecossistema produtivo e econômico. São eles o Decreto nº 9.573/2018 [84], instituindo a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) e o Decreto nº 9.637/2018 [85] que instituiu a Política Nacional de Segurança da Informação (PNSI).

Em 2020 foi editado o Decreto nº 10.222, de 5 de fevereiro de 2020 - Estratégia Nacional de Segurança Cibernética (ENSC) [6], cujos objetivos, baseados nos parâmetros estabelecidos pela PNSI, almejam guiar as ações estratégicas do país em segurança cibernética servindo como macrodiretrizes para as ações.

Para Brasil (2020, não paginado) [6], são os objetivos estratégicos da ENSC:

1. Tornar o Brasil mais próspero e confiável no ambiente digital;
2. Aumentar a resiliência brasileira às ameaças cibernéticas; e
3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional.

Este decreto possui diversos eixos temáticos, sendo o mais importante para o tema central desta pesquisa o de Governança da Segurança Cibernética Nacional, onde são abordados aspectos sobre mecanismos e medidas para o guiamento e auxílio em governança cibernética, metodologia de gestão de riscos, confiança e segurança no uso de certificado digital, centralização da coordenação da segurança cibernética nacional, e monitoramento do espaço cibernético.

Dentro desta perspectiva, surgem algumas vertentes de interesse, que são: conhecer os parâmetros de performance dos centros de tratamento e respostas de incidentes cibernéticos; a criação de um *dashboard* de segurança cibernética em nível nacional; estabelecer planos de vigilância de adequação da segurança cibernética nas organizações de interesse; construir parcerias na área; levar o tema segurança cibernética para a área da educação.

5.1.2 Ações realizadas pelo Governo Federal para a implantação da segurança cibernética

A proteção do espaço cibernético de interesse para o NuCDCAer inclui como foco secundário a segurança das infraestruturas críticas da informação brasileiras que sejam dependentes de serviços que a FAB possa oferecer. Segundo o Decreto 9573/2018 que institui a Política Nacional de Infraestruturas Críticas [85], a definição de infraestrutura crítica é:

“Instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.”

Ainda segundo este decreto, a segurança destas infraestruturas compreende medidas de caráter preventivo e/ou reativo para garantir a preservação e a restauração dos serviços prestados por estas infraestruturas críticas.

Segundo Lima e Silva [48] as ameaças podem empregar o espaço cibernético para ações que podem gerar efeitos cinéticos e não cinéticos, com danos significativos às infraestruturas críticas de interesse, sujeitando suspensão de atividades de processos estratégicos ao país, motivo pelo qual as Forças Armadas são ligadas à Defesa Cibernética, aumentando

a resiliência cibernética e evitando os problemas reportados como exemplo na Estônia e na Ucrânia.

Uma ação importante para o Brasil é o estudo de incidentes cibernéticos em infraestruturas críticas. Segundo Lima e Silva [48], um evento conjunto de defesa cibernética denominado Exercício Guardião Cibernético [86], já ocorreu 3 vezes desde 2018, com previsão para uma nova edição em 2022. Acontece com a participação das Forças Armadas e de representantes de diversas empresas públicas e privadas ligadas ao funcionamento das infraestruturas críticas dos setores elétrico, financeiro, nuclear e de telecomunicações. O foco do exercício de proteção cibernética é o treinamento operacional em segurança cibernética para formação de mão-de-obra especializada e testar a resiliência cibernética das organizações envolvidas.

Conhecidos os princípios legais, normativos e ações práticas que habilitaram o processo de criação de infraestrutura para a segurança cibernética, cabe compreender as ações resultantes, a partir de suas bases conceituais, como será visto a seguir.

5.2 Entendimento do processo de CSC do NuCD-CAer

A compreensão dos Níveis de Alerta Cibernéticos NAC, definidos pelo Sistema Militar de defesa Cibernética - SMDC permitirá diagramar o processo de CSC do NuCDCAer e reconhecer seus subprocessos componentes.

5.2.1 Identificação da saída do processo – NAC

A função do Sistema Militar de defesa Cibernética - SMDC mais visível é o estabelecimento dos níveis de alerta cibernéticos, que compõem os graus de risco a que está sujeito o EC brasileiro e representa um importante insumo para as tomadas de decisão em defesa cibernética. Para o estabelecimento destes níveis faz-se necessário um conjunto de atividades de identificação de índices para sua composição.

Este trabalho visa o estabelecimento de um processo de avaliação de riscos cibernéticos cujo produto final esperado é o índice de riscos cibernéticos (IRC) cuja estruturação será apresentada no capítulo 5, item 5.5.

Faz-se importante compreender o significado e importância dos Níveis de alerta cibernéticos, e este será apresentado a seguir:

A Doutrina Militar de Defesa Cibernética estabelece níveis de alerta para que as medidas dos graus de risco tenham significado estratégico, tático e operacional para a tomada de decisões em defesa cibernética.

Segundo a Doutrina Militar de Defesa Cibernética [7] a importância deste conhecimento ocorre em função de seu significado quanto à profundidade e intensidade das ações de resposta às ameaças cibernéticas em geral. Em casos de elevado risco, decisões de início de ações de defesa cibernética em níveis táticos e operacionais poderão ser tomadas, até o limite estratégico de uma guerra cibernética. Vale ressaltar que o significado de guerra cibernética não é o mesmo de uma guerra ou conflito internacional tradicional, para a qual existe o consequente uso de tropas e material bélico, sendo usados, neste caso, ferramentas de comando e controle (C2) e pessoal treinado em ações com ferramentas de Tecnologia da Informação e Comunicações (TIC).

A Tabela 5.1 exibe os níveis de alerta cibernéticos, suas cores, nomes e significado formal do comprometimento do espaço cibernético respectivos:

Tabela 5.1: Níveis de Alerta Cibernético

Nível de Alerta		Significado / Interpretação (*)
Cor	Nome	
Branco	Baixo	<ul style="list-style-type: none"> - Aplicável quando as ameaças cibernéticas percebidas não afetam o Espaço Cibernético de interesse do MD e das FA. - Situação normal ou rotineira, considerando o histórico. - Probabilidade de concretização de ameaças cibernéticas baixa, considerando o histórico.
Azul	Moderado	<ul style="list-style-type: none"> - Aplicável quando as ameaças cibernéticas percebidas afetam o Espaço Cibernético de interesse do MD e das FA, sem comprometer as infraestruturas críticas da Informação. - Probabilidade de concretização de ameaças cibernéticas entre baixa e média, considerando o histórico.
Amarelo	Médio	<ul style="list-style-type: none"> - Aplicável quando ações cibernéticas hostis afetam o Espaço Cibernético de interesse, sem comprometer as infraestruturas críticas da informação. - Aplicável quando houver a percepção de ameaças cibernéticas contra as infraestruturas críticas da informação. - Probabilidade da concretização de ameaças cibernéticas entre média e alta, considerando o histórico.
Laranja	Alto	<ul style="list-style-type: none"> - Aplicável quando as ações cibernéticas hostis degradam alguma Infraestrutura Crítica da Informação. - Probabilidade de concretização de ameaças cibernéticas entre média e alta, considerando o histórico. - Infraestrutura Crítica da Informação atingida, porém com possibilidade de restabelecimento das condições de segurança ou dos serviços em tempos aceitáveis para o cumprimento da missão. - Infraestrutura Crítica da Informação atingida com impacto entre médio e alto, considerando o histórico.
Vermelho	Muito Alto	<ul style="list-style-type: none"> - Aplicável quando ações cibernéticas hostis exploram ou negam a disponibilidade das infraestruturas críticas da informação. - Probabilidade de concretização de ameaças cibernéticas muito alta, considerando o histórico. - Infraestrutura Crítica da Informação atingida com impacto alto ou superior, considerando o histórico. - Infraestrutura Crítica da Informação atingida, com possibilidade de restabelecimento da condição de segurança ou dos serviços em tempos além dos aceitáveis para o cumprimento da missão.

Fonte: Doutrina Militar de Defesa Cibernética [7]

Os níveis de alerta cibernéticos foram criados para uso no âmbito do Ministério da

Defesa (MD) e das Forças Armadas (FA), tanto em ações individuais e diárias, quanto no emprego combinado, dependendo do grau de risco e implicação estratégica envolvidos, de acordo com a possibilidade de concretização das ameaças cibernéticas.

5.2.2 Análise dos índices componentes do NAC

No estudo da legislação pertinente, na etapa 1, pode-se destacar três grandes grupos de processos (macroprocessos) para o estabelecimento de uma consciência situacional cibernética a partir da identificação dos ativos críticos de informação, exibidos pela Figura 5.2.

Estes processos foram definidos pelo MD no Projeto de Implantação e Consolidação da Estrutura de Desenvolvimento Conjunto de Defesa Cibernética. Esta estrutura norteou a pesquisa e guiou o desenvolvimento de soluções teóricas e práticas para a obtenção dos Níveis de Alerta Cibernéticos, que representam o resultado do processo de aquisição de consciência situacional.

Para obtenção da Consciência Situacional Cibernética (CSC), foi identificada a necessidade de se observar e correlacionar três aspectos distintos (macroprocessos) no Espaço Cibernético (EC) de interesse conforme descrito na Figura 5.2:

1. Gestão de Incidentes de rede (Ocorrência/tentativa de ataques) – obtida via Índice de Incidentes de Redes (IIC)
2. Gestão de Riscos Cibernéticos (Suscetibilidade a ataques) – obtida via Índice de Riscos Cibernéticos (IRC)
3. Inteligência (Gestão) de Ameaças Cibernéticas (Ameaças latentes no EC) – obtidas via Índice de Ameaças Cibernéticas (IAC)

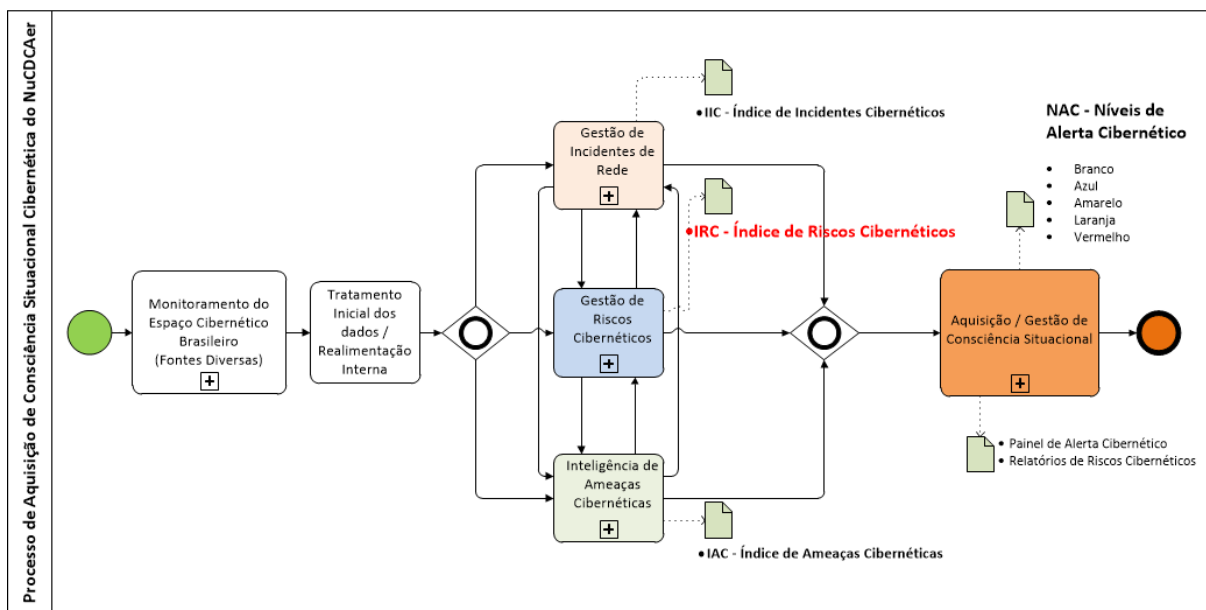


Figura 5.2: Processos de Aquisição de CSC

Fonte: Autoria própria

Em relação aos três aspectos listados acima, cabe ressaltar que tanto o IIC quanto o IAC são índices que medem a intenção de atores capazes de realizar um ataque no EC de interesse. Já o IRC mede o quão suscetível está o EC de interesse a um ataque, com a identificação de vulnerabilidades e ameaças possíveis. Este índice, além de oferecer uma avaliação do nível de maturidade de todo o processo de gestão de riscos, serve como elo central do processo de aquisição de consciência situacional. Ao se correlacionar a probabilidade da existência de ameaças com o nível de exposição (vulnerabilidades existentes) dos serviços críticos da Força, é possível obter uma medida para a possibilidade de concretização de uma ameaça cibernética.

A Figura 5.2 representa, de forma resumida, os processos componentes da aquisição da consciência situacional cibernética (CSC), componente central da gestão da segurança cibernética, em espectro mais amplo para o COMAER e de defesa cibernética, representando o aspecto mais específico do trabalho.

Para tal, remete-se à Doutrina Militar de Defesa Cibernética [7] e aos trabalhos já avaliados de Endsley [2] e no trabalho que estende o de Endsley, sob os olhares de Tadda e Salerno [13] em sua divisão por níveis de significância da CSC.

Basicamente os processos estão divididos em:

1. Processos de monitoramento do espaço cibernético: entrada dos dados de vulnerabilidades ou ameaças no processo, cuja função primordial é a de aquisição dos dados brutos, via observação de tráfego de redes, e recepção de logs de uso de ativos de rede conforme visto no nível 0 no trabalho de Tadda e Salerno [13]; relatórios de análises de vulnerabilidades de organismos ou entidades especializadas e confiáveis, nacionais ou internacionais; relatórios ou resultados de varreduras efetuadas pelos setores responsáveis internamente ao NuCDCAer, como scans de rede e testes de invasão (pentests); ou quaisquer notificações formais ou informais que possam ser de interesse da segurança ou da defesa cibernéticas;
2. Tratamento inicial (preliminar) dos dados de entrada para que possam ser qualificados e endereçados aos três macroprocessos principais de CSC, conforme o nível 1 em Tadda e Salerno [13];
3. Processos de Gestão de Incidentes de Rede: este macroprocesso é o responsável por receber as informações sobre tráfego de redes, via espelhamento e direcionamento para ativos de rede especializados na análise e detecção de anomalias, além da recepção e análise automatizada de logs dos demais ativos de rede configurados e sob responsabilidade do NuCDCAer, conforme o normativo do COMAER ICA 7-42 item 4 [87]. Geram alertas, tickets de incidentes de rede (formalizações técnicas dos incidentes) e envolvem o uso de equipes especializadas, conhecidas como equipes de tratamento de incidentes de rede (ETIR), espalhadas nas diversas organizações do COMAER. A saída deste processo é composta pelos tickets de incidentes de rede, relatórios de tráfego anômalo, estatísticas diversas sobre as detecções e incidentes e, finalmente o Índice de Incidentes Cibernéticos (IIC), um dos subíndices que compõem o Nível de Alerta Cibernético ao final de todo o processo de CSC;
4. Processos de Inteligência de Ameaças: processo de análise, por meio da avaliação constante do EC, a fim de se identificarem atores adversos e suas técnicas, táticas e procedimentos. São condizentes com o nível 1 sob a ótica de Tadda e Salerno [13], com fontes que podem situar-se em notícias ou informes de ameaças potenciais ou ataques em andamento em organizações diversas. Podem, inclusive ser identificadas via mídias sociais e noticiários jornalísticos, consideradas como inteligência de fontes abertas (Open Souce Intelligence – OSINT) conforme os trabalhos de Evangelista et al. [88] e Glassman [89]. Para que se identifiquem ameaças, deve ser utilizado um processo que passe pelas seguintes fases: planejamento, para determinar a informação a ser obtida e as fontes de dados a serem buscadas; coleta, tratamento e armazenamento de dados; validação de dados, análise e geração de informações; e disseminação das informações aos interessados, o que remete à fase 2 do trabalho de

Tadda e Salerno [13]. Os produtos finais deste processo são reportes de inteligência de ameaças e o Índice de Ameaças Cibernéticas (IAC); e

5. Processos de Gestão de Riscos Cibernéticos: O Índice de Riscos Cibernéticos (IRC) é obtido por meio da realização do processo de avaliação dos riscos sobre um ativo ou serviço, onde reforça-se que, para a geração do IRC, o escopo do processo limita-se a prosseguir até a etapa de avaliação dos riscos, quando os riscos identificados e analisados são organizados em gradação de intensidade e os mais críticos são evidenciados.
6. Processo de Aquisição/Gestão de CSC: processo que inclui a condensação das informações dos índices dos outros grupos de processo e sua interpretação com o objetivo de geração do índice NAC, de relatórios diversos sobre os riscos aos ativos e serviços, bem como o painel (*dashboard*) visual do estado de riscos do EC de interesse do COMAER.

5.2.3 Exame dos procedimentos de cálculo do NAC

Conforme exibido na Figura 5.2, o processo de obtenção de consciência situacional cibernética utilizar-se-á de três índices (IIC, IAC e IRC) para se obter uma medida da propensão do espaço cibernético de interesse à concretização de ameaças.

Essa medida citada no parágrafo anterior servirá de base para a autoridade competente determinar o Nível de Alerta Cibernético (NAC). Dessa maneira, o processo de obtenção de consciência situacional cibernética calculará o NAC segundo a fórmula 5.1:

$$NAC = [\max(IIC, IAC) + IRC]/2 \quad (5.1)$$

Na fórmula 5.1, é calculado o valor máximo entre os índices IIC e o IAC, que mede a probabilidade de existência de atores adversos. Em seguida, esse valor máximo é correlacionado com o índice IRC, que reflete a suscetibilidade do EC da Força em ser explorado. Com isso, obtém-se uma medida da propensão de concretização de ameaças no espaço cibernético de interesse, visto que é necessária a combinação de atores mal-intencionados com a existência vulnerabilidades para que a ameaça se concretize.

Uma vez conhecidos os Níveis de alerta cibernéticos, faz-se necessário aprofundar o entendimento sobre a gestão dos riscos cibernéticos e como ela será obtida, bem como os detalhes, as entradas, e o uso de uma ferramenta auxiliar para facilitar a obtenção do IRC, o que será demonstrado na etapa 3.

5.3 Estabelecimento do processo de Avaliação de Riscos Cibernéticos para o NuCDCAer

A função da gestão de riscos para o NuCDCAer é estabelecer o suporte para a defesa cibernética dentro de sua área de atuação, definida como sendo, primariamente, o espaço cibernético de interesse para a Força Aérea Brasileira, também denominada Comando da Aeronáutica (COMAER). A segunda função básica desta organização é compartilhar as informações de seu trabalho com o órgão superior da defesa cibernética do Brasil, o Comando de Defesa Cibernética (ComDCiber). Este compartilhamento não é direto ou instantâneo, devendo passar pela cadeia hierárquica de comando dentro da Força Singular (COMAER), pois há informações de uso exclusivo interno ao COMAER.

Neste tópico foi mantida a denominação de gestão de riscos cibernéticos para que a compreensão aconteça de forma ampla na aquisição de consciência situacional cibernética e nas atividades de defesa cibernética, as quais necessitam de uma visão completa do processo de gestão de riscos, conforme a ABNT NBR ISO/IEC 27005:2019 [3]. Porém para a geração do processo de avaliação de riscos cibernéticos e o resultante índice de riscos cibernéticos prescinde-se do processo completo e se limita até a fase de avaliação dos riscos, motivo pelo qual foi cunhado o acrônimo ARCiber, representando o processo de avaliação de riscos cibernéticos. Por avaliação de riscos compreende-se um macroprocesso constituído por identificação, análise e avaliação dos riscos, conforme o processo constante na ABNT NBR ISO/IEC 27005:2019 [3].

Para a correta operacionalização da função operacional do NuCDCAer, faz-se necessário compreender que há uma necessidade e uma dependência da capacidade de aquisição de consciência situacional cibernética (CSC), a qual se constitui em um processo que ultrapassa os limites do escopo deste trabalho, mas que será citado para o entendimento dos compromissos de um processo de avaliação de riscos em relação à sua composição. Neste contexto, foi mantido exclusivamente neste tópico, o termo mais abrangente, o de gestão de riscos cibernéticos (GRCiber) que estende a avaliação de riscos cibernéticos, conforme a ABNT NBR ISO/IEC 27005:2019 [3], como já citado anteriormente no item 3.3. Isto corresponde a entender que a CSC é um componente crucial para a tarefa da organização e para tal será explicada a seguir.

5.3.1 Seleção do modelo de gestão de riscos cibernéticos

O processo completo de gestão dos riscos cibernéticos inclui as seguintes fases: definição do contexto, identificação, análise e avaliação de riscos, tratamento, aceitação, comunicação e

análise crítica periódica para melhoria do processo como um todo, conforme a ABNT NBR ISO/IEC 27005:2019 [3], motivo pelo qual foi selecionado como ponto de partida para o entendimento de como se processa sua especialização em gestão de riscos cibernéticos.

Após a contribuição de REFSDAL e STØLEN [42] sobre a gestão de riscos cibernéticos, foi criado um diagrama de processos com a união das abordagens destes autores e da ABNT NBR ISO/IEC 27005:2019 [3], permitindo a seleção dos processos que compõem a avaliação dos riscos cibernéticos, necessária para a tarefa do NuCDCAer no foco desta pesquisa, ou seja, o processo de avaliação de riscos cibernéticos (ARCiber) para gerar o IRC e conseqüentemente o NAC. A seqüência de funcionamento é ilustrada pela Figura 5.3.

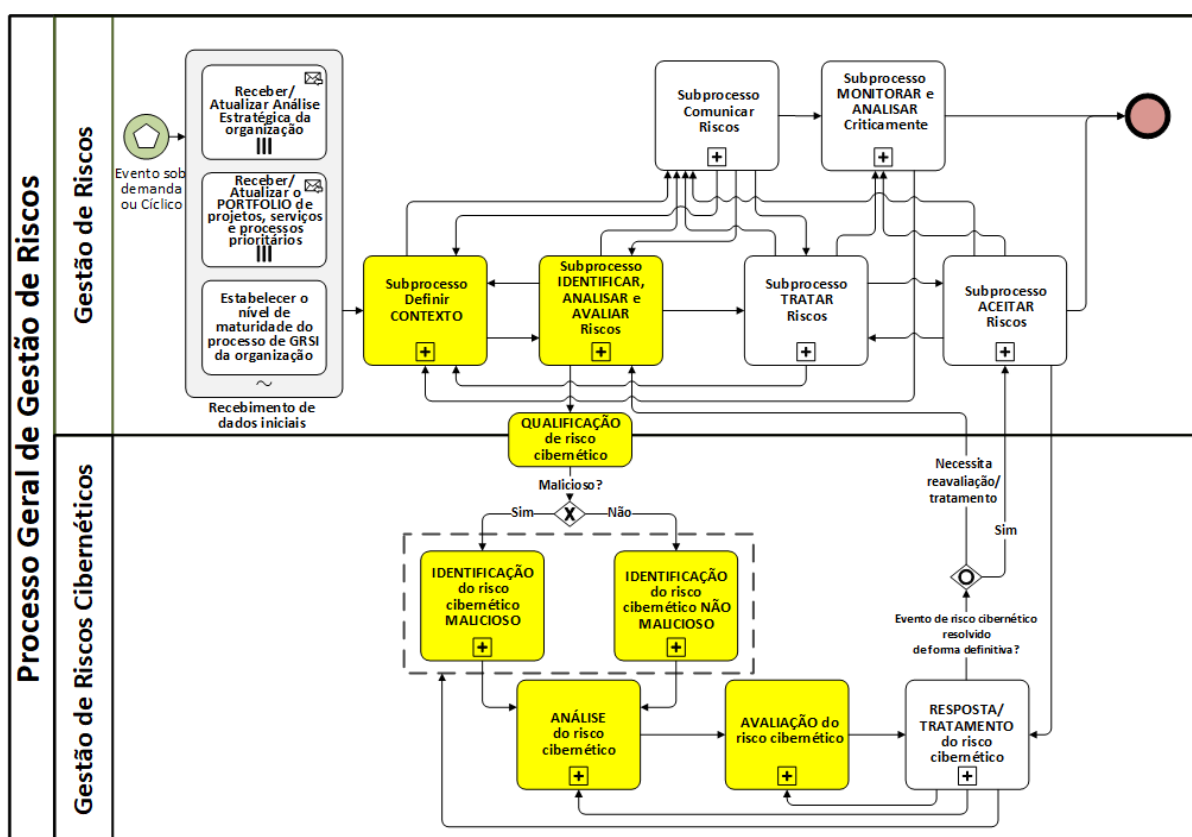


Figura 5.3: Processo de Avaliação de Riscos Cibernéticos

Fonte: adaptado de ABNT NBR ISO/IEC 27005:2019 [3] e REFSDAL e STØLEN [42]

Os subprocessos específicos componentes do processo de Avaliação de Riscos Cibernéticos (ARCiber) são aqueles grifados em amarelo. O conjunto completo compreende os processos que estendem o entendimento além do escopo da pesquisa, compondo o processo completo de Gestão de Riscos gerais e Cibernéticos, mantidos para estabelecer um foco

didático e visual sobre o tema abrangente de Gestão de Riscos. O processo ARCiber terá os seus subprocessos definidos a seguir.

Subprocesso Definir Contexto

A gestão de riscos (geral ou de ativos) parte da qualificação de todo o ambiente estratégico da organização, de forma pormenorizada, conforme o processo constante na norma ABNT NBR ISO/IEC 27005:2019 [3], com a identificação dos objetivos estratégicos da organização, definição de apetite ao risco, das tabelas de risco, seguida da definição do contexto, com a criação de um inventário minucioso de todos os ativos de informações importantes ao negócio da organização, qualificação dos mesmos quanto ao tipo, importância ao processo e suas dependências em relação a outros ativos e processos.

O três próximos processos (Identificar, Analisar e Avaliar Riscos) estão representados no gráfico como um único macroprocesso, conforme exposto na norma ABNT NBR ISO/IEC 27005:2019, mas serão aqui desmembrados para melhor entendimento individual de suas funções.

Subprocesso Identificar Riscos

Após este definir o contexto de riscos, são executados processos de identificação de ameaças e vulnerabilidades possíveis aos ativos e os consequentes níveis de probabilidade e impacto, para a criação de uma lista decrescente de riscos, com uma análise criteriosa e a geração dos planos de tratamento e aceitação dos riscos segundo a ABNT NBR ISO/IEC 27005:2019 [3].

A gestão de riscos gerais, segundo a ABNT NBR ISO/IEC 27005:2019 baseia-se na análise dos riscos identificados por sua probabilidade de ocorrência e por seu impacto ao ativo, dados nem sempre de fácil obtenção quando se trata de riscos cibernéticos, pois, segundo Kaffenberger e Kopp [90], informações sobre os tipos de atacantes responsáveis pelas ações cibernéticas de ataque podem ser classificados como: criminosos, hactivistas e insiders (atuantes internos, como inimigos infiltrados ou funcionários descontentes, entre outros tipos de público interno às organizações) com ataques de baixa até alta complexidade; Atores de ciber ataques, além dos anteriormente mencionados, acrescidos daqueles que agem sob procuração, ou em função de outros (proxy actors), que podem agir como soldados mercenários para patrocinadores que podem ser concorrentes, governos ou grupos de pessoas; e ataques promovidos por Nações ou Estados com interesses estratégicos, geopolíticos ou de espionagem, conduzidos por suas estruturas internas de defesa/guerra

cibernética ou os já citados mercenários.

Estes atores estabelecem a necessidade de uma análise de interesses e/ou patrocínios, os quais podem aumentar significativamente a complexidade de se estabelecerem critérios de probabilidade, pois um fato reconhecidamente relevante nos conflitos de qualquer tipo, descritos há mais de 2000 anos por Sun Tzu em seu livro “A arte da Guerra” [91] é o de que conhecer seu inimigo e conhecer seu próprio potencial é preponderante em se alcançar a vitória na guerra. Logo, ataques cibernéticos já foram citados neste trabalho e configuram uma estrutura de conflito muito similar ao combate militar, excetuando-se por, normalmente, não incluir diretamente armamento bélico tradicional, o que torna a análise do inimigo igualmente crucial.

Kaffenberger e Kopp [90] citam o significativo nível de incertezas que os ataques cibernéticos podem provocar, resultando no desafio da identificação dos impactos potenciais diretos e indiretos. Desta forma, os mesmos autores alegam ser muito produtivo o uso de cenários de risco como forma de estabelecer uma análise mais prática dos níveis de risco a que os ativos pode estar sujeitos. Fato este que evidenciou a busca por esta forma de análise e avaliação dos riscos para o processo em desenvolvimento neste trabalho.

Subprocesso Analisar Riscos

Conhecidos os valores de vulnerabilidades a serem investigadas, volta-se a atenção no processo a ser usado para a comparação entre o valor de criticidade da vulnerabilidade e os controles que podem estar implementados no ativo em análise.

A maior dificuldade encontrada é que os incidentes cibernéticos decorrentes da concretização de ameaças cibernética possuem grandes incertezas, dificultando a estimativa das probabilidades de um evento de risco ocorrer e de seu impacto. Segundo Li et al. [92] lidar com ameaças cibernéticas é algo inevitável e impreciso, havendo a necessidade de se confiar em cada informação para tentar detectar um ataque real e prevenir seus impactos, promovendo o melhor gerenciamento de riscos possível. Isto pode ser interpretado de forma que alguns alertas como falsos positivos podem ocorrer, e deverão ser tratados, como, por exemplo respostas de sistemas IPS ou alertas dos IDS e podem representar o nível de incertezas na interpretação destes alertas.

Segundo Paté-Cornell et al. [93] o gerenciamento de riscos cibernéticos pode ter um foco nas respostas possíveis que os tomadores de decisão das organizações podem lançar mão, podendo estas Respostas serem consideradas como contramedidas, como adição de criptografia, dispositivos de filtragem de tráfego como firewalls, IDS e IPS, detecção de malwares, compartimentalização etc. Há outras que podem ser consideradas como medidas administrativas, como identificação de implicações legais decorrentes dos incidentes

ou planejamento de continuidade como garantia do funcionamento em caso de problemas, garantindo alguma produtividade e manutenção mínima do funcionamento em caso de necessidade de resiliência cibernética.

Estas informações condizem com a metodologia e análise de ataques cibernéticos da publicação do NIST, o Cybersecurity Framework [66], citado no trabalho de Paté-Cornell et al. [93], cujos princípios são: identificar, proteger, detectar, responder e recuperar.

Cabe ressaltar que estes princípios e ações fazem parte de outros frameworks e métodos em cibersegurança, como o do MITRE Att&ck [63] (acesso inicial, execução, persistência, escalção de privilégios, evasão das defesas, acesso a credenciais superiores, descoberta de dados de interesse, movimento lateral na rede, coleção de dados de interesse, comando e controle da estrutura, exfiltração da rede e impacto ao alvo atacado), Cyber Kill Chain [94] (reconhecimento, armamento e alvo, entrega, exploração, instalação do malware, comando e controle para manipulação remota, ações sobre o objetivo), além do mais específico destes, o MITRE D3fend [64] (endurecer, detectar, isolar, enganar e despejar), criado para facilitar não o entendimento do ataque, mas diretamente a defesa e é alinhado aos processos e técnicas do MITRE Att&ck. O ponto em comum entre estes frameworks é que buscam padronizar o entendimento das ações em segurança cibernética, tanto sobre os ataques quanto sobre as contramedidas possíveis, o que permitiu a compreensão das necessidades que o processo de avaliação de riscos para o NuCDCAer precisa satisfazer.

Paté-Cornell et al. [93] ilustram ainda que estas atividades podem ser subdivididas em cenários de riscos para análise de suas contramedidas porventura existentes. Cenários como os definidos por Kaffenberger e Kopp [90] observando a escala e o *timing* do acontecimento, sobre como podem influir no impacto da ocorrência e da mesma forma sobre as características das defesas, em termos de tamanho e tempestividade. Sobre a escala do ataque Kaffenberger e Kopp observaram 5 tipos de cenários: cenário único massivo; múltiplos cenários massivos; múltiplos cenários de ataque de pequena monta simultaneamente; múltiplos cenários de pequena monta distribuídos no tempo; poucos cenários em estreita sucessão simultânea com efeitos em cascata, promovendo uma visão dos impactos que cada tipo de cenário pode ocasionar. Esta análise permite que se possa ter uma ideia de como interpretar os riscos com base em visões predefinidas (cenários ou controles), motivo pelo qual foi adicionada a este trabalho, como forma de enriquecer o processo por estabelecer uma medida prática de avaliação dos riscos cibernéticos para as necessidades da organização.

Subprocesso Avaliar Riscos

Para a avaliação dos riscos, segundo a ABNT NBR ISO/IEC 27005:2019 [3], deve-se

organizar os riscos em ordem decrescente de valor, de forma que os maiores fiquem no topo da lista de riscos. Para o processo do NuCDCAer, só há a necessidade de se estabelecer qual é o maior valor encontrado, não se necessitando descrever o risco. Para tal será desenvolvido, na ferramenta de cálculo, a avaliação automática e identificação do maior valor numérico de risco (neste caso o risco residual, após a análise e comparação com os controles/cenários).

Subprocesso Qualificação de Risco Cibernético

Relembrando que a abordagem da gestão de riscos cibernéticos se dá de uma forma um pouco mais prática, durante a identificação dos riscos, onde um risco pode ser evidenciado como risco cibernético, quando sua origem (ameaça) é advinda do espaço cibernético conforme a Doutrina Militar de Defesa Cibernética [7] e REFSDAL e STØLEN [42], tendo seu processo de identificação, análise e avaliação redirecionado para a gestão de riscos cibernéticos.

Identificação do Risco Cibernético Malicioso ou Não-malicioso

Segundo REFSDAL e STØLEN [42] há dois motivos básicos que distinguem os riscos para ativos cibernéticos de riscos considerados gerais: o primeiro é ligado ao alcance da ameaça, que pode ser originada à distância e com participação de agentes em escala global; o segundo diz respeito à fonte da ameaça, a qual pode ser dividida em ameaça de fonte maliciosa e ameaça de fonte não-maliciosa (ou acidental).

Ao chegar no processo de identificação dos riscos, este pode ser qualificado como risco cibernético e então pode ser adotada a forma identificada no trabalho de REFSDAL e STØLEN [42], Figura 5.3, onde o risco sofrerá a identificação de sua fonte de ameaça (maliciosa ou não-maliciosa), como na Figura 5.4, com prosseguimento para a etapa de análise (da criticidade da ameaça).

Análise do Risco Cibernético

Para uma correta avaliação dos riscos, segundo Doynikova e Kotenko [95], deve haver uma consecução dos seguintes estágios: reunião dos dados de entrada como matéria-prima básica da avaliação; seleção de uma técnica de avaliação de riscos que dependerá do tipo de ativo, bem como dos dados de entrada; e, finalmente, cálculo do nível de risco, fato este que corrobora a escolha, neste trabalho, da diferenciação dos riscos em cibernéticos e não cibernéticos (ou de riscos gerais a ativos).

Para o cálculo do risco cibernético Doynikova e Kotenko [95] estabelecem o uso do framework CVSS (Common Vulnerabilities Scoring System) [20], o qual permite uma identificação preliminar de valor de criticidade de vulnerabilidades, com equações que consideram a probabilidade e o impacto das ameaças e suas correlações com os riscos baseado em perguntas (configurando-se cenários), sendo o CVSS uma iniciativa da organização sem fins lucrativos com sede nos EUA, o *Forum of Incident Response and Security Teams* (FIRST.org).

Este framework é usado para análise das vulnerabilidades detectadas e catalogadas pelo serviço *Common Vulnerabilities Datasource* (CVEDetails) [96], o qual possui reportes de vulnerabilidades para divulgação.

O CVSS [20] possui três grupos de métricas: Básicas ou de base, Temporais e Ambientais. O valor padrão de vulnerabilidades divulgado pelos bancos de dados de vulnerabilidades leva em conta, exclusivamente as métricas básicas, sendo as outras de utilização adicional sob decisão de cada usuário avaliador. Para o processo de ARCiber do NuCD-CAer esta ideia será levada em conta na criação da ferramenta de cálculo do IRC.

Os subprocessos de identificação dos componentes dos riscos maliciosos e não maliciosos identificam uma variação na sequência de abordagem para geração do modelo do risco que será usado para alterar a ordem de busca, segundo REFSDAL e STØLEN [42], tornando mais lógico e eficaz o processo e permitindo a criação de um modelo de risco, usado como subsídio para a análise, avaliação e tratamento do risco cibernético. Estes subprocessos estão explicitados na Figura 5.4.

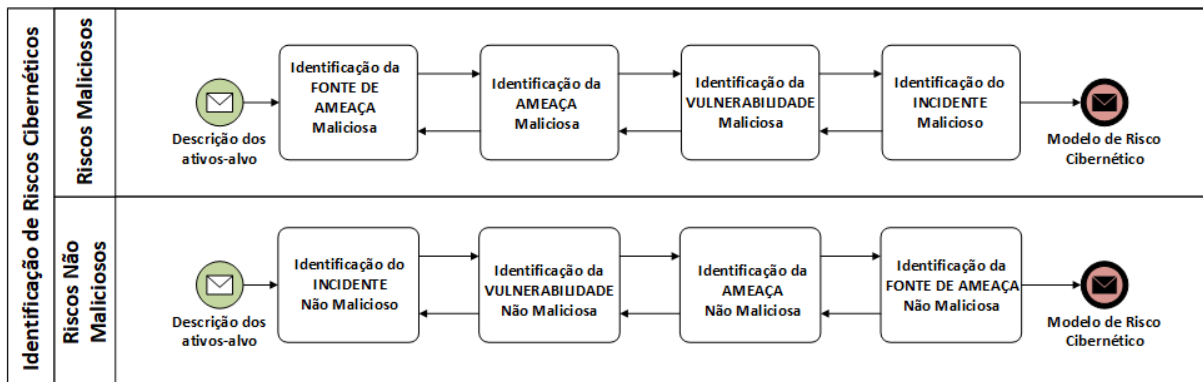


Figura 5.4: Subprocessos de identificação de riscos cibernéticos maliciosos e não maliciosos
 Fonte: adaptado de REFSDAL e STØLEN [42]

Há também o recebimento de reportes de possíveis ameaças via serviços de inteligência de ameaças, cujos relatórios levam à identificação de vulnerabilidades que podem ser

afetadas por estas ameaças e assim gerando-se listas de vulnerabilidades para análise via cenários de risco da organização de forma intempestiva e com necessidade de análise imediata.

Tais reportes são recebidos via serviços internos ao MD e ao Governo Federal como o CERT.br, setores de inteligência e monitoramento das Forças Armadas, como também pode ser obtidos por serviços externos ao governo e ao país, advindo de empresas como os fabricantes de soluções contra malwares e produtores de software como os sistemas operacionais, sendo exemplos o Kaspersky Resource Center [97], McAfee Enterprise Threat Center [98], Microsoft Security Blog [99] em seus blogs, alertas e relatórios regulares; serviços de divulgação e alertas de vulnerabilidades como o Common Vulnerabilities Database (CVEDetails) [96], National Vulnerabilities Database (NIST NVD) [100], Cybersecurity Infrastructures Security Agency Alerts (CISA Alerts) [101], Center for Internet Security Cybersecurity Threats (CIS CT) [102]. Estes serviços fornecem importantes informações acerca de vulnerabilidades e/ou ameaças e são de uso livre, com alguns como o do NIST (NVD), o CVEDetails fornecendo listas com vulnerabilidades analisadas. Os outros fornecem avisos e notícias mais pontuais e dependem de algum retrabalho para identificação dos níveis de riscos divulgados, sendo, em quaisquer dos casos de importância fundamental na tarefa de proatividade e tempo de resposta por parte de equipes de gestão de riscos e de incidentes.

Identificou-se, pelo processo de CSC do NuCDCAer e pela pesquisa em si, que outra importante fonte de informações acerca de riscos reais ou potenciais é obtida por meio da análise dos tráfegos de rede pelos setores ou equipes de tratamento de incidentes de rede (ETIR). Após análise destes dados pode-se inferir possíveis agressões ao espaço cibernético utilizado pela organização ou indícios de tráfego malicioso ou de assinaturas de possíveis ataques em preparação ou em andamento, conforme descrito e estabelecido na Norma Complementar nº 8 da Instrução Normativa Nº 1 do Gabinete de Segurança Institucional da Presidência da República (NC 08/IN01/DSI/GSIPR) [103] que versa sobre diretrizes para gerenciamento de incidentes em redes computacionais dos órgãos da APF.

Todas estas informações geram listas de vulnerabilidades que podem ser exploradas e assim provocarem impactos à organização. Estes conhecimentos obtidos geram as informações de entrada para o processo de gestão de riscos cibernéticos.

5.3.2 Desenho do processo de Avaliação do Risco Cibernético para o NuCDCAer

Compreende-se, por análise da avaliação dos riscos em geral, que este subprocesso acontece sob a mesma técnica, ou seja, os riscos cibernéticos serão ordenados de forma decrescente de seus valores obtidos durante a fase de análise de riscos cibernéticos. Esta lista ordenada permite a indicação do maior valor encontrado de forma a compor as fórmulas de cálculo do Nível de Alerta Cibernético.

Para uma compreensão mais adequada e visual do processo ARCiber, segue a figura 5.5 para observação:

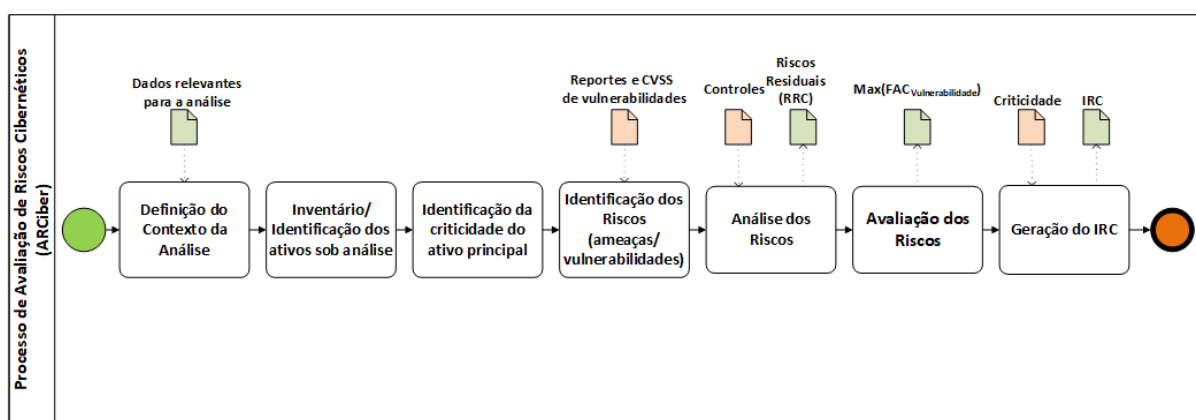


Figura 5.5: Diagrama do Processo de Avaliação de Riscos Cibernéticos do NuCDCAer
Fonte: autoria própria

Em resumo, para estabelecer o processo de avaliação de riscos cibernéticos da organização, diversos fatores devem ser levados em consideração:

- 1) Definição do Contexto da Análise: Para que se estabeleça uma avaliação adequada, e de acordo com o processo definido para a gestão completa dos riscos gerais e cibernéticos exibido na Figura 3.7 necessita haver uma correta identificação do contexto da análise, de acordo com os ativos reportados como vulneráveis, sendo da organização ou de fora desta, quando houver demanda de análise externa, conforme a norma ABNT NBR ISO/IEC 27005 [3] em seu item 7;
- 2) Inventário/Identificação dos ativos sob análise: Após a identificação do contexto da avaliação, devem ser conhecidos os ativos a serem analisados, conforme a norma ABNT NBR ISO/IEC 27005 [3] em seu item 8.2.2, quer tenham sido evidenciados por reportes de ameaças ou vulnerabilidades, testes de penetração ou escaneamentos

de rede, quer tenham sido indicados pela Subdivisão de Segurança da Informação, em virtude de serem considerados ativos críticos para os objetivos estratégicos da organização;

- 3) Identificação do valor de criticidade do ativo agregador/principal da análise: Após a seleção do ativo para análise, faz-se necessário conhecer nível de criticidade do ativo em relação à importância estratégica para a organização. Este valor indicará, de acordo com a definição do triângulo do risco, no item 3.3 deste trabalho o valor da criticidade do ativo, independentemente de seu valor monetário, pois será um fator multiplicador do risco, indicando que um ativo de alto valor estratégico para uma organização deve ter seu valor de risco proporcional à sua importância, e consequentemente sua proteção deve ser proporcional ao seu valor estratégico. Nesta fase será identificado o ativo agregador, ou seja, quando um ativo como um serviço é composto por diversos outros ativos, o valor de criticidade será dado ao ativo que reúne os outros. Como, por exemplo, um serviço de controle de estoque pode ser composto por diversos ativos, como servidor de aplicações, servidor web, sgbd, dispositivos de controle de acesso, etc. O valor da criticidade é o da importância estratégica do serviço, e não de qualquer ativo individual. Ou seja o valor de criticidade será o do ativo Controle de Estoque, que corresponde a um serviço ou sistema.
- 4) Identificação dos Riscos (ameaças/vulnerabilidades): Conhecido o valor estratégico do ativo faz-se necessária a coleta de possíveis vulnerabilidades ou ameaças, para que se possa compreender o universo de riscos a que o ativo pode estar submetido. Neste caso, cabe a comparação com o trabalho de Tadda e Salerno [13] em seu nível 0 onde se gerenciam as fontes de dados e a qualidade dos dados em si, com possível necessidade de tratamento destes dados brutos para que se transformem em informações úteis, além do nível 1 dos mesmos autores em função da percepção da pertinência das vulnerabilidades em relação aos ativos. As fontes de informações podem ser bastante diversas, como o tráfego de redes, onde a equipe de tratamento de incidentes de redes (ETIR) pode fazer análises diversas, como o uso do framework CVSS [20] para inquirição do valor de criticidade da vulnerabilidade; podem ser também advindas de solicitações de testes de vulnerabilidades em ativos (pentests), cujos resultados comumente já são configurados no padrão do CVSS, e cuja operacionalização pode ser efetuada pela equipe de gestão de vulnerabilidades (STD); ou podem advir de informes de serviços especializados em análises de ameaças (inteligência de ameaças) cuja operacionalização ficaria a cargo da equipe de inteligência de ameaças (IAC). Esta última fonte de dados pode necessitar de manipulação dos dados para

interpretação de ameaças ou vulnerabilidades reportadas e sua consequente análise via CVSS para composição de um valor objetivo de criticidade.

- 5) Análise dos Riscos (identificação dos cenários/controles): Conhecidas as vulnerabilidades, precisam ser estabelecidos cenários ou controles, como os evidenciados por Paté-Cornell et al. [93], para comparação de cada vulnerabilidade do ativo analisado com o a presença dos controles em maior ou menor grau, de forma a serem estabelecidos, qualitativamente, valores que indiquem ter a vulnerabilidade maior ou menor propensão de atingir o ativo neste quesito específico. Neste caso, leva-se em conta o trabalho de Radanliev [104] no qual há a evidenciação de que o risco residual corresponde ao risco inerente (valor bruto da vulnerabilidade), com a redução promovida pelos controles efetivos implementados (escala de valores dos controles/cenários), conforme a Fórmula 5.2:

$$RRC = RI * CE \tag{5.2}$$

Onde: RRC significa o risco residual cibernético; RI significa o risco inerente (valor bruto da vulnerabilidade, em valores da escala do CVSS); e CE significa o valor do controle efetivo (obtido da análise da relação dos controles do ambiente em relação à vulnerabilidade em foco), escolhido pelo analista em função de uma escala de eficácia do controle em relação à vulnerabilidade. Esta fórmula representa o quanto uma vulnerabilidade pode ter sua criticidade variada em função da presença ou ausência de controles mitigantes. Esta fórmula evidencia a interação de uma única vulnerabilidade com um único controle, fornecendo um valor de mitigação para esta relação vulnerabilidade/controlado/ativo único.

- 6) Análise dos Riscos (Comparação com os cenários/controles): Após o estabelecimento dos cenários/controles para análise das vulnerabilidades, estas devem ser comparadas com cada controle e deve ser escolhido um valor que corresponda ao nível do controle que o ambiente sob análise possui. Esta seleção vai evidenciar se o ambiente possui ou não proteção ou contramedidas adequadas à ameaça ou à vulnerabilidade em análise. Neste caso, o valor final da mitigação dos controles em relação à vulnerabilidade em foco será representado pela média aritmética dos valores mitigados (RRC) por todos os controles analisados. Para esta fase o trabalho de Tadda e Salerno [13] em seu nível 2 estabelece o princípio da compreensão da situação atual, com a comparação entre as vulnerabilidades e os controles permitindo a avaliação da situação atual.

- 7) Análise dos Riscos (Cálculo do Risco Residual): Para que haja a correta avaliação dos riscos, necessita-se que seja calculado o RRC de cada vulnerabilidade, levando-se em conta todos os controles analisados para cada vulnerabilidade. Este valor evidenciará se a presença de controles adequados reduziu o valor do risco inerente ou se a ausência destes controles possibilitou um aumento do risco inerente, configurando, em ambos os casos o risco residual daquela vulnerabilidade em relação aos controles. Para esta fase o trabalho de Tadda e Salerno [13] em seu nível 3 estabelece o princípio da compreensão da situação futura, quando uma interpretação do nível de risco residual em relação ao risco inerente permite uma identificação a partir de visão de futuro possível (nível de risco inerente) uma visão de futuro plausível (risco residual). O resultado será o valor FAC (Fator de Ameaça Cibernética) de uma vulnerabilidade, representado pela Fórmula 5.3:

$$FAC_{Vulnerabilidade} = \frac{\sum RRC}{qtdControles} \quad (5.3)$$

Onde: $FAC_{Vulnerabilidade}$ significa a média dos riscos residuais cibernéticos; RRC significa o risco residual cibernético de uma única vulnerabilidade com um único controle; e qtdControles significa a quantidade de controles analisados, representando o divisor da média aritmética das mitigações. Esta fórmula representa o quanto uma vulnerabilidade pode ser mitigada pela presença de diversos controles no ambiente analisado.

- 8) Avaliação dos Riscos: A fase anterior gerará uma lista de valores de riscos residuais, e a função deste processo é estabelecer um nível de risco que identifique o nível necessário de proteção a ser solicitada. Para isto optou-se por uma abordagem conservadora, na qual as ações de proteção devem possuir capacidade de reagir ao maior risco encontrado. Logo, além da lista de valores individuais dos riscos residuais, o maior valor de risco para o ativo deverá ser identificado e registrado.
- 9) Geração do Índice de Riscos Cibernéticos: O maior valor de risco residual encontrado em cada ativo será enviado automaticamente para o gerador de relatório que fará a conciliação e retornará o maior valor encontrado entre todos os ativos da avaliação e multiplicará este maior valor de risco residual encontrado pelo valor de criticidade do ativo agregador, conforme descrito no item 3, pois, segundo a empresa Módulo Security Solutions S.A. em sua metodologia de GRC (governança, riscos e

compliance) aplicada ao software Risk Manager [105] o risco pode ser calculado segundo o critério de relevância do ativo, compondo o índice PSR (probabilidade, severidade/impacto e relevância) onde o valor do risco se encontra por meio da Fórmula 5.4:

$$Risco(PSR) = Probabilidade * Severidade * Relevância. \quad (5.4)$$

No caso do processo de avaliação de riscos/geração do IRC para o NuCDCAer, esta fórmula será usada com a seguinte fórmula 5.5:

$$IRC = \max(FAC_{vulnerabilidade}) * C \quad (5.5)$$

Onde: IRC significa índice de riscos cibernéticos, $IRC = \max(FAC_{vulnerabilidade}) * C$ significa o máximo valor de risco residual (risco inerente * controle) encontrado na avaliação entre todos os ativos do grupo e C significa o valor da criticidade do ativo agregador.

Esta asserção encontra eco em diversos órgão públicos pesquisados como os Tribunais Regionais do Trabalho da 3ª Região (TRT3), 4ª Região (TRT4), da 8ª Região (TRT8), da 11ª Região (TRT11) [106] do Tribunal de Justiça do Estado do Ceará (TJCE) [107], no Comando de Defesa Cibernética (ComDCiber), no Ministério da Saúde, via DATASUS [108];

Este valor final será indicado como o IRC desta análise e será categorizado e utilizado para a composição do NAC, em uma fase além dos propósitos desta pesquisa.

Estas fases devem servir de base para geração do índice de riscos cibernéticos (IRC) e para a criação de uma ferramenta computacional que permita a inserção dos dados dos componentes dos riscos (vulnerabilidades/ameaças incidentes) para a correta estimativa do nível de risco a que um ativo possa estar sujeito. Cabe ressaltar que este processo está sendo desenvolvido para ações de defesa cibernética, por órgãos governamentais, mais especificamente militares, com abrangência de ativos críticos de informação para as instituições estratégicas do país. A geração de um índice de comprometimento do espaço cibernético (NAC), conforme a Doutrina Militar de Defesa Cibernética fornecerá aos escalões de nível mais alto o subsídio para emprego do tipo de ação mais adequado a responder proporcionalmente ao índice estabelecido pelas avaliações.

Evidenciadas as necessidades do processo de avaliação de riscos cibernéticos, necessita-se agora descrever como ocorrerá o cálculo efetivo do índice de riscos cibernéticos (IRC),

para tal a próxima etapa permitirá esta compreensão.

5.4 Geração do processo de obtenção do IRC

Após as reflexões obtidas na etapa 3, com o entendimento de como o processo de avaliação de riscos deve ocorrer, se faz necessário refletir sobre os passos para a identificação e o cálculo do índice que representa o risco cibernético dos ativos dentro do espaço cibernético de interesse, estes riscos são adicionados à análise por formas diversas, como observado na etapa anterior, formando um valor de risco inicial, mas são comparados a controles que alteram positivamente ou negativamente estes valores de acordo com a presença ou ausência (parcial ou total) destes controles, formando um resultado básico de um risco calculado.

Para esta etapa faz-se necessário compreender quais parâmetros serão observados, quais controles serão analisados, e quais padrões consagrados se encaixam no processo do NuCDCAer de avaliação de riscos cibernéticos.

Compreensão do Índice de Riscos Cibernéticos - IRC

O valor do IRC, conforme o processo de avaliação de riscos demonstrado na etapa 3, via Figura 5.5, resulta do cálculo iniciado com o recebimento das vulnerabilidades por diversos meios (com valores de criticidade padronizados pela escala do CVSS) [20], as quais são confrontadas com controles mitigadores identificados, sendo analisadas estas relações sob a ótica de escala de valores de eficácia destes controles conforme descrito no Roteiro de Auditoria de Gestão de Riscos do Tribunal de Contas da União – TCU [109], oferecendo, como resultado um valor de risco calculado, observando o fator de mitigação da vulnerabilidade pelo controle.

Em seguida esta vulnerabilidade individual analisada é confrontada com os demais controles que representam o estado atual do ambiente de segurança da organização. Este ambiente compõe parte do espaço cibernético de interesse da organização e configura o quão preparada está para enfrentar as ameaças advindas do espaço cibernético que pode ter alcance global.

Ao estabelecer a análise dessa vulnerabilidade com todo o kit de controles disponível para este tipo de ativo, por meio de uma média aritmética dos valores de riscos calculados por cada controle, é estabelecido o valor do Fator de Ameaça Cibernética (FAC), nome aplicado ao risco residual desta vulnerabilidade após a mitigação do nível de risco pelos controles.

Para o estabelecimento do IRC será levado em conta os valores obtidos dos FAC de todas as vulnerabilidades identificadas para o ativo em análise, momento em que será identificado o de maior gravidade (maior nível numérico) para ser registrado como o FAC deste ativo específico. O IRC é um índice que mede o nível de risco cibernético do ativo denominado agregador (também denominado como sendo do tipo sistema, pelo NuCDCAer), pois pode ser composto por diversos outros ativos componentes, conforme Chiavenato [110]. Como exemplo pode-se pensar em um portal web corporativo que presta inúmeros serviços a uma organização, o qual é composto por inúmeros ativos como servidores, meios de comunicação, ativos de rede e de software, todos apontados, para avaliação de seu IRC sob o nome genérico de Portal Web da Organização.

Cada ativo componente será igualmente avaliado e seu FAC será registrado, até que o último ativo do grupo seja avaliado. Em seguida, de posse de todos os FAC dos ativos, será escolhido o de maior gravidade para ser multiplicado pelo valor de criticidade (estratégico) do ativo agregador (sistema, processo, serviço ou outra qualificação que denote ser um ativo de nível estratégico ao negócio da organização). Este valor de resultado será denominado índice de Risco Cibernético (IRC).

Após a compreensão de como se chegar ao IRC, resta compreender como foi o caminho para este índice.

Entrevista para Criação do IRC

Para a criação do IRC, compreendeu-se que havia a necessidade do entendimento sobre diversos fatores, como: identificação do contexto da organização cujos ativos estarão em análise; identificação das formas das entradas das vulnerabilidades; definição sobre os valores de criticidade possíveis para os ativos estratégicos sob análise; definição do formato padronizado dos valores das vulnerabilidades; decisão sobre um método ou framework que possa padronizar os processos de reconhecimento de ataques cibernéticos que possam ocorrer ou das defesas que se pode lançar mão; definição de cenários de risco com grupos de controles para avaliar o ambiente da organização quanto às ameaças possíveis; definição de controles específicos para os cenários identificados; confirmação (decisão) sobre a regra de cálculo para a geração dos FAC; e confirmação sobre a regra (fórmula) de geração do IRC.

A ferramenta identificada como adequada para a identificação, entendimento e seleção dos fatores de análise ou de ação sobre as vulnerabilidades foi o de entrevista ou reunião semiestruturada, que foi referenciada por Sonia Vieira [62] como sendo do tipo de procedimento de coleta de dados de forma qualitativa, baseada em ideias, juízos e opiniões, podendo possuir um roteiro delineador, mas com perguntas essencialmente abertas. Para

esta coleta foi escolhida a amostra das 10 pessoas com nível de liderança e conhecimento técnico sobre segurança/defesa cibernética, dentro da população da subdivisão de segurança da informação, cujos demais componentes possui perfil predominante de execução dos processos definidos por suas lideranças e com treinamento em nível operacional para suas áreas de ação.

Conhecer somente o processo de geração não ilustra a necessidade de comprovação das origens e importâncias das informações componentes. Necessita-se compreender que todo o processo adveio de uma combinação de ações conjuntas que foram iniciadas com uma entrevista semiestruturada, constante no apêndice C e no item 4.1 subitem V desta pesquisa, com os profissionais de nível estratégico da SDSI do NuCDCAer, que compreendem o negócio da organização e as implicações teórico-práticas da segurança ou defesa cibernéticas.

Análise da entrevista semiestruturada com os especialistas

(i) Respostas obtidas na parte 1 da entrevista semiestruturada com os especialistas

Como explicado anteriormente, esta parte da entrevista serviu para evidenciar aos entrevistados o caráter participativo necessário para o estabelecimento do processo de ARCiber. Por constar da entrevista, se faz necessário um resumo interpretativo das respostas oferecidas durante as entrevistas.

Para a primeira pergunta: "Por quê a informação é uma commodity para a atividade do NuCDCAer?"

Ficou evidenciado que a informação em vários níveis é o bloco de construção para os processos de segurança/defesa cibernéticas, pois é imprescindível para que sejam identificados, analisados e avaliados os componentes do risco cibernético, representando indiscutivelmente uma commodity para as atividades da organização.

Para a segunda pergunta: "Há uma definição clara sobre o contexto informacional para as atividades da organização?"

As respostas foram unânimes sobre a importância da criação do NuCDCAer, em virtude de sua missão e de advir da transformação funcional de uma organização (CCA-BR) cuja vocação era a de trabalhar em função da Tecnologia da Informação (TI) de uma maneira mais ampla, com desenvolvimento de aplicações, suporte técnico à plataformas de software, hardware e redes, além de ter sido escalada para garantir a segurança básica das redes via estabelecimento de um centro de tratamento de incidentes de redes (CTIR.FAB). Logo, há uma definição bem clara sobre

as necessidades e o contexto informacional necessário para as atividades da atual organização.

Para a terceira pergunta: "Por favor, cite 3 ou mais palavras que imediatamente lhe vem à mente em termos de fontes de informação que entende como confiáveis ou úteis para a consecução dos objetivos da atuação da organização ou de sua atividade."

As respostas mais recebidas como palavras que primeiro vêm à mente dos entrevistados foram: CVSS, NIST, MITRE, Cyber, Chain, Kaspersky, attack, defend, Oval, entre outras, ficando sua distribuição em termos de quantidade ilustrado na nuvem de palavras exibida pela Figura 5.6.



Figura 5.6: Nuvem de palavras que primeiro vêm à mente dos entrevistados em SC/DC
Fonte: autoria própria

Para a quarta pergunta do bloco: "Poderia discorrer, em poucas palavras como se processa a busca pelas informações em sua atividade (início, modo, utilização, dificuldades etc.)?"

As respostas diferiram de acordo com o foco de trabalho de cada participante, pois há os que lideram equipes de gestão de vulnerabilidades, com testes de penetração, escaneamentos de vulnerabilidades de rede, entre outras atividades deste tipo, cuja busca por informações é ativa e sob demanda; há os líderes de equipes que trabalham com gestão de incidentes de rede, cujo foco é a busca no tráfego corrente de rede e de logs de ativos em busca de assinatura de possíveis ataques ou de atividades anômalas ao tráfego normal da rede; outra atividade é a de gestão de ameaças com a busca em diversas fontes de consultas, inclusive as não especializadas em

segurança como o Twitter, mídias sociais diversas, sites de notícias, em especial sobre geopolítica e atividades ilegais, não descuidando inclusive de informes sobre a dark web com possíveis ameaças em curso pelo mundo; e finalmente a atividade que é executada *post mortem*, ou seja, após o fato ocorrido, em ativos afetados, neste caso a perícia forense, cuja busca de informações ocorre sob estrita demanda e autorização expressa para execução, com a finalidade de estabelecer indícios de crimes, bem como de investigação sobre as causas do ocorrido.

(ii) **Análise da Parte 2, Bloco B - A discussão sobre o framework de riscos**

Durante a pesquisa, e conforme os contatos com os especialistas durante as etapas anteriores, houve um consenso sobre a necessidade de se estabelecerem padrões de identificação, análise e avaliação dos riscos cibernéticos, o que se traduz em como compreender as implicações dos componentes do risco, como já descrito no item 3.3, Figura 3.3, ou seja, o entendimento de como as ameaças cibernéticas podem explorar vulnerabilidades presentes nos ativos expostos ao espaço cibernético de interesse.

Na etapa 3 foi discutido que há diversos frameworks de risco cibernético desenvolvidos por organizações e empresas com comprovada importância no tema segurança cibernética, como o National Institute of Standards and Technology (NIST) [111], The MITRE Corporation [112], e a Lockheed Martin (LM), cujas finalidades estão em compreender as ameaças representadas por atacantes diversos via espaço cibernético, tanto por examinar e qualificar as técnicas e métodos de ataque, quanto as técnicas e métodos que se pode empreender para a defesa preventiva e/ou corretiva dos possíveis ataques.

Os frameworks levantados na entrevista foram o NIST Cybersecurity Framework (NIST CSF), o MITRE Att&ck, o MITRE D3fend e o Lockheed Martin Cyber Kill Chain (LM CKC). Dentre estes o único exclusivamente voltado para técnicas de defesa cibernética é o MITRE D3fend, mas trabalha em conjunto e sob referências do MITRE Att&ck que possui a capacidade de analisar as técnicas de ataques cibernéticos; os outros dois, NIST CSF e LM CKC possuem capacidades tanto de compreender as técnicas de ataque quanto de defesa cibernéticas. O consenso entre os especialistas foi que o NIST CSF possui características mais voltadas para os processos em curso no NuCDCAer, e, portanto, será utilizado para identificar e diferenciar os cenários de risco para o processo de ARCiber da organização.

(iii) **Análise da Parte 2, Bloco C - A discussão sobre os grupos de controles e controles**

Conforme o t3pico anterior, o framework escolhido foi o NIST Cyber Security Framework (NIST CSF) e sua estrutura de an3lise e identifica3o de atividades de seguran3a (t3cnicas de ataque e defesa). Segundo o NIST CSF h3 5 fun3o3 b3sicas: Identificar, Proteger, Detectar ou Diagnosticar, Responder e Recuperar, conforme pode ser observado na Tabela 5.2. Dentro destas fun3o3 foram escolhidos grupos de controles e controles de acordo com as necessidades de identifica3o do ambiente da organiza3o avaliada em rela3o aos ativos ou processos sob an3lise.

Tabela 5.2: Fun3o3 e categorias do NIST CSF

Identificador exclusivo de fun3o	Fun3o	Identificador exclusivo de categoria	Categoria
ID	Identificar	ID.AM	Gerenciamento dos Ativos
		ID.BE	Contexto Empresarial
		ID.GV	Governan3a
		ID.RA	Avalia3o de Risco
		ID.RM	Estrat3gia de Gerenciamento de Riscos
		ID.SC	Gerenciamento de Riscos da Cadeia de Suprimento
PR	Proteger	PR.AC	Gerenciamento de Identidade e Controle de Acesso
		PR.AT	Conscientiza3o e Treinamento
		PR.DS	Seguran3a de Dados
		PR.IP	Processos e Procedimentos de Prote3o da Informa3o
		PR.MA	Manuten3o
		PR.PT	Tecnologia Protetora
DE	Detectar ou Diagnosticar	DE.AE	Anomalias e Incidentes
		DE.CM	Monitoramento Cont3nuo de Seguran3a
		DE.DP	Processos de Detec3o
RS	Responder	RS.RP	Planejamento de Resposta
		RS.CO	Comunica3o
		RS.AN	An3lise
		RS.MI	Mitiga3o
		RS.IM	Aperfei3oamentos
RC	Recuperar	RC.RP	Planejamento de Recupera3o
		RC.IM	Aperfei3oamentos
		RC.CO	Comunica3o3

Fonte: Adaptado de NIST CSF [66]

Os grupos de controles, durante a entrevista foram classificados como os seguintes: Entrada das vulnerabilidades (n3o se configura em controle, mas possui referenciamento importante no NIST CSF), An3lise da vulnerabilidade, Aspectos/Implica3o3

Legais, Ações de Resposta/Continuidade dos negócios, Proteção do Perímetro da Rede, Proteção da Aplicação, Proteção de Acesso à Sistema ou Serviço, e Proteção do Ativo/Serviço. O apêndice D possui uma tabela com descrição completa e as referências necessárias para a compreensão dos aspectos escolhidos para análise/avaliação do ambiente, conforme a Tabela 5.3.

Tabela 5.3: Agrupamentos de controles e controles para avaliação de riscos

Agrupamentos	Controles
Entrada das Vulnerabilidades	Criticidade da Vulnerabilidade
Análise da Vulnerabilidade	Tempo da Vulnerabilidade Limitação no escopo da análise
Aspectos/Implicações Legais	Impactos por Aspectos Legais Contratuais Logs
Ações de Resposta / Continuidade dos negócios	Impactos por Tempo de Recuperação Resposta aos Riscos / ETIR Plano de Continuidade Backup
Proteção de Perímetro da Rede	Firewall de Borda IPS/IDS
Proteção da Aplicação	Proxy Reverso Firewall de Aplicação web
Proteção de Acesso ao sistema ou serviço	Privilégios desnecessários Contas Desnecessárias Ativas
Proteção do Ativo / Serviço	Criptografia Portas abertas Nível de Exposição do ativo Homologação de Sigilo Proteção contra malwares Proteção física dos ativos

Fonte: Autoria própria

Entrada das vulnerabilidades

Há uma observação importante a ser discutida, em razão de as vulnerabilidades recebidas via reportes de serviços como o CVE ou outros similares já virem analisadas via padrões do CVSS e possuírem valores de criticidade que levam em conta algumas necessidades presentes em controles que a avaliação pelo processo do NuCDCAer irá reavaliar. Para esta característica não se deve confundir a análise da vulnerabi-

lidade em si com os controles presentes no ambiente analisado. Os reportes geram informações genéricas sobre a vulnerabilidade, enquanto a análise do ambiente traz informações específicas sobre a interação da vulnerabilidade com os controles presentes.

Caso a entrada de vulnerabilidades se dê por meio de escaneamento de vulnerabilidades de rede ou de testes de penetração diretamente em ativos, cujos relatórios são compatíveis com o padrão CVSS [20], estas poderão ter sido analisadas segundo as vulnerabilidades do ambiente, incluindo os controles presentes, sem que isso altere o resultado. Uma reanálise manual da vulnerabilidade confirmará o valor recebido ou o reduzirá em virtude de ter sido mais criteriosamente investigada com o olhar do analista, tendo por base sua experiência e amplitude de visão sistêmica do ambiente.

O importante é o estabelecimento do valor da vulnerabilidade, considerado o risco inicial ou inerente, para que seja analisado por cada controle e assim determinar se há mitigação deste valor inicial e em qual proporção de redução pelo controle.

Há referências no NIST CSF [66] que embasam a entrada das vulnerabilidades, via funções identificar (ID), proteger (PR) e detectar (DE), nas categorias avaliação de riscos (RA), processos e procedimentos de proteção da informação (IP) e monitoramento contínuo de segurança (CM).

Além do NIST CSF [66] identificou-se importantes recomendações via CIS Controls [113] em seu controle nº7, Gestão contínua de vulnerabilidades, bem como nas métricas-base do CVSS [20] e no MITRE D3fend em sua tática DETECTAR, com suas diversas técnicas disponíveis.

Análise da vulnerabilidade

Para este grupo de controles, foram identificados e definidos na entrevista, dois controles importantes, o tempo ou idade da vulnerabilidade e a existência de alguma limitação no escopo da análise. O tempo ou idade da vulnerabilidade foi entendido como o período em que a vulnerabilidade existe, como identificado nas métricas temporais do CVSS [20], cujas informações analisadas referem-se à confirmação da existência da ameaça e/ou maturidade de técnicas de exploração, divulgação de exploits para ataques, e a existência de patches de reparo ou remediação, reforçado pelas recomendações do NIST em sua publicação especial (Special Publication 800-53 Revision 4) [114], item RA-5, Escaneamento de Vulnerabilidades e pela norma ABNT NBR ISO/IEC 27001:2013 [36], em seu item A.12.6 (Gestão de vulnerabilidades técnicas).

Para o controle que observa se houve alguma limitação no escopo da análise da vulnerabilidade, a preocupação dos especialistas é identificar se, por algum motivo, a busca por vulnerabilidades sofreu alguma limitação técnica, legal ou por falta de permissão do proprietário do ativo. As referências técnicas são abordadas no NIST CSF [66] em suas funções de proteger (PR) e detectar (DE), nas categorias segurança de dados (DS) e monitoramento contínuo de segurança (CM).

Há também referência técnica via CIS Controls [113] em seu controle nº18, Testes de invasão, além do MITRE D3fend em sua tática DETECTAR, com suas diversas técnicas disponíveis.

Aspectos/Implicações Legais

Este grupo de controles foi levantado e definido pelos especialistas em função de implicações que vão além do escopo identificado pelo CVSS. A preocupação foi com as implicações legais, contratuais e registro de logs de atividades.

Para o primeiro controle, o qual se preocupa com impactos por aspectos legais estabeleceu-se que a norma ABNT NBR ISO/IEC 27001:2013 [36] em seu item A.18.1, conformidade com requisitos legais e contratuais, identifica os requisitos legais que se deve observar, pois há uma ameaça de judicialização que pode causar impacto financeiro e de imagem à organização. Com a edição da lei 13.709 (LGPD) [115] esta necessidade se acentuou, em função das exigências de proteção dos dados pessoais e preservação da privacidade das pessoas naturais.

Além destes argumentos o NIST CSF [66] possui referências diretas em sua função identificar (ID), na categoria governança (GV) que compreende políticas, procedimentos e processos para gerenciar os requisitos de conformidade em geral, em suas subcategorias: “ID.GV-1: A política organizacional de segurança cibernética é estabelecida e comunicada; e ID.GV-3: Os requisitos legais e regulamentares relativos à segurança cibernética, incluindo a privacidade e as obrigações das liberdades civis, são compreendidos e gerenciados” O segundo controle foi identificado pelos especialistas como sendo importante em função do tipo de organização (da Administração Pública Federal), muito atrelada a legislações restritivas e dependente de contratos bem redigidos. Neste caso a preocupação ocorreu em função da observância de alguma cláusula contratual que interfira em boas práticas de segurança cibernética. Seu embasamento técnico ocorreu via NIST CSF [66] em sua função identificar (ID), nas categorias governança (GV) e gerenciamento da cadeia de suprimentos (SC), em suas subcategorias: “ID.SC-3: Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender

aos objetivos do programa de segurança cibernética de uma organização e do Plano de Gerenciamento de Riscos da Cadeia de Suprimentos Cibernéticos.” Por último, mas não menos importante, os especialistas debateram sobre uma exigência da lei nº 12.965/14 [116], conhecida como Marco Civil da Internet, em seus artigos 10, 11 e 13, a qual exige coleta armazenamento e proteção de logs de acesso e uso de aplicações disponibilizadas na Internet, o que pode causar impacto legal à organização caso desrespeitada. Para este controle, diversas fontes legais e técnicas foram identificadas, à começar pela ABNT NBR ISO/IEC 27001:2013 [36], em seu item A.12.4 (Registros e monitoramento); pela lei 13.709 (LGPD) [115]; pela Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13/2013) [117] em seu anexo B, item 1.33; pela instrução Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações do Comando da Aeronáutica (ICA200-8) [118]; bem como pelo NIST CSF [66] em sua função proteger (PR), na categoria tecnologia protetora (PT).

Além do CIS Controls [113] em seu controle nº8 Gestão de registros de auditoria. Para este aspecto o Mitre D3fend não possui nenhuma referência.

Ações de Resposta/Continuidade dos negócios

Este agrupamento de controles é o que mais contém controles individuais, em virtude de possuir diversos aspectos a serem observados no ambiente, como: Impactos por tempo de recuperação, ou seja, quanto tempo o negócio da organização suporta ficar inativo sem que haja prejuízo catastrófico, referenciado pela ABNT NBR ISO/IEC 27001:2013 [36], em seu item A.17, que trata de aspectos da segurança da informação na continuidade dos negócios, e pela ABNT NBR ISO/IEC 22301: 2013 [119], a qual trata, em sua totalidade, da continuidade dos negócios. Há referências na Norma Complementar nº06 da IN01/GSIPR [120] que normatiza a atividade de continuidade dos negócios dentro da APF, além do normativo ICA7-1 [121], que trata de continuidade dos negócios dentro do âmbito da FAB.

E finalmente, o NIST CSF [66] também possui uma função identificar (ID) e uma categoria avaliação de riscos (RA).

O outro controle trata de resposta a incidentes de rede, observando a presença ou não de pessoal treinado para responder adequadamente a problemas relacionados a anomalias comportamentais do tráfego de rede (incidentes). É o controle com mais referências para ação desta pesquisa, possuindo indicações na Norma Complementar nº05 da IN01/GSIPR [122], que trata dos aspectos de criação e características necessárias a uma ETIR. Da Norma Complementar nº08 da IN01/GSIPR [103], que

trata das diretrizes para gerenciamento de incidentes em redes nos órgãos e entidades da APF. Da ABNT NBR ISO/IEC 27001:2013 [36], em seu item A.16, que trata da gestão de incidentes de segurança da informação. Via CIS Controls [113] em seu controle nº17, gestão de respostas a incidentes e da publicação especial do NIST (Special Publication 800-53 Revision 4) [114] em seu item IR-10 (Equipe de análise de segurança da informação integrada). Como referência básica (framework) escolhido pelos especialistas, o NIST CSF [66], nas funções identificar (ID), detectar (DE) e responder (RS).

Há um controle que verifica se há um plano de continuidade definido na organização, o que pode fazer toda a diferença em caso de incidente catastrófico. Sua escolha foi unânime e seu referenciamento já era de amplo conhecimento profissional dos especialistas, estando em normativos gerais e já citados como a ABNT NBR ISO/IEC 27001:2013 [36], em seu item A.17, e pela ABNT NBR ISO/IEC 22301: 2013 [119], Norma Complementar nº06 da IN01/GSIPR [120], e pela Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13/2013) [117], em seu item 3.11 (Plano de Continuidade dos Negócios) e ICA7-1 [121] em seu item 3.1.1. As referências no NIST CSF [66] se situam nas funções proteger (PR) e recuperar (RC).

Por último neste conjunto escolheu-se um quesito que deveria ser de suma importância, tantas vezes negligenciado por organizações, e que pode fazer a diferença em um incidente, as cópias de segurança ou backups.

Neste caso há a importância de se averiguar se existem, se estão completos e atualizados, além de serem testados para verificação de integridade, conforme a ABNT NBR ISO/IEC 27001:2013 [36] em seu item A.12.3 (cópias de segurança). Há referências internas à FAB na Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13/2013) [117], em seu item 3.11 e anexo J, itens f, g, h, i e j. Via CIS Controls [113] em seus controles nº3 Proteção de dados e nº 11 Recuperação de dados. Para o NIST CSF [66] as referências são encontradas em sua função proteger (PR).

Proteção do Perímetro da Rede

Para este agrupamento de controles levou-se em conta os critérios de proteção mais óbvios para profissionais de segurança de redes e afins, ou seja, a presença e o estado de configuração de ativos de rede cuja função é a de trabalharem como filtros do tráfego da rede.

Buscou-se aferir a situação de firewalls de borda de rede e detectores/agentes inibidores de invasão (IDS/IPS). Para ambos os tipos de ativos, as referências são as mesmas: a norma FAB NSCA 7-13/2013 [117](item 3.3 e Anexo E) , a norma ABNT NBR ISO/IEC 27001:2013 [36] em seu controle A.13 (Segurança nas comunicações), a norma ABNT NBR ISO/IEC 27032:2015 [38] em seu controle 11.4.2.3 (Monitoramento e resposta de rede), CIS Controls [113] em seu controle nº13 (Monitoramento e defesa da Rede), além do NIST CSF [66] em suas funções de proteger (PR) e detectar (DE), nas categorias controle de acesso (AC) e monitoramento contínuo de segurança (CM).

Proteção da Aplicação

Da mesma forma que houve a preocupação com a segurança do perímetro de rede, para as aplicações foram levados em conta os serviços de Proxy Reverso e Firewall de Aplicação, cuja proteção é sob medida para cada aplicação específica. Apesar de ser um foco específico de monitoramento, as referências para proteção das aplicações são exatamente as mesmas da proteção do perímetro da rede.

Proteção de Acesso ao Sistema ou Serviço

Os especialistas debateram este tema que, segundo eles, recorrentemente causa problemas, o controle de acesso. Mas a preocupação não foi sobre o acesso em si, o qual pode ser testado por aplicações de escaneamento de vulnerabilidades em ativos, mas, sobretudo, das funcionalidades administrativas. Para os especialistas há um certo descuido quanto à manutenção das permissões, com usuários com permissão superior à necessária às suas atividades, podendo comprometer a confidencialidade, a integridade e a disponibilidade dos sistemas da organização.

Um segundo ponto de preocupação é quanto às contas de usuários que foram desligados da organização ou que estão inativos por estarem em licença médica, férias ou em viagem. Ou seja, há contas que deveriam estar inativadas definitivamente ou temporariamente, mas continuam ativas, sujeitando a organização à riscos desnecessários. As referências para ações de identificação e proteção contra estas práticas são as mesmas, com as normas NSCA 7-13/2013 [117], em seu anexo B, item 1.27; a norma ABNT NBR ISO/IEC 27001:2013 [36] itens A.9.2 (Gerenciamento de acesso do usuário) e A.9.4 (Controle de acesso ao sistema e à aplicação); CIS Controls [113] em seu controle nº5, gerenciamento de contas; e o NIST CSF [66] em sua função proteger (PR), na categoria controle de acesso (AC) e monitoramento

contínuo de segurança (CM).

Proteção do Ativo/Serviço

Para este grupo de controles, os itens ou controles identificados fazem parte da proteção dos ativos individuais, sob diversos aspectos, como: a necessidade ou não do uso de criptografia na comunicação; se há portas de rede desnecessariamente abertas, incluindo o acesso remoto ao ativo; sobre o nível de exposição do ativo ao ambiente do espaço cibernético, ou seja, se o mesmo está em uma rede segregada ou desconectado, se está em uma intranet, ou se está no ambiente externo à rede da organização, ou na Internet; se o ativo faz parte de um sistema de tráfego de dados sigilosos, com implicações legais ou de inteligência; se há proteção lógica contra malwares diversos; e quanto à proteção física do ativo. As principais referências continuam sendo a norma ABNT NBR ISO/IEC 27001:2013 [36], a NSCA 7-13/2013 [117] e o NIST CSF [66] , portanto, os próximos parágrafos se restringirão aos itens pouco comuns em análises de risco, em função do ambiente específico do NuCDCAer em sua missão.

Quanto a nível de exposição do ativo, a discussão levou a um consenso de que seria um controle imprescindível, por estabelecer qual nível de proteção normal ou adicional o ativo necessita, em função de sua exposição ao ambiente externo (Internet), o qual é definido na norma ABNT NBR ISO/IEC 27032:2015 [38] como componente que caracteriza o espaço cibernético. Para tal, as referências situam-se na publicação NIST SP 800-115 [123] que trata de testes de penetração que podem abranger diversos níveis de atuação dentro e fora do perímetro interno da rede e do Lockheed Martin Cyber Kill Chain, durante a fase Reconhecer e Entregar dos ataques cibernéticos, durante a qual a exposição maior do ativo facilita o ataque.

O controle de homologação de sigilo diz respeito aos sistemas que tratam de dados sigilosos, como sistemas de inteligência e de comunicações de Estado, que necessitam de certificação de órgãos de inteligência para serem utilizados e garantirem o sigilo necessário. Há duas publicações na FAB que norteiam este tipo de controle, a ICA205-47-Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica [124] e a ICA 200-8- Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações do Comando da Aeronáutica [118].

(iv) Análise da Parte 2, Bloco D - A discussão sobre as escalas de controles

Para a pergunta que tratava sobre as escalas de avaliação dos controles, surgiu uma dúvida sobre a padronização da eficácia dos controles, ou seja, como avaliar

se um controle foi efetivo, de forma qualitativa, por meio da escolha de um texto que ofereça uma informação clara para o analista. A resposta surgiu pelos próprios especialistas, com a referência ao TCU e sua campanha para fortalecimento da resiliência aos riscos na APF, com pesquisas sobre nível de maturidade em gestão de riscos e acórdãos norteadores de atividades em gestão de riscos.

O Tribunal de Contas da União (TCU) exerce a função de órgão de controle externo do governo federal, além de promover ações de aperfeiçoamento da Administração Pública do país, segundo o Portal Institucional do TCU [125]. Desde 2011 o Tribunal vem estabelecendo objetivos estratégicos para a gestão de riscos na Administração Pública Federal (APF), culminado em 2017 com a publicação do Roteiro de Auditoria de Gestão de Riscos do TCU [109]. Em sua metodologia para gestão de riscos, o TCU estruturou uma escala para avaliação de controles de mitigação de riscos, que podem ser usados nos processos de avaliação de riscos do NuCDCAer. Estruturar uma referência para definição de escalas de análises de controles de riscos pode proporcionar uma visão menos subjetiva dos valores e justificativas para seleção do nível de eficácia dos controles em relação às vulnerabilidades a serem mitigadas. Esta redução de subjetividade decorre da criação do quanto cada definição prática e compreensível destes controles pode representar em proporção de proteção (mitigação) ou não. A Tabela 5.4 evidencia os requisitos para a criação das escalas individuais de avaliação dos controles, em virtude de os mesmos possuírem interpretações específicas para cada tipo utilizado. Para cada grau de confiabilidade dos controles foi elaborado um texto que facilita a comparação do ambiente de TI analisado sobre a presença total, parcial ou ausência de controles mitigadores em relação a cada vulnerabilidade investigada.

Tabela 5.4: Definição da Eficácia dos Controles

Nível de Confiança ou eficácia do controle (NC)	Situação do Controle Existente	Multiplicador do Risco Inerente	Valores para a seleção qualitativa do nível do controle ¹
Inexistente NC = 0%	Ausência completa de controle ou controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1,00	5
Fraca NC = 20%	Controle deixa de atender o requisito de mitigação de riscos em sua maior parte. Apoiado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual havendo confiança no conhecimento das pessoas.	0,80	4
Mediana NC = 40%	Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	0,60	3
Satisfatória NC = 60%	Controle normatizado e embora passível de aperfeiçoamento, está sustentado por ferramentas adequadas e mitiga o risco razoavelmente.	0,40	2
Forte NC = 80%	Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrado num nível de “melhor prática”.	0,20	1

Fonte: adaptado de Brasil.TCU.2017 [109]

Portanto, a escala embasada pelo TCU auxiliou a tradução dos requisitos de confiança dos controles em textos compatíveis com os controles analisados, permitindo a interpretação correta dos analistas frente às comparações entre interações das vulnerabilidades e seus valores de criticidade com o nível de confiança permitido pelo controle.

(v) **Análise da Parte 3 - A discussão sobre o cálculo das FAC**

Para o estabelecimento da fórmula de cálculo do risco residual (FAC) de cada vulnerabilidade em relação aos controles estabelecidos e analisados, os analistas apontaram o consenso de haver uma necessidade de se estabelecer uma média entre os valores de mitigação da vulnerabilidade frente a cada controle analisado. Logo a fórmula foi traduzida como a soma de todas os fatores (valor da vulnerabilidade, multiplicado pelo fator de mitigação do controle), dividido pela quantidade de controles com valor diferente de zero, conforme a Fórmula 5.6. Esta característica se deve à possibilidade de eliminação de algum controle durante a análise por este não ser compatível com o tipo de ativo analisado.

¹Este valor é diagramado para ser coerente com os valores da vulnerabilidade. Exibe de forma numérica uma escala de 1 a 5, correspondente aos graus de criticidade dos controles. São amparados por escalas qualitativas que informam ao analista o grau a ser selecionado sendo corroborado com a coloração indicativa similar às da vulnerabilidade, desde vermelho o nível mais inseguro, passando por laranja, amarelo e verde, como o nível mais confiável dos controles.

$$FAC_m = \frac{\sum_{i=1}^n V_m * E_{Ci}}{i}, \forall E_{Ci} > 0 \quad (5.6)$$

Fator de Ameaça Cibernética da Vulnerabilidade em análise

Fonte: Autoria própria.

Onde: FAC_m = Fator de Ameaça Cibernética (risco residual após controles) relativa à vulnerabilidade m; V_m = vulnerabilidade m analisada; E_{Ci} = Eficácia do controle (i); i=índice do controle específico analisado.

Esta fórmula indica o risco residual (FAC) após mitigação ou não pelos controles. Porém falta a definição de um valor que represente o FAC do ativo em análise. Optou-se, após discussão, pela estratégica conservadora de riscos, ou seja, que seja escolhido o maior risco residual como representativo do risco do ativo (componente do ativo agregador) em análise, conforme a Fórmula 5.7.

$$FAC_n = \max (FAC_m) \quad (5.7)$$

Fator de Ameaça Cibernética do Ativo em Análise

Fonte: Autoria própria.

Onde: FAC_n = Fator de Ameaça Cibernética (risco residual representativo do ativo n em análise) relativa à vulnerabilidade m; FAC_m = Fator de Ameaça Cibernética (risco residual após controles) relativa à vulnerabilidade m.

Para o cálculo do IRC, após a obtenção dos valores de FAC_m e FAC_n, necessita-se do valor estratégico do ativo, o qual representa não o valor monetário do ativo em si, mas de seu valor para o negócio da organização, conforme será visto a seguir.

(vi) **A discussão sobre a escala de criticidade do ativo agregador**

Para a discussão sobre o valor de criticidade do ativo agregador, o qual pode ser referenciado como sistema ou serviço, cuja composição possui outros diversos ativos de informação, deve ter sua criticidade determinada e evidenciada, em função de compor o valor de risco já discutido na subseção 5.3.1 item 9 deste trabalho, com a Fórmula 5.4, que estabelece o valor do risco, levando-se em consideração a importância estratégica do ativo em análise.

Para a definição dos valores de criticidade em termos numéricos, necessitou-se de uma descrição qualitativa para que o analista possa fazer a escolha adequada de

acordo com o nível correto. Levou-se em conta a definição de infraestrutura crítica do Decreto 9573/2018 [85]:

“Instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.” (Brasil, 2018, não paginado)

Esta definição embasou a escolha dos critérios de seleção de criticidade, em função da importância aos objetivos estratégicos do país, e ao sistema de defesa, compreendido pelo Ministério da Defesa e Forças Armadas; em função da importância para a área de pesquisa e desenvolvimento tecnológico da FAB (neste primeiro momento, mas podendo ser expandido a outras estruturas organizacionais); criticidade para as atividades administrativas da FAB; e ativos pouco críticos com importância ou alcance local ou de objetivos ou processo de importância reduzida ou baixo custo, conforme a Tabela 5.5.

Tabela 5.5: Valores e condições de criticidade dos ativos ou serviços estratégicos

Aspectos de CRITICIDADE da Aplicação	Valor
Crítico para os objetivos estratégicos da FA, Min. Defesa ou do País	5
Crítico para a área de P&D (Objetivos de desenvolvimento da ciência ou tecnológicos)	4
Crítico para atividades administrativas de grande porte (Objetivos Essenciais de Negócios)	3
Pouco críticos por alcance somente local às atividades ou objetivos de importância reduzida	2

Fonte: Autoria própria.

Para que a avaliação se complete, necessita-se definir como todos os valores analisados sejam utilizados para o cálculo do índice de riscos cibernéticos (IRC) desejado, o que será visto no tópico a seguir.

(vii) A discussão sobre o cálculo do IRC

A obtenção do valor do IRC se tornou possível após a definição do processo de avaliação dos riscos pelos especialistas do NuCDCAer, pois foram definidas a sequência e origem básica dos dados a serem analisados e avaliados, além de suas relações funcionais, seus valores intrínsecos e a forma de cálculo dos riscos residuais de cada vulnerabilidade após interagir com os controles selecionados.

Tornou-se um consenso a utilização da estratégia conservadora em relação ao risco. Para tal, entendeu-se que os valores dos FAC dos ativos (FAC_n) seriam comparados e o maior valor de FAC_n seja o valor a ser multiplicado pelo nível de criticidade do serviço ou ativo agregador e assim estabelecer o valor de risco efetivo para o ativo,

relativo à sua importância estratégica. A este valor denominou-se Índice de Risco Cibernético do serviço ou ativo agregador, representado pela Fórmula 5.8.

$$IRC = FAC_n * C \quad (5.8)$$

Índice de Risco Cibernético do serviço ou ativo agregador.

Fonte: Autoria própria.

Onde: IRC = Índice de Risco Cibernético do serviço ou ativo agregador. FAC_n = Fator de Ameaça Cibernética (risco residual representativo do ativo n em análise) relativa à vulnerabilidade m; C = valor de criticidade do serviço ou ativo agregador.

Após a obtenção do processo de cálculo do IRC, identificou-se que a sequência lógica seria a de estabelecer uma ferramenta computacional básica para facilitar o registro e o cálculo dos fatores componentes deste índice. O próximo tópico refere-se ao processo levado a termo para a construção de um protótipo em formato de pasta de trabalho do Microsoft Excel 365, seja pela facilidade da implementação, custo financeiro, praticidade, confiabilidade e senso didático para o desenvolvimento ou aquisição de uma ferramenta comercial que possa ser adaptada para o processo diagramado para o NuCDCAer.

5.5 Criação da ferramenta computacional para cálculo do IRC

Para a consecução do cálculo do IRC, havia a necessidade da criação de um instrumento capaz não somente de receber os dados para análise e nível de mitigação das vulnerabilidades por meio dos controles, mas de ser didático o suficiente para oferecer subsídios sobre os requisitos básicos e permitir a compreensão da finalidade do IRC. Após este entendimento, a organização poderia ser capaz de escolher uma ferramenta comercial de gestão de riscos ou de desenvolver uma ferramenta internamente ou de forma terceirizada.

5.5.1 Estruturação da ferramenta de cálculo do IRC

O processo de avaliação dos riscos cibernéticos (ARCiber) já foi ilustrado neste trabalho, no item 5.3.1, na Figura 5.5, porém falta a definição de uma sequência lógica que possa ser usada em uma ferramenta computacional, seguindo os passos do processo em si, de forma a ser compreensível e factível ao usuário. Esta sequência é evidenciada na Figura 24 5.7 e os passos são pormenorizados em seguida.

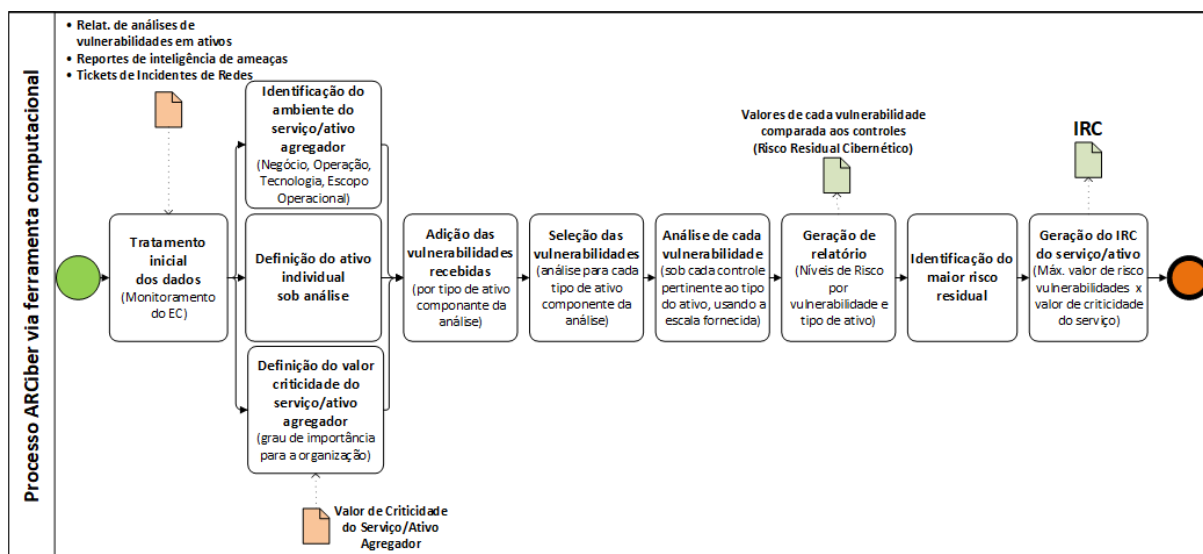


Figura 5.7: Diagrama do Processo de Avaliação de Riscos Cibernéticos do NuCDCAer

Fonte: autoria própria

Os passos para a execução do processo de avaliação de riscos cibernéticos com o uso de uma ferramenta auxiliar de cálculo, são:

1. Recebimento dos relatórios ou listas de vulnerabilidades (Fase Identificação de Riscos);
2. Identificação do cenário de risco sob ameaça (ativo agregador ou serviço) (Fase Identificação de Riscos);
3. Identificação dos componentes do cenário (ativos contidos no inventário do serviço ou ativo agregador) para análise independente de cada componente (Fase Identificação de Riscos);
4. Definição do valor e grau de importância (Valor de Criticidade) do cenário para a organização (Forças Armadas individuais, Ministério da Defesa, Brasil) (Fase Definição do Contexto);
5. Preenchimento da planilha de análise com as vulnerabilidades listadas para cada componente do cenário (Fase Análise de Riscos);
6. O usuário deverá escolher cada vulnerabilidade dentre as listadas para comparar com cada controle definido na ferramenta, estabelecendo um valor para a comparação, dentro da escala oferecida pela ferramenta e este valor poderá manter ou reduzir

o valor final de criticidade da vulnerabilidade (risco residual). (Fase Análise de Riscos);

7. O sistema multiplicará o valor da criticidade da vulnerabilidade pelo valor escolhido na escala, compondo, ao final da análise de cada vulnerabilidade por todos os controles disponíveis, uma média aritmética para o valor da criticidade da vulnerabilidade, correspondente ao risco residual cibernético, denominado Fator de Ameaça Cibernética (FAC) daquela vulnerabilidade (Fase Análise de Riscos);
8. Há controles que deverão ser de análise obrigatória para o componente e há outros que serão de análise opcional, em virtude de o componente ou a vulnerabilidade não ser compatível com a análise sob aquele controle, momento no qual o usuário deve ou pode usar o valor de nível do controle 0 (zero), que eliminará aquele controle daquela análise em especial, sem adulterar o valor correto da média aritmética;
9. Cada vez que o usuário determinar um valor de criticidade de vulnerabilidade (FAC), o sistema atualizará o relatório de valores de criticidade dos componentes do cenário em análise, apontando o valor máximo da criticidade para aquele tipo de componente (Fase Avaliação de Riscos);
10. Ao final da última análise de vulnerabilidade do último componente do cenário, o relatório já será capaz de informar o valor máximo de criticidade de vulnerabilidade (FAC) de cada tipo de componente do cenário de análise (Fase Avaliação de Riscos);
11. Estabelecidos os valores do item 12, o sistema fará a multiplicação do maior valor de criticidade (FAC) dentre todos os componentes pelo valor de criticidade do cenário (item 4), estabelecendo assim o Índice de Risco Cibernético (IRC) para aquele cenário específico de risco para a organização (Fase Avaliação de Riscos).

5.5.2 Desenvolvimento da ferramenta de cálculo

A ferramenta visa reunir os valores inseridos como insumos para a efetiva composição do Índice de Riscos Cibernéticos.

Para o desenvolvimento do protótipo da ferramenta computacional, levou-se em conta a necessidade da averiguação dos requisitos do processo de ARCiber. Seguindo este entendimento, detectou-se que uma planilha de cálculo seria ideal para esta pesquisa, pois possui os meios de cálculo e a integração básica dos dados entre os campos de informações (células de uma planilha) e campos de outras planilhas dentro da mesma pasta de trabalho, definindo um protótipo de ferramenta com finalidade didática e de averiguação da teoria de ARCiber. Definiu-se que o aplicativo seria o Microsoft Excel, versão 365, cuja

interface é de conhecimento dos integrantes do NuCDCAer, bem como seu uso é intuitivo e eficaz.

O processo básico exige que haja campos com informações sobre o contexto básico da análise, com as informações básicas que permitam a estimação da importância do ambiente em análise, com o nível de criticidade do serviço ou ativo agregador, e o inventário de ativos que o compõe. Para as planilhas de análise, deverão ser informadas, nos campos respectivos as identificações e os valores brutos de criticidade das vulnerabilidades, advindos dos relatórios das equipes de gestão de vulnerabilidades e de inteligência de ameaças, bem como já estarão cadastrados os controles básicos para análise do ambiente em relação às vulnerabilidades reportadas.

Foram criadas ao total 6 planilhas em uma pasta de trabalho, sendo a primeira a responsável por possuir o cadastro do cenário de risco (contexto da análise), com a identificação da operação a ser efetuada, o processo de negócio ao qual o serviço pertence, o próprio serviço ou ativo agregador, o escopo operacional para a FAB desta avaliação, e o nível de criticidade do cenário de risco. Possui também as informações (relatório) dos valores dos riscos máximos dos ativos componentes (FAC_{ativo}), além de suas classificações qualitativas, com um campo indicando, dentre os valores de FAC_{ativo} o maior valor para ser considerado, juntamente com o valor de criticidade do serviço, como componentes da fórmula de cálculo do IRC, cujo valor final é exibido na parte superior direita da planilha, em conjunto com seu valor qualitativo e sua cor de indicação. A Figura 5.8 ilustra o visual desta planilha.

COMPOSIÇÃO DO ÍNDICE DE RISCO CIBERNÉTICO		Operação	Avaliação de Riscos		
		Processo de Negócio	11.3 - Promover informações ao cidadão		
		Serviço/Produto (ativo agregador)	Portal FAB		
		Escopo operacional	Análise de Riscos do Portal FAB		
		Criticidade	Crítico para a área de P&D (Objetivos de desenvolvimento da ciência ou tecnológicos)		
				IRC = 20	
				Extremo	
Classificação dos Tipos de Ativos		Ativos analisados	Valor de Risco do Ativo (FAC _{ativo})	Classificação do Risco do Ativo (FAC _{ativo})	
ATIVOS DE TECNOLOGIA	ATIVOS DE SOFTWARE	ATIVO 1	4,95	Extremo	
		ATIVO 2	5,00	Extremo	
		ATIVO 3	4,48	Alto	
		ATIVO 4	4,62	Extremo	
Valor máximo de Risco Encontrado (FAC_{serviço})			5,00		
Fórmulas para cálculo dos Riscos					
$FAC_{vulnerabilidade} = \text{SOMA}(Vulnerabilidade_m * ValorControle) / \text{Conta}(SE(ValorControle > 0))$ $FAC_{ativo} = \text{MÁXIMO}(FAC_{vulnerabilidade})$ $FAC_{serviço} = \text{MÁXIMO}(FAC_{ativo})$			$FAC_m = \frac{\sum_{i=1}^n V_m * E_{Ci}}{i}, \forall E_{Ci} > 0$		
$IRC = FAC_{serviço} * Criticidade_{serviço}$					
<p>1-Planilha_Relatório_V1 Planilha ATIVO 1 Planilha ATIVO 2 Planilha ATIVO 3 Planilha ATIVO 4 Tabelas de Riscos</p>					

Figura 5.8: Planilha 1 – Cadastro do Contexto e relatório de IRC

Fonte: autoria própria

As planilhas 2 a 5 correspondem aos 4 ativos componentes usados de forma didática. A quantidade de 4 ativos foi escolhida por ser um número prático de análises para testar o processo e a ferramenta, podendo, em uma situação real, o serviço ou ativo agregador possuir uma quantidade não determinada de ativos componentes. Para estas planilhas, há um cabeçalho que repete os dados cadastrado na planilha 1 como lembrete ao analista sobre os dados em análise, bem como o nível de criticidade. Na parte inferior há diversos campos organizadores, como a classificação do tipo do ativo, e seus aspectos tecnológicos (função na TI). Na parte superior há os cabeçalhos da planilha e, principalmente, as células com os grupos de controles, agrupando os diversos controles a serem comparados com as vulnerabilidades, segundo as escalas de cada controle, logo abaixo destes.

Na parte esquerda há as células com espaço para cadastramento das vulnerabilidades recebidas das equipes de gestão de vulnerabilidades, em formato de relatório, com seus respectivos valores no padrão CVSS (que, para esta ferramenta didática foram limitados na escala de 1 a 5). Nas células mais à direita situam-se os espaços para serem adicionados os valores de mitigação dos controles, de acordo com os valores das escalas respectivas. Estes valores são o resultado da análise manual pelos analistas da interseção de entendimento entre uma vulnerabilidade à esquerda e o controle acima desta célula específica. Este valor permite que a fórmula contida na penúltima célula desta linha da planilha calcule o valor do fator de ameaça cibernética desta vulnerabilidade em análise ($FAC_{vulnerabilidade}$),

e resulte em um valor numérico nesta célula e um valor qualitativo de sua intensidade na célula à direita.

Para todas estas células (criticidade da vulnerabilidade, $FAC_{vulnerabilidade}$, valores de mitigação, e valor qualitativo) possuem esquema de cores no estilo semáforo, com o verde em seus valores menores, passando pelo amarelo, laranja e vermelho, de acordo com o aumento dos valores. Há uma célula na parte inferior direita que indica o maior valor de $FAC_{vulnerabilidade}$ que será transportado para a primeira planilha como sendo o valor da FAC_{ativo} , ou seja o fator de ameaça cibernética do ativo analisado. A Figura 5.9 ilustra este tipo de planilha usada, exibindo somente seu visual, pois, em virtude da quantidade de dados, não possível exibi-la em detalhes neste formato de documento.

Figura 5.9: Planilha 2 – Análise de vulnerabilidades pelos controles

Fonte: autoria própria

O terceiro e último tipo de planilha usado é o das tabelas de riscos, criticidade de controle e eficácia dos controles, servindo de repositório para os valores de cálculos usados nas fórmulas das planilhas anteriores, conforme ilustra a Figura 5.10. Em virtude do tamanho e complexidade da página da planilha, esta imagem possui somente valor ilustrativo, não sendo viável, nem indispensável a exibição dos detalhes de cada célula.

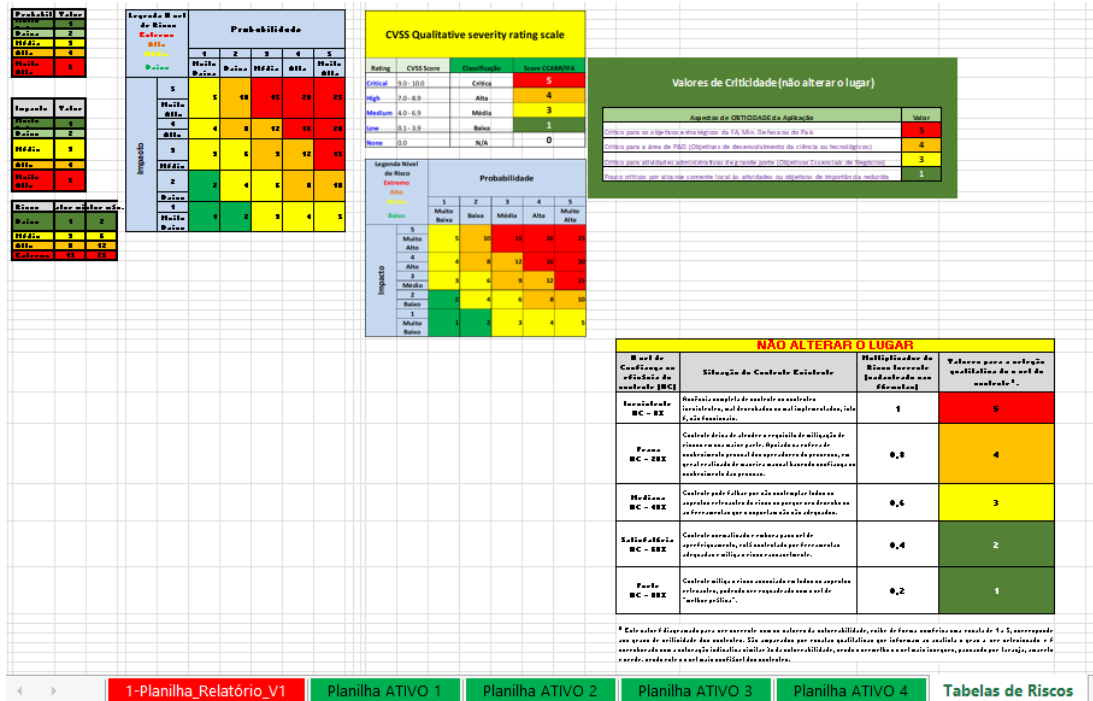


Figura 5.10: Planilha 3 – Tabelas de valores de base para os controles
 Fonte: autoria própria

Vários analistas da subdivisão de segurança da informação utilizaram preliminarmente a ferramenta de avaliação de riscos durante seu desenvolvimento, e seus comentários auxiliaram na escolha de seu layout e na apresentação dos controles. A avaliação efetiva será objeto de um processo de investigação pela técnica Delphi, após este período de uso experimental.

O NuCDCAer, por meio de sua diretoria de TI adquiriu há pouco tempo a ferramenta de governança, risco e compliance RSA Archer [60], que possui muitas funcionalidades úteis para o uso da seção de gestão de riscos. Possui um sistema de inventário, gestão de ameaças e vulnerabilidades, mas não possui nenhum módulo que possa efetuar a gestão de riscos cibernéticos, resumindo-se aos riscos gerais a ativos (não cibernéticos). Foi apresentado o processo de avaliação de riscos proposto neste trabalho, tornando-se objeto de avaliação por parte da empresa representante da RSA no Brasil. Sugeri-se a criação de uma aplicação interna que pudesse utilizar o sistema de gestão de ativos e agrupamento de informações de avaliações de vulnerabilidades (escaneamentos de redes de computadores e testes de penetração em sistemas) efetuadas por ferramentas diversas, as quais a organização possui em seu arsenal de soluções.

Foram adaptados diversos módulos do Archer para compor o processo de avaliação de riscos e geração do IRC, estando atualmente em fase de avaliação. A ferramenta cons-

truída em formato planilha é recorrentemente consultada para a confirmação dos passos do processo, pois foi considerada didática, revelando as informações de maneira simples e prática. As figuras a seguir ilustram os diversos tipos de tela com as funcionalidades necessárias para a consecução do processo. A Figura 5.11 representa o serviço, produto ou ativo agregador cujos dispositivos integrantes são registrados; a Figura 5.12 representa o cadastro manual ou automatizado de dispositivos; a Figura 5.13 representa os controles (em formato de questionário) para avaliação das vulnerabilidades dos ativos em função do ambiente onde estão hospedados; a Figura 5.14 demonstra como os processos de negócio cujos ativos serão analisados são registrados; a Figura 5.15 finalmente compõe a funcionalidade de cadastro da avaliação de risco do serviço, condizente com o processo ARCiber do NuCDCAer, permitindo a exibição do IRC corretamente.

The screenshot displays the RSA Archer interface for the 'FORÇA AÉREA BRASILEIRA' (Brazilian Air Force) environment. The main header shows navigation options: 'Gestão de Risco Cibernético', 'Gerenciamento de riscos de seg...', and 'Gestão de Ativos'. The current view is titled 'Produtos e serviços : OA1_SVC.PortaIFAB'. Below the title, it indicates the first publication date (03/11/2021 12:29) and the last update (09/12/2021 15:09). The interface is divided into several sections:

- SOBRE**: A section for general information.
- INFORMAÇÕES GERAIS**: A section containing various attributes:
 - ID do produto: PSID-281299
 - Nome de produto/serviço: OA1_SVC.PortaIFAB
 - Unidade de negócios: [CECOMSAER](#)
 - Descrição:
 - Impacto no cliente: Sim
 - Status: Ativo
 - Classificação de conformidade:
 - Categoria: Externo
 - Divisão/escritório: [GABAER - Gabinete do Comandante da Aeronáutica](#)
 - Informações sobre o impacto no cliente:
- Equipe**: A section for team information, currently showing 'Infraestrutura de suporte'.
- SOBRE EQUIPE**: A section for team details.
- EQUIPE**: A section for team members.
- CONTATOS DO PRODUTO/SERVIÇO**: A section for contact information.
- ANEXOS**: A section for attachments.
- ATIVIDADES/TAREFAS ABERTAS**: A section for open tasks.
- REGISTRO DO HISTÓRICO**: A section for the history record.

Figura 5.11: Produtos ou Serviços (ativo agregador)

Fonte: RSA Archer [60]

🏠 **Gestão de Risco Cibernético** ▾ | **Gerenciamento de riscos de seg...** ▾ | **Gestão de Ativos** ▾ | ⋮

Dispositivos : 10.30.20.1

Primeira publicação: 24/02/2022 14:13 Última atualização: 04/04/2022 11:19 ◀ Registro 2 de 1 171 ▶

▶ **SOBRE**

▼ **INFORMAÇÕES GERAIS**

🔗 ID do dispositivo: DID-292683	Origem: Manual
Nome do dispositivo: 10.30.20.1 - Portal de pesquisas da FAB	Última atualização por: Manual
🔗 Tipo: Servidor da Web	Manual: Sim
🔗 Unidade de negócios: CCA-BR - Centro de Computação de Aeronáutica de Brasília Adicionar	🔗 Categoria: Interno
Grupo(s) de ativos: Demonstração do Archer	🔗 Classificação de risco: Not Rated
Propriedade do grupo de ativos: Administrator, System Mitchell, Cleber	🔗 Classificação de conformidade: Not Rated
🔗 Data da próxima avaliação:	🔗 Classificação de relevância: Não classificado
🔗 Última atualização: 04/04/2022 11:19	Estado de análise do dispositivo: Novo
	🔗 Registro do histórico: Exibir registro histórico

▶ **ANTIVÍRUS**

▶ **DETALHES DA TECNOLOGIA**

▶ **EQUIPE**

▶ **CONTAS COM ACESSO IDENTIFICADO POR SCANNER**

Perfil de tecnologia	Contexto de negócio	Gerenciamento de riscos	Gerenciamento de conformidade	Continuar
Gerenciamento de problemas	Gerenciamento de vulnerabilidades	Incidentes Detectados		

▶ **SOBRE GERENCIAMENTO DE RISCO**

▶ **AVALIAÇÃO DE RISCOS DO DISPOSITIVO**

▶ **PROJETOS DE RISCO**

▼ **FATOR DE AMEAÇA CIBERNÉTICA**


Fator de Ameaça Cibernética: 	F.A.C (numérico): 5
Maior CVSS do Dispositivo:	

Figura 5.12: Dispositivos (ativos componentes)

Fonte: RSA Archer [60]

FORÇA AÉREA BRASILEIRA
 RSA Archer Suite
 AMBIENTE DE HOMOLOGAÇÃO

Gestão de Risco Cibernético | Gerenciamento de riscos de seg... | Gestão de Ativos

Avaliação de Controle - Dispositivo : 292710

Data de criação: 25/02/2022 09:57 Última atualização: 25/02/2022 10:04

Registro 8 de 15

INSTRUÇÕES

INFORMAÇÕES GERAIS

ID do questionário: 292710
 Destino: [10.40.30.2](#)
 Status geral: ✔
 Status de progresso: 0%
 Data de entrega: 25/02/2022
 Registro do histórico: [Exibir registro histórico](#)

Remetente:
 Status de envio: Enviado
 Data de envio: 25/02/2022
 Revisor: [Alves, Felipe](#)
 Status de revisão: Aprovado
 Data de revisão: 25/02/2022

CONTROLES

Controle 01 - Tempo da vulnerabilidade Controle 1:
 (Tempo de existência, descoberta confirmada ou maturidade do ecossistema da vulnerabilidade e dos controles)
 (Escala padrão CVSS)
 5 = Existência confirmada, exploits funcional sem patch de remediação
 4 = Existência confirmada, Exploits não totalmente funcionais ou baixo nível de remediação
 3 = Existência confirmada, exploits não confirmados, patches de remediação temporários ou com algum nível de remediação
 2 = Existência da vulnerabilidade confirmada, mas de baixo nível de impacto, sem exploits publicados ou patch de remediação oficial disponível
 1 = Vulnerabilidade não confirmada.

Controle 02 - Limitação no escopo da análise Controle 2:
 (Existe alguma limitação no escopo da análise de vulne-rabilidades (PenTest) em virtude do ambiente de Avaliação (produção , homologação ou teste, grau de sigilo, permissão do proprietário ou autoridade etc.)
 (Escala)
 5 = Houve limitação da análise de vulnerabilidades em função de o sistema estar em produção ou ser crítico
 1 = Não houve limitação ao teste de vulnerabilidade ou penetração

Controle 03 - Impactos por aspectos legais Controle 3:
 (Escala)
 5 = Alto / Nunca foi avaliado (processos e sanções de alto custo à instituição)
 3 = Médio (Multas ou danos à imagem da instituição pela judicialização)
 1 = Irrelevante possibilidade de judiciali-zação ou sanções econômicas ou legais
Sem seleção = Eliminar aspecto da análise

...

Controle 18 - Nível de exposição do ativo Controle 18:
 (Escala)
 5 = Disponível via Internet (acessível a ataques externos/outsider)
 3 = Disponível via Intranet (acessível a ataques de insiders ou comprometimento de gateways externos/Internet/Extranet)
 1 = Disponível via Rede Segregada / Ativo de uso isolado ou sem conexão de rede (necessidade de acesso via insider pela rede ou acesso físico ao ativo)

Controle 19 - Homologação de sigilo Controle 19:
 (Escala)
 5 = Não, o sistema tramita ou armazena dados sigilosos e nunca foi homologado por órgão de inteligência responsável
 1 = Sim, o sistema tramita e/ou armazena dados sigilosos e foi homologado por órgão de inteligência responsável
 0 = O Sistema não manipula dados sigilosos

Controle 20 - Proteção contra malwares Controle 20:
 (Escala)
 5 = Não há qualquer proteção por softwa-re contra códigos maliciosos
 3 = Há uma proteção parcial por software contra alguns tipos de códigos maliciosos
 1 = Sim, há proteção por software contra códigos maliciosos
 0 = Remover aspecto da análise

Controle 21 - Proteção física dos ativos Controle 21:
 (Escala)
 5 = Não há proteção física adequada para os ativos importantes
 3 = Há uma proteção física parcial, não eficaz aos ativos importantes
 1 = Sim, há proteção fica adequada aos principais ativos

Contador: 21
 Soma: 14,4

Figura 5.13: Controles para avaliação do ambiente dos ativos(questionário)
 Fonte: RSA Archer [60] (com recorte em função do comprimento da imagem)

Processos de negócio : OA1_PROC.Estrategico_1

Primeira publicação: 03/11/2021 12:26 Última atualização: 09/12/2021 15:09

◀ Registro 4 de 14 ▶

▶ **SOBRE**

▼ **INFORMAÇÕES GERAIS**

<p>🔗 ID do processo: BPID-281295</p> <p>Nome do processo: OA1_PROC.Estrategico_1</p> <p>🔗 Unidade de negócios: Adicionar</p> <p>🔗 Tipo de processo:</p> <p>Objetivos dos negócios:</p> <p>🔗 Análise de impacto No realizada?:</p> <p>Descrição:</p>	<p>🔗 Categoria de oportunidade:</p> <p>🔗 Categoria de ITIL:</p> <p>🔗 Financeiramente Erro significativo?:</p> <p>🔗 Categoria:</p> <p>🔗 Classificação de Não classificado relevância:</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


▶ **DETALHE DO PROCESSO SECUNDÁRIO**

▶ **PROCESSOS FILHOS**

Detalhes	Gerenciamento de riscos	Histórico de avaliações	Análise de impacto nos negócios	Contexto de r
Continuidade de negócios	Infraestrutura de suporte	Gerenciamento de conformidade	Gerenciamento de vulnerabili	

▶ **SOBRE GERENCIAMENTO DE RISCOS**

▼ **ÍNDICE DE RISCO CIBERNÉTICO**

I.R.C:  I.R.C do processo: 21,3

▶ **REGISTRO DE RISCOS**

▶ **PERFIL DE GERENCIAMENTO DE RISCOS**

▶ **SELECIONAR RISCOS INDIVIDUAIS NA BIBLIOTECA DE REGISTRO DE RISCOS**

▶ **SELECIONAR RISCOS POR GRUPO**

▶ **PROJETOS DE RISCO**

▶ **EVENTOS DE PERDA**


▶ **ANEXOS**

▼ **ATIVIDADES/TAREFAS ABERTAS**

▶ **REGISTRO DO HISTÓRICO**

Figura 5.14: Cadastro de Processos de Negócio

Fonte: RSA Archer [60]


Gestão de Risco Cibernético ▾ |
 Gerenciamento de riscos de seg... ▾ |
 Gestão de Ativos ▾ |
 ⋮

Registro de riscos : RISCO_10.30.20.1

Primeira publicação: 24/02/2022 15:09 Última atualização: 24/02/2022 15:09
 ◀ Registro 5 de 11 ▶

▶ SOBRE

▼ INFORMAÇÕES GERAIS

- ID do risco: RSK-292689
- Risco: RISCO_10.30.20.1
- Risco intermediário:
- Descrição:
- Unidades de negócios: Adicionar
- Proprietário de unidade de negócios:
- Categoria de evento de risco:
- Coordenador de unidade de negócios:
- Abordagem da avaliação: Risco Cibernético
- Gerente de riscos:
- Status: Ativo

Análise de riscos | Resposta ao risco e tratamento | Monitoramento de riscos | Risco calculado | Análise de ce
 Mapeamentos | Informações sobre o provedor de conteúdo

▶ SOBRE ANÁLISE DE RISCOS

▼ ÍNDICE DE RISCO CIBERNÉTICO

- Produtos e Serviços: [Servidor Oracle v1.0](#)
- Processos de negócio: [ProcNeg_10.30.20.1](#)
- Criticidade (Serviço x 4 -Crítico para a área de P&D (Objetivos de desenvolvimento da Processo): ciência ou tecnológicos)
- Índice de Risco Cibernético:
- I.R.C (numérico): 20

▶ ATIVIDADES/TAREFAS ABERTAS

▶ REGISTRO DO HISTÓRICO

Figura 5.15: Registro de Riscos (avaliação dos riscos de serviços ou produtos)

Fonte: RSA Archer [60]

Com esta interação com a equipe representante do fabricante desta aplicação, pôde-se comprovar que a pesquisa tem influenciado positivamente na maturidade do NuCDCAer em termos de gestão de riscos, podendo discutir no mesmo nível que empresas dedicadas e estabelecer métodos de trabalho especializados, cujo protótipo simplificado revelou-se de grande utilidade prática.

Desta forma, a ferramenta computacional criada pode estabelecer um novo patamar de trabalho, ou seja, pode passar a ser avaliada pelos integrantes do NuCDCAer em termos

teóricos, com método conhecido e eficaz (técnica Delphi), para checagem final do alcance e validade de seus controles, cujo processo será efetivado na etapa a seguir.

5.6 Validação da ferramenta computacional e do método de cálculo do IRC

Para que um processo ou método de trabalho seja considerado eficaz, faz-se necessário que haja uma validação, com a finalidade de confrontar a teoria com a prática. Durante o processo de desenvolvimento da teoria e conseqüentemente da ferramenta de operacionalização da Avaliação de Riscos Cibernéticos (ARCiber), usou-se técnicas de levantamento de necessidades via entrevistas não estruturadas ou semiestruturadas para a definição dos requisitos e debates sobre controles de mitigação de riscos.

Após a construção do protótipo da ferramenta computacional em formato didático de planilha, houve o período de testes de funcionamento, cuja finalidade foi a de familiarizar os técnicos de gestão de riscos com os conceitos e técnicas de avaliação de riscos utilizados no processo de ARCiber. A função desta fase é a de obter respostas objetivas sobre os controles, as escalas de avaliação e os cálculos efetuados.

Dentre as possibilidades de avaliação usadas em pesquisas acadêmicas, optou-se por utilizar a técnica Delphi, em função do tamanho da amostra de técnicos a serem inquiridos e do caráter qualitativo do processo de ARCiber sob diversos aspectos.

5.6.1 Emprego da ferramenta computacional e definição do processo de validação

A etapa 6 contempla a avaliação dos parâmetros (controles) usados na ferramenta após o uso efetivo, pelos especialistas, da ferramenta computacional prototipada. Para exemplificar a seqüência de ações tomadas, segue-se a Figura 5.16 com o processo completo desde a criação da ferramenta até a etapa final de validação, de maneira genérica, sem aprofundamentos desnecessários ao entendimento do fluxo de atividades.

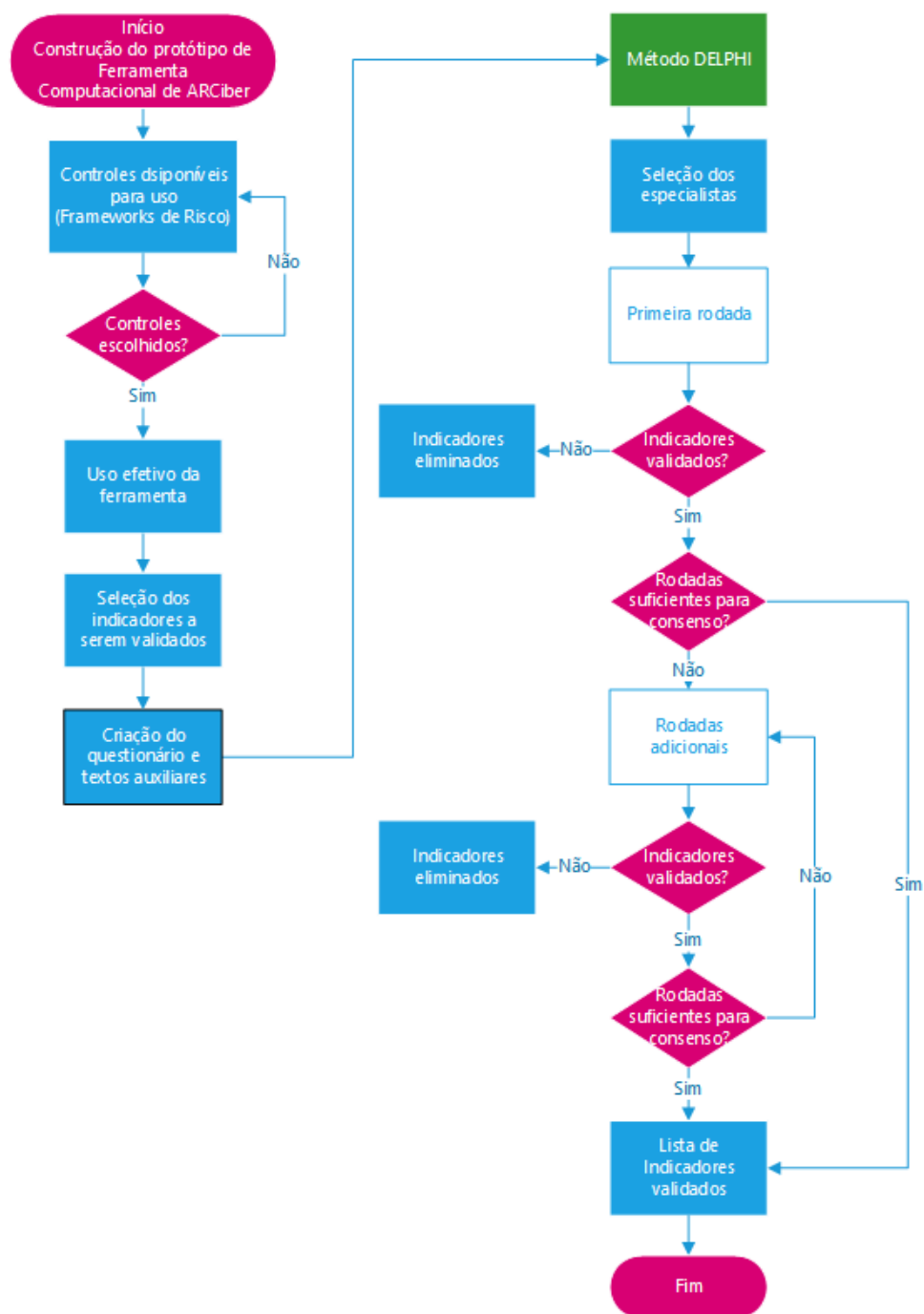


Figura 5.16: Modelo conceitual de fluxo do método Delphi para esta pesquisa

Fonte: Adaptado de Rozados (2015) [74]

5.6.2 Execução da investigação para validação

Os especialistas convidados foram solicitados a responder às perguntas segundo as escalas de valores indicadas, sempre havendo, para cada questão uma resposta adicional, aberta,

para coleta de opiniões além das escalas de validação objetiva.

Após esta primeira fase, as respostas foram coletadas e analisadas em termos de consenso e tendo suas respostas abertas interpretadas sob uma nova redação do entendimento do organizador. As respostas cujo coeficiente de consenso foi suficientemente elevado, estabeleceram a aceitação das opiniões. Caso algumas questões não obtivessem suficiente consenso, seria preparada uma nova rodada de questionários com a inclusão das interpretações das respostas abertas como forma de orientação dos respondentes e facilitação do consenso, além de alguma correção no texto da pergunta em si, pois poderia ter havido dificuldade no entendimento. Após esta possível rodada, nova avaliação seria efetuada, e, se muitas questões ainda não tivessem obtido consenso seria preparada uma nova rodada similar com as questões cujo nível de aceitação estivesse próximo da faixa ideal, sendo as que tivessem distante deste valor limite consideradas como não aceitas por não comporem grau aceitável de consenso e descartadas.

Durante a execução observou-se que todas as questões obtiveram consenso na primeira rodada, eliminando a necessidade de rodadas adicionais, estando este resultado em conformidade com o trabalho de Rozados [74], analisado na metodologia desta pesquisa.

Havia a expectativa de os participantes agirem sem ressalvas quanto a escolha de questões objetivas sem respostas neutras, conforme a descrição na metodologia da pesquisa. Neste caso, após as análises, observou-se que os respondentes escolheram criteriosamente, em virtude da distribuição das respostas positivas, das poucas negativas e de um número expressivo de comentários, tanto de confirmação, quanto de crítica.

O período de envio e respostas dos questionários via e-mail institucional da organização se deu no período de 13/12/2021 a 21/12/2021, data da última resposta recebida.

Para esta parte da pesquisa foram criados 2 textos introdutórios (para envio via e-mail e para introdução ao questionário), o manual de uso da ferramenta computacional, e um questionário com 25 perguntas objetivas, com 4 respostas fechadas e objetivas, sem opção neutra de resposta, conforme explicado na metodologia. Para cada questão há um campo disponível para comentários, para o qual foi incentivado que os respondentes estabelecessem julgamentos de valores, quer em formato de crítica, de sugestão ou de interpretação.

Os textos, questionário, respostas (estatística), comentários e resultado de aprovação/rejeição das questões podem ser observados no apêndice E, deste trabalho.

O universo de respondentes foi o da amostra de 30 pessoas da SDSI, mas em virtude do período de final do ano, houve algumas ausências (4 pessoas se desligaram do NuCDCAer e 5 encontravam-se afastadas em virtude de licenças de saúde ou de férias), perfazendo um total de 21 pessoas convidadas para a primeira rodada do processo, com somente uma abstenção de respondente, até o fechamento da rodada, cujo prazo foi de 8 dias corridos.

Esta quantidade de respondentes é condizente com o observado nos trabalhos de Marques (2018) [53] e de Rocha-Filho [72] já analisados na metodologia.

Como resultado final da rodada 1 e em função da aprovação de todas as questões, do processo de consenso do método Delphi para esta etapa da pesquisa, a tabela 5.6 evidencia a estatística básica e as condições de aprovação/reprovação das questões. Para a definição dos critérios, seguiu-se as recomendações de Rocha-Filho [72], bem como a de Reguant-Álvarez [126], que sugerem o estabelecimento do consenso no intervalo acima de 50% a 80%, sendo tanto mais difícil o atingimento quanto maior for a meta. Ou seja, o consenso é obtido a partir da maioria aceitar as hipóteses ou questionamentos, e a reprovação poderia ficar como sendo uma baixa aceitação ou alta rejeição aos questionamentos.

Para este trabalho optou-se por uma abordagem bastante conservadora, exigindo-se o mínimo, para aprovação de uma questão observando-se o somatório de suas duas respostas positivas sendo igual ou superior a 80%, sendo as questões neste patamar completamente aprovadas, sem necessidade de retestagem. A reprovação comportando valores de aceitação abaixo de 50% ou de rejeição (somatório das respostas negativas) acima de 50%, onde as questões neste patamar seriam eliminadas do processo. Para as demais situações, onde a taxa de aprovação esteja no intervalo entre 50% e abaixo de 80% ocorreria a avaliação dos comentários, reedição das questões nesta situação e geração de nova rodada de questões. Em resumo, segue-se que:

- Respostas POSITIVAS (aceitação): Concordo totalmente, Concordo.
- Respostas NEGATIVAS (rejeição): Discordo totalmente, Discordo.

Fórmula de aprovação/reprovação do consenso de cada questão:

- Aprovação: $\% \text{Concordo totalmente} + \% \text{Concordo} \geq 80\%$
- Reprovação: $\% \text{Discordo totalmente} + \% \text{Discordo} > 50\%$ ou $\% \text{Concordo totalmente} + \% \text{Concordo} < 50\%$
- Sujeita à revisão em outra rodada: $80\% > (\% \text{Concordo totalmente} + \% \text{Concordo}) \geq 50\%$

As 25 questões foram respondidas e as estatísticas básicas de respostas estão evidenciadas na Tabela 5.6.

O apêndice E reflete, além da estrutura da entrevista, a análise das questões aceitas e suas ressalvas (comentários), sendo, no caso desta pesquisa, composto pelos controles e escalas de avaliação dos riscos cibernéticos aceitos como corretos e viáveis para o processo de ARCiber. A tabela 5.6 resume os resultados básicos do consenso obtido no uso do método Delphi.

Tabela 5.6: Resultado da validação da ferramenta via método Delphi

Nº da Pergunta	Nº Respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	% Aprovação	% Reaprovação	Resultado
1	20	60%	40%	0%	0%	100%	0%	Aprovada
2	20	65%	35%	0%	0%	100%	0%	Aprovada
3	20	55%	40%	5%	0%	95%	5%	Aprovada
4	20	65%	35%	0%	0%	100%	0%	Aprovada
5	20	30%	55%	15%	0%	85%	15%	Aprovada
6	20	50%	40%	10%	0%	90%	10%	Aprovada
7	20	60%	30%	5%	5%	90%	10%	Aprovada
8	20	60%	35%	5%	0%	95%	5%	Aprovada
9	20	65%	35%	0%	0%	100%	0%	Aprovada
10	20	60%	35%	5%	0%	95%	5%	Aprovada
11	20	65%	35%	0%	0%	100%	0%	Aprovada
12	20	65%	35%	0%	0%	100%	0%	Aprovada
13	20	45%	45%	10%	0%	90%	10%	Aprovada
14	20	60%	40%	0%	0%	100%	0%	Aprovada
15	20	70%	25%	5%	0%	95%	5%	Aprovada
16	20	70%	25%	5%	0%	95%	5%	Aprovada
17	20	55%	40%	5%	0%	95%	5%	Aprovada
18	20	75%	25%	0%	0%	100%	0%	Aprovada
19	20	75%	25%	0%	0%	100%	0%	Aprovada
20	20	55%	35%	10%	0%	90%	10%	Aprovada
21	20	75%	25%	0%	0%	100%	0%	Aprovada
22	20	65%	35%	0%	0%	100%	0%	Aprovada
23	20	30%	60%	0%	10%	90%	10%	Aprovada
24	20	25%	60%	5%	10%	85%	15%	Aprovada
25	20	45%	40%	5%	10%	85%	15%	Aprovada

Fonte: Autoria própria

Apesar de parecer incomum, para esta pesquisa o questionário revelou uma aprovação de 100% dos controles e das escalas e interface básica da ferramenta em função de fatores que, segundo Rocha-Filho [72], uma seleção de respondentes ou painelistas segundo o termo específico usado pelo autor, pode influenciar as respostas em função de suas experiências profissionais, acadêmicas e áreas de formação, podendo padronizar entendimentos. Este entendimento é corroborado por Marques [53], para o qual a seleção dos especialistas é fundamental, apesar de os autores estudados serem, em sua grande maioria advindos das ciências sociais, onde os temas são mais polêmicos, mais sujeitos à discussão pela característica redução do consenso. Segundo Rozados [74] a técnica Delphi tornou-se uma ferramenta fundamental na área de projeções tecnológicas, permitindo incorporar informações subjetivas em avaliação de objetos compostos por problemas complexos. Logo, pode-se depreender que para as ciências exatas, segundo os mesmos autores, há mais padronização de entendimentos em função de técnicas utilizadas e entendimentos sob uso de escalas exatas, o que pode sugerir o nível de consenso obtido em uma única rodada do método Delphi.

Em segundo lugar, alguns fatores internos ao NuCDCAer podem revelar o sucesso da empreitada de obtenção de dados da avaliação do processo em si. O primeiro deles refere-se ao treinamento e/ou capacitação dos integrantes da SDSI em Segurança/Defesa Cibernética, dependentes diretamente da gestão de riscos, facilitando o entendimento das

necessidades de controles; em segundo lugar, apesar da pouca experiência de alguns integrantes em termos absolutos, durante o processo de interação para a construção do processo de ARCiber, muito aprendizado aconteceu em função deste intercâmbio de informações, produzindo uma capacitação informal e um aumento de maturidade em segurança.

O NuCDCAer é uma organização recém-formada, cujas tecnologias e estruturas ainda estão em processo de formação, e esta organização funciona provisoriamente no bojo de outra instituição já consagrada de longa data, o Centro de Computação da Aeronáutica de Brasília (CCA-BR), com foco em TI, extra-segurança. Em função desta modernidade de criação, está havendo um esforço incomum nesta estruturação, com desenvolvimento de processos, técnicas, métodos e estruturas de ação, além de capacitações diversas que têm motivado o efetivo na persecução de um objetivo comum de desenvolvimento integrado. O sucesso no uso do método Delphi pode se justificar neste sentido, onde a boa-vontade e a presteza nas respostas se evidencia em resultados palpáveis.

Um outro motivo que pode justificar o nível de responsividade é a implantação, mesmo que de forma preliminar, da ferramenta de gestão de governança, riscos e compliance RSA Archer, cujo processo de implantação está diretamente ligado à SGSI, Seção de Gestão da Segurança da Informação, cujo autor deste trabalho é integrante. Esta ferramenta promete e evidencia ser uma possibilidade de interface única aos processos do NuCDCAer em suas diversas atividades, facilitando em alto nível a integração dos trabalhos e esforços, como, por exemplo, a gestão dos ativos, das vulnerabilidades, ameaças e geração de relatórios.

Juntamente com os convites para os respondentes, foram enviados links para a ferramenta (planilha) desenvolvida, ressaltando que se tratava de uma ferramenta didática, que implementaria o processo de ARCiber, o qual seria complementado e disponibilizado via RSA Archer. Foram ainda enviados links para um manual de uso e os textos explicativos informaram sobre o processo de avaliação dos controles a serem implementados. A equipe da SGSI também foi disponibilizada para dirimir eventuais dúvidas e alguns integrantes fizeram uso deste recurso.

Finalmente algumas respostas negativas ou comentários com dúvidas refletiram que alguns integrantes da pesquisa não leram os materiais ou não perguntaram à equipe. Estes respondentes foram diretamente ao link do questionário, mas a quantidade revelou uma parcela pequena, não comprometendo a pesquisa.

Para cada comentário que necessitou de alguma interpretação, esta foi dada e disponibilizada no apêndice E, ao final deste trabalho. Este apêndice oferece as informações completas sobre o processo de pesquisa via método Delphi, como o texto de convite via e-mail, o texto introdutório do questionário, o questionário em si, já contando com a quantidade e qualificação das respostas (estatística básica), os comentários às questões, a

análise dos comentários e finalmente o resumo das estatísticas das questões.

Capítulo 6

Conclusão

Neste tópico são apresentados os resultados obtidos com a pesquisa, seus sucessos, limitações e sugestões para trabalhos futuros, com o objetivo de estender os limites da pesquisa, aumentando sua utilidade como ferramenta científica.

Como uma conclusão geral, observa-se que o resultado foi satisfatório, com os objetivos alcançados e tanto os procedimentos quanto suas validações obtiveram sucesso.

6.1 Resultados obtidos

Dentro dos objetivos propostos pela pesquisa, entende-se que o objetivo geral foi completamente atendido, em função de ter sido criado, executado e validado um processo de avaliação de riscos cibernéticos, para o processo de obtenção de consciência situacional cibernética, o que permitiu o entendimento dos diversos conceitos relacionados à segurança da informação em geral, especializado para a segurança/defesa cibernéticas.

Os conceitos pesquisados permitiram a compreensão da importância da organização recém-criada, o NuCDCAer no contexto da Defesa Cibernética em sua área de atuação (Espaço Cibernético de interesse) e dentro das necessidades do Ministério da Defesa do país. A pesquisa revelou a diferença entre gestão de riscos em geral e a gestão de riscos cibernéticos, ambos baseados em metodologias próprias e tendo por base normativos que sustentam as atividades correlatas. A compreensão do foco em cenários de riscos foi fundamental para o estabelecimento das diferenças conceituais e na formação dos processos de aquisição de consciência situacional cibernética e da avaliação dos riscos cibernéticos.

De posse destes conceitos e entendimentos, buscou-se e obteve-se consenso acerca das necessidades de informações para a criação do processo de identificação, análise e avaliação dos riscos, com vistas a obtenção de um índice quantitativo destes, obtido sob a forma de uma análise baseada em critérios qualitativos, mas que permitiram uma correta avaliação dos riscos em função de valores de vulnerabilidades e criticidades de ativos por meio da

utilização de serviços internos à organização sobre gestão de vulnerabilidades, ameaças e incidentes cibernéticos, permitindo a consolidação de informações de forma plausível e econômica.

Foi desenvolvida uma ferramenta conceitual, que permitiu a validação do processo em si, apesar de ser construída de forma simples, em formato de planilha, mas que produziu resultados importantes e permitiu a avaliação de uma aplicação comercial adquirida pelo órgão ao qual a instituição é subordinada. Esta aplicação não possuía função específica para executar o processo de avaliação de riscos cibernéticos (ARCiber), em especial este feito sob medida para o serviço da instituição, mas permitiu guiar a equipe da empresa no estabelecimento de uma funcionalidade que permitiu a implementação da ARCiber sem necessitar de desenvolvimento de nova aplicação. A ferramenta prototipada pela SGSI permitiu, igualmente reproduzir os resultados obtidos segundo as mesmas entradas de vulnerabilidades para ambas as ferramentas, validando tanto o processo de ARCiber, quanto a precisão da ferramenta adquirida e customizada.

Finalmente foi efetuada uma validação conceitual da ferramenta, por meio da técnica Delphi, em conjunto com os profissionais qualificados do NuCDCAer, a qual verificou a concordância dos profissionais quanto ao aspecto metodológico do processo e quanto aos procedimentos operacionais para a obtenção dos valores de riscos cibernéticos, bem como da validade dos resultados.

Todos estes passos dados em direção à consolidação do NuCDCAer como organização voltada à defesa cibernética revelou um aumento da maturidade em gestão de riscos cibernéticos, em relação à organização da qual foi derivada, o Centro de Computação da Aeronáutica de Brasília (CCA-BR).

Esta organização original possuía a semente dos processos de defesa cibernética e cumpria sua função basicamente como um centro de tratamento de incidentes cibernéticos. A alteração funcional trouxe em seu bojo novas obrigações e uma necessidade de processos mais específicos dentro da grande área da segurança cibernética, mais especificamente a de defesa cibernética, além de aumento da quantidade de técnicos disponíveis, bem como de orçamento ampliado.

A aquisição de treinamentos e de ferramentas como o RSA ARcher foi um ganho visível em termos de ferramentas e as entrevistas para definição dos processos revelaram comentários que indicam um aumento da maturidade nos conhecimentos e nos processos de segurança cibernética e seus processos derivados, observados durante o tempo desta pesquisa, em função do tempo decorrido entre o início da diagramação dos processos e o término deste trabalho.

6.2 Limitações da pesquisa

As limitações impostas à pesquisa não foram resultado de restrições por parte da instituição, mas do limite temporal e metodológico de uma pesquisa de mestrado, que se impõe como um aprofundamento sobre assunto pontual. Houve completa autonomia por parte do pesquisador no acesso às informações e liberdade nos procedimentos empreendidos. O tempo se mostrou o maior limitante, pois ainda há pouco material e profissionais no campo específico da defesa cibernética, motivo pelo qual muitos assuntos foram obtidos de literaturas de segurança da informação, segurança cibernética, manuais militares de defesa em geral e cibernética, tanto nacionais quanto os internacionais disponíveis.

6.3 Sugestões para aprofundamento e pesquisas correlatas

Em virtude da limitação temática da pesquisa, verifica-se que muitos outros pontos podem ser estendidos e outros assuntos abordados. Observa-se que foram analisados conceitos de avaliação de riscos, sem, no entanto, levar-se em conta os outros subprocessos envolvidos na gestão de riscos, como o tratamento destes, em virtude de o objetivo focar na identificação e quantificação do nível de risco em dado momento por ativos críticos ou relevantes. Logo, os procedimentos de tratamento ou de resposta a incidentes cibernéticos podem ser um bom campo de pesquisa futura.

Um segundo ponto a ser considerado é diretamente ligado ao parágrafo anterior, são os procedimentos de gestão da continuidade dos negócios ou dos processos críticos, alinhados com os procedimentos de tratamento ou de respostas aos incidentes cibernéticos, como forma de garantir a devida resiliência cibernética ao espaço cibernético de interesse da organização que implementa tais processos.

Uma terceira sugestão passa pela implementação de processos de gestão de ameaças, igualmente ligados aos processos de gestão de riscos cibernéticos, os quais possuem estrutura processual bastante interessante e ampla para uma pesquisa, mas similar aos processos de gestão de continuidade, iniciam-se pelas mesmas atividades, com a identificação do contexto da organização, inventário e classificação dos ativos relevantes, e consequentemente avaliação dos principais riscos, logo, são uma extensão natural ao tema desta pesquisa.

Referências

- [1] Brasil. Ministério da Defesa: *Política e Estratégia Nacional de Defesa.*, 2012. 1, 3, 73
- [2] Endsley, M. R.: *Toward a theory of situation awareness in dynamic systems.* Human Factors, 37(1):32–64, 1995, ISSN 00187208. 1, 13, 14, 17, 22, 23, 41, 44, 80
- [3] ABNT: *ABNT NBR ISO/IEC 27005:2011 - Tencologia da Informação - Técnicas de Segurança - Gestão de Riscos de Segurança da Informação*, 2011. 2, 32, 33, 35, 36, 54, 83, 84, 85, 87, 91
- [4] Sonicwall: *2018 SonicWall Cyber Threat Report.* Relatório Técnico July, 2018. 2
- [5] Sonicwall: *2021 SonicWall Cyber Threat Report.* Relatório Técnico, 2021. 3, 5
- [6] Brasil. Presidência da República.: *Decreto N° 10.222, de 5 de fevereiro de 2020 - Estratégia Nacional de Segurança Cibernética (ENSC).* 2020. 3, 4, 75
- [7] Brasil. Ministério da Defesa.: *Doutrina Militar de Defesa Cibernética - MD31- M-08.*, 2014. 5, 30, 36, 39, 53, 62, 73, 74, 78, 80, 88
- [8] Lakatos, Eva Maria e Marina de Andrade Marconi: *Fundamentos de Metodologia Científica.* Atlas, São Paulo, ^a8^aa edição, 2017, ISBN 9788597010763. 7, 61, 63, 64, 66
- [9] Mariano, Ari Melo e Maíra Santos Rocha: *Revisão da literatura: apresentação de uma abordagem integradora.* Em *AEDEM International Conference*, volume 18, páginas 427–442, 2017. 7, 8, 15, 20, 21
- [10] Franke, Ulrik e Joel Brynielsson: *Cyber situational awareness—a systematic review of the literature.* Computers & security, 46:18–31, 2014. 13, 14, 17, 22
- [11] Barford, Paul, Marc Dacier, Thomas G Dietterich, Matt Fredrikson, Jon Giffin, Sushil Jajodia, Somesh Jha, Jason Li, Peng Liu, Peng Ning *et al.*: *Cyber sa: Situational awareness for cyber defense.* Em *Cyber situational awareness*, páginas 3–13. Springer, 2010. 14, 22
- [12] Webb, Jeb, Atif Ahmad, Sean B Maynard e Graeme Shanks: *A situation awareness model for information security risk management.* Computers & security, 44:1–15, 2014. 14, 17, 22

- [13] Tadda, George P. e John S. Salerno: *Overview of Cyber Situation Awareness*. *Advances in Information Security*, 46:15–35, 2010, ISSN 15682633. 14, 42, 43, 44, 45, 46, 80, 81, 82, 92, 93, 94
- [14] Eck, Nees Jan van e Ludo Waltman: *Vosviewer*, 2021. <https://www.vosviewer.com/>, acesso em 29 set 2021. 17, 19, 20, 21
- [15] Yang, Shanchieh J, Adam Stotz, Jared Holsopple, Moises Sudit e Michael Kuhl: *High level information fusion for tracking and projection of multistage cyber attacks*. *Information Fusion*, 10(1):107–121, 2009. 17
- [16] Endsley, Mica R: *Final reflections: situation awareness models and measures*. *Journal of Cognitive Engineering and Decision Making*, 9(1):101–111, 2015. 17, 21, 23
- [17] Holm, Hannes, Mathias Ekstedt e Dennis Andersson: *Empirical analysis of system-level vulnerability metrics through actual attacks*. *IEEE Transactions on dependable and secure computing*, 9(6):825–837, 2012. 17, 22, 23
- [18] Granasen, Magdalena e Dennis Andersson: *Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study*. *Cognition, Technology & Work*, 18(1):121–143, 2016. 17
- [19] Vykopal, Jan, Martin Vizváry, Radek Oslejsek, Pavel Celeda e Daniel Tovarnak: *Lessons learned from complex hands-on defence exercises in a cyber range*. Em *2017 IEEE Frontiers in Education Conference (FIE)*, páginas 1–8. IEEE, 2017. 17
- [20] FIRST.org: *Common vulnerability scoring system version 3.1: Specification document*. 2019. <https://www.first.org/cvss/specification-document>, acesso em 04 mai 2021. 18, 89, 92, 96, 103
- [21] Mariano, Ari, Rosario Cruz e Jorge Arenas-Gaitán: *Meta análises como instrumento de pesquisa: Uma revisão sistemática da bibliografia aplicada ao estudo das alianças estratégicas internacionais. meta analysis as a tool of research: A systematic review of bibliography applied study of international strategic alliances*. setembro 2011. 18
- [22] Champion, Michael A, Prashanth Rajivan, Nancy J Cooke e Shree Jariwala: *Team-based cyber defense analysis*. Em *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, páginas 218–221. IEEE, 2012. 21
- [23] Gordon, Lawrence A e Martin P Loeb: *The economics of information security investment*. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002. 21
- [24] Anderson, Ross e Tyler Moore: *The economics of information security*. *science*, 314(5799):610–613, 2006. 21
- [25] Young, Derek, Juan Lopez Jr, Mason Rice, Benjamin Ramsey e Robert McTasney: *A framework for incorporating insurance in critical infrastructure cyber risk strategies*. *International Journal of Critical Infrastructure Protection*, 14:43–57, 2016. 21, 23

- [26] Zhu, Quanyan, Juntao Chen e Tamer Başar: *Dynamic contract design for systemic cyber risk management of interdependent enterprise networks*. *Dynamic Games and Applications*, páginas 1–32, 2020. 21, 23
- [27] Xu, Zhiheng e Quanyan Zhu: *A cyber-physical game framework for secure and resilient multi-agent autonomous systems*. Em *2015 54th IEEE Conference on Decision and Control (CDC)*, páginas 5156–5161. IEEE, 2015. 21, 23
- [28] Okhravi, Hamed, Kevin M Carter e James F Riordan: *A game theoretic approach to strategy determination for dynamic platform defenses*. Em *Proceedings of the first ACM workshop on moving target defense*, páginas 21–30, 2014. 21
- [29] Hong, Junho, Reynaldo F Nuqui, Anil Kondabathini, Dmitry Ishchenko e Aaron Martin: *Cyber attack resilient distance protection and circuit breaker control for digital substations*. *IEEE Transactions on Industrial Informatics*, 15(7):4332–4341, 2018. 21, 22, 23
- [30] Sridhar, Siddharth e Manimaran Govindarasu: *Model-based attack detection and mitigation for automatic generation control*. *IEEE Transactions on Smart Grid*, 5(2):580–591, 2014. 22
- [31] Ganesan, Rajesh, Sushil Jajodia e Hasan Cam: *Optimal scheduling of cybersecurity analysts for minimizing risk*. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 8(4):1–32, 2017. 22
- [32] Srinivas, Jangirala, Ashok Kumar Das e Neeraj Kumar: *Government regulations in cyber security: Framework, standards and recommendations*. *Future Generation Computer Systems*, 92:178–188, 2019. 22
- [33] Tang, MingJian, Mamoun Alazab e Yuxiu Luo: *Big data for cybersecurity: Vulnerability disclosure trends and dependencies*. *IEEE Transactions on Big Data*, 5(3):317–329, 2017. 22
- [34] Touhiduzzaman, Md, Adam Hahn e Anurag K Srivastava: *A diversity-based substation cyber defense strategy utilizing coloring games*. *IEEE Transactions on Smart Grid*, 10(5):5405–5415, 2018. 22
- [35] Yang, Lu Xing, Pengdeng Li, Xiaofan Yang e Yuan Yan Tang: *Security evaluation of the cyber networks under advanced persistent threats*. *IEEE access*, 5:20111–20123, 2017. 22
- [36] ABNT: *ABNT NBR ISO 27001:2013 - Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos*, 2013. 25, 103, 104, 105, 106, 107, 108
- [37] ABNT: *ABNT NBR ISO 27002:2013 - Tecnologia da Informação-Técnicas de Segurança – Código de Prática para controles de segurança da informação*, 2013. 25, 32

- [38] ABNT: *ABNT NBR ISO/IEC 27032/2015 - Tecnologia da Informação - Técnicas de Segurança - Diretrizes para Segurança Cibernética*, 2015. 26, 27, 28, 29, 30, 54, 107, 108
- [39] Brasil. Ministério da Defesa. Exército Brasileiro.: *EB70-MC-10.232 - Manual de Campanha de Guerra Cibernética*, 2017. 30, 31, 75
- [40] ABNT: *ABNT NBR ISO 31010:2012 - Gestão de riscos — Diretrizes*, 2018. 31, 33, 35, 36
- [41] Aven, Terje: *The science of risk analysis: Foundation and practice*. Routledge, 2020. 31
- [42] Refsdal, Atle, Bjørnar Solhaug e Ketil Stølen: *Risk management*, volume 0. Springer International Publishing, 2015, ISBN 9783319235691. 31, 32, 36, 37, 38, 54, 84, 88, 89
- [43] Flores, Bráulio Cançado; Ornelas, Éliton Ataíde ; Dias Leônidas Eduardo: *Fundamentos de Combate a Incêndio Manual de Bombeiros*. Corpo de Bombeiros Militar do Estado de Goiás, Goiânia, GO, 2016. 32
- [44] Cepik, Marco, Diego Rafael Canabarro e Thiago Borne: *A Securitização do Ciberespaço e o Terrorismo: Uma Abordagem Crítica*, 2014, ISBN 9788578111953. 39
- [45] Jackson, Camile Marie: *Estonian cyber policy after the 2007 attacks: Drivers of change and factors for success*. New Voices in Public Policy, 7(1), 2013. 39, 40
- [46] Michael J. Assante, Robert M. Lee, Tim Conway: *Analysis of the cyber attack on the ukrainian power grid*. Electricity Information Sharing and Analysis Center (E-ISAC). "https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf". 40
- [47] Michael J. Assante, Robert M. Lee, Tim Conway: *Ics defense use case no. 6: Modular ics malware*. Electricity Information Sharing and Analysis Center (E-ISAC). "https://www.eisac.com/cartella/Asset/00006542/TLP_WHITE_E-ISAC_SANS_Ukraine_DUC_6_Modular_ICs_Malware_Final.pdf?parent=64412". 40
- [48] Silva, Walbery Nogueira de Lima e: *Atuação colaborativa da defesa cibernética na proteção de infraestruturas críticas de interesse para a defesa nacional*. Data & Hertz, 1(1 jan./Dez):52–59, 2020. 40, 76, 77
- [49] CCDCOE: *The NATO Cooperative Cyber Defence Centre of Excellence - CCDCOE*, 2021. <https://ccdcoe.org/>, acesso em 21 out 2021. 41
- [50] CCDCOE: *Cyberlaw Toolkit*, 2021. <https://cyberlaw.ccdcoe.org/wiki/>, acesso em 21 out 2021. 41
- [51] Alberts, David S, John J Garstka, Richard E Hayes e David A Signori: *Understanding information age warfare*. Relatório Técnico, Assistant Secretary Of Defense (C3i/Command Control Research Program . . . , 2001. 44

- [52] Henriqson, Éder, Guido César Carim Júnior, Tarcísio Abreu Saurin e Fernando Gonçalves Amaral: *Consciência situacional, tomada de decisão e modos de controle cognitivo em ambientes complexos*. Production, 19(3):433–444, 2009. 45
- [53] Marques, Dick e Estevam Luconi: *A integração entre a inteligência de imagens e a consciência situacional*. A Defesa Nacional, 106(837), 2018. 45, 69, 128, 129
- [54] Jung, Carlos Fernando: *Metodologia para pesquisa e desenvolvimento: aplicada a novas tecnologias, produtos e processos*. Axcel Books, 2004. 48
- [55] Wazlawick, Raul Sidnei: *Metodologia de pesquisa para ciência da computação*. Elsevier, ^{a2^{aa}} edição, 2014, ISBN 978-85-352-7782-1. 48, 49
- [56] Azevedo, Rogério Cabral de e Leonardo Ensslin: *Metodologia da Pesquisa para Engenharias*. 2020, ISBN 978-65-00-10268-0. 49
- [57] Botelho, Joacy Machado e Vilma Aparecida Gimenes da Cruz: *Metodologia científic*. Pearson Education do Brasi, São Paulo, 2013, ISBN 9788543000060. 49
- [58] Baldam, Roquemar, Rogerio Valle e Henriq Rozenfeld: *Gerenciamento de Processos de Negócio-BPM: uma referência para implantação prática*. Elsevier Brasil, 2014. 54, 67
- [59] BPM, ABPMP: *Guia para o gerenciamento de processos de negócio corpo comum de conhecimento - CBOOK*, volume 3. 2013. 54, 67
- [60] LLC, RSA Security: *Rsa archer platform*, 2021. <https://www.rsa.com/de-de/products/integrated-risk-management/archer-platform>, acesso em 12 mai 2021. 56, 119, 120, 121, 122, 123, 124
- [61] Vianna, Eduardo Wallier: *Análise do comportamento informacional na gestão da segurança cibernética da administração pública federal*. Tese de Mestrado, Universidade de Brasília, Brasília, 2015. 58, 61
- [62] Vieira, Sonia: *Como elaborar questionários*. Atlas, São Paulo, SP, 2009. 63, 70, 97
- [63] MITRE Corporation: *Mitre attéck matrix*, 2021. <https://attack.mitre.org/matrices/enterprise/>, acesso em 01 jul 2021. 64, 87
- [64] MITRE Corporation: *Mitre d3fend matrix*, 2021. <https://d3fend.mitre.org/>, acesso em 30 jun 2021. 64, 87
- [65] The National Cyber Security Centre: *Cybok version 1.0 © crown copyright, the national cyber security centre*, 2019. <https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf>, acesso em 12 jul 2021. 64
- [66] National Institute of Standards and Technology - NIST: *Nist cybersecurity framework version 1.1*, 2018. <https://nvd.nist.gov/>, acesso em 14 jul 2021. 64, 87, 101, 103, 104, 105, 106, 107, 108
- [67] Likert, Rensis: *A technique for the measurement of attitudes (archives of psychology, no: 140)*. New York City: Columbia University, 7(3), 1932. 65, 69

- [68] ABNT: *ABNT NBR ISO 31010:2018 - Gestão de riscos — Técnicas para o processo de avaliação de riscos*, 2012. 66
- [69] Rosemberg, Carlos, Albert Schilling, Cristianne Bastos e Rodrigo Araripe: *Prototipação de software e design participativo: uma experiência do atlântico*. IHC, 8:312–315, 2008. 67
- [70] Wazlawick, Raul: *Engenharia de software: conceitos e práticas*. Elsevier Editora Ltda., 2019. 67
- [71] Castilla-Polo, Francisca, María del Consuelo Ruiz-Rodríguez e Carlos Delgado-Marfil: *La técnica delphi para la validación de escalas de medida: las variables innovación y reputación dentro de almazaras cooperativas*. REVESCO. Revista de Estudios Cooperativos, 136:e71852, nov. 2020. <https://revistas.ucm.es/index.php/REVE/article/view/71852>, acesso em 17 out 2021. 68, 69
- [72] Rocha-Filho, César Ramos: *Método e-delphi modificado: um guia para validação de instrumentos avaliativos na área da saúde*. Brazil Publishing, Curitiba, PR, 2019. 68, 69, 128, 129
- [73] Oliveira, Joelma de Oliveira, Maíra Murrieta Costa, Marina Ferreira Wille e Patricia Zeni Marchiori: *Introdução ao método delphi*. 2008. 68
- [74] Rozados, Helen Frota: *O uso da técnica delphi como alternativa metodológica para a área da ciência da informação*. Em *Questão*, 21(3):64–86, 2015. 69, 70, 126, 127, 129
- [75] Hill, Manuela Magalhães e Andrew Hill: *A construção de um questionário*. 1998. https://repositorio.iscte-iul.pt/bitstream/10071/469/4/DINAMIA_WP_1998-11.pdf, acesso em 18 dez 2021. 70
- [76] Brasil. Presidência da República.: *Decreto nº 6.703, de 18 de dezembro de 2008*, 2008. 72
- [77] Brasil. Gabinete de Segurança Institucional.: *Portaria Nº 45, de 8 de setembro de 2009*. Diário Oficial da União nº 172- Seção 1, de 09 de setembro de 2009., páginas 8–9, 2009. 72
- [78] Canongia, Claudia e Raphael Mandarino Junior: *Livro Verde: segurança cibernética no Brasil*. 2010. 72
- [79] Brasil. Ministério da Defesa: *Diretriz Ministerial nº 14. Integração e Coordenação dos Setores Estratégicos de Defesa*, 2009. 72
- [80] Brasil. Ministério da Defesa.: *Glossário das Forças Armadas - MD35-G-01*. 2015. 73
- [81] Brasil. Ministério da Defesa.: *Portaria Normativa nº 2.777/MD, de 27 de outubro de 2014*, 2014. 75

- [82] Brasil. Ministério da Defesa.: *Política para o Sistema Militar de Comando e Controle - MD31-P-01*. 2015. 75
- [83] Brasil. Presidência da República. Controladora-Geral da União: *Instrução Normativa Conjunta nº 1- PR/CGU/2016.*, 2016. 75
- [84] Brasil. Presidência da República.: *Decreto 9.637/2018 - Política Nacional de Segurança da Informação - PNSI*, 2018. 75
- [85] Brasil. Presidência da República.: *Decreto 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas - PNSIC*, 2018. 75, 76, 112
- [86] Brasil. Comando da Aeronáutica: *Militares da fab participam de exercício de defesa cibernética*, 2011. <https://www.fab.mil.br/noticias/mostra/38012/>, acesso em 01 nov 2021. 77
- [87] Brasil. Ministério da Defesa. Comando da Aeronáutica.: *ICA 7-42 Gerenciamento de Incidentes de Segurança em Redes de Computadores no Comando da Aeronáutica*, 2016. 81
- [88] Evangelista, João Rafael Gonçalves, Dacyr Dante de Oliveira Gatto e Renato José Sassi: *Classificação por ranqueamento de acesso: Análise web em ferramentas de inteligência de fontes abertas*. Em *VII Congresso Brasileiro de Engenharia de Produção – Ponta Grossa, PR: 2018*, São Paulo, 2018. 81
- [89] Glassman, Michael e Min Ju Kang: *Intelligence in the internet age: The emergence and evolution of open source intelligence (osint)*. *Computers in Human Behavior*, 28(2):673–682, 2012. 81
- [90] Kaffenberger, Lincoln e Emanuel Kopp: *Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment*. Carnegie Endowment for International Peace., 2019. 85, 86, 87
- [91] Tzu, Sun: *A arte da guerra*. Editora Schwarcz-Companhia das Letras, 2019. 86
- [92] Li, Jason, Xinming Ou e Raj Rajagopalan: *Uncertainty and risk management in cyber situational awareness*. *Cyber Situational Awareness*, páginas 51–68, 2010. 86
- [93] Paté-Cornell, M Elisabeth, Marshall Kuypers, Matthew Smith e Philip Keller: *Cyber risk management for critical infrastructure: a risk analysis model and three case studies*. *Risk Analysis*, 38(2):226–241, 2018. 86, 87, 93
- [94] Lockheed Martin: *The cyber kill chain*. 2021. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>, acesso em 02 set 2021. 87
- [95] Doynikova, Elena e Igor Kotenko: *Cvss-based probabilistic risk assessment for cyber situational awareness and countermeasure selection*. Em *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*, páginas 346–353. IEEE, 2017. 88, 89

- [96] MITRE Corporation: *www.cvedetails.com*, 2021. <https://www.cvedetails.com/>, acesso em 10 set 2021. 89, 90
- [97] Kaspersky inc.: *Kaspersky resource center*, 2021. <https://www.kaspersky.com.br/resource-center/threats>, acesso em 18 set 2021. 90
- [98] McAfee Inc.: *Mcafee enterprise threat center*, 2021. <https://www.mcafee.com/enterprise/en-us/threat-center.html>, acesso em 10 set 2021. 90
- [99] Microsoft Inc.: *Microsoft security blog*, 2021. <https://www.microsoft.com/security/blog/>, acesso em 10 out 2021. 90
- [100] National Institute of Standards and Technology - NIST: *Nvd - national vulnerability database*, 2021. <https://nvd.nist.gov/>, acesso em 10 set 2021. 90
- [101] Cybersecurity Infrastructures Security Agency - CISA: *Cybersecurity infrastructures security agency alerts*, 2021. <https://us-cert.cisa.gov/ncas/alerts/2021>, acesso em 10 out 2021. 90
- [102] Center for Internet Security - CIS: *Center for internet security cybersecurity threats (cis ct)*, 2021. <https://www.cisecurity.org/cybersecurity-threats/>, acesso em 10 out 2021. 90
- [103] Brasil. Gabinete de Segurança Institucional.: *Norma Complementar nº 8 da Instrução Normativa nº 1. Gestão de ETIR: Diretrizes para gerenciamento de incidentes em redes computacionais dos órgãos da APF*. Norma Complementar nº 8 da Instrução Normativa nº 1, páginas 8–9, 2010. 90, 105
- [104] Radanliev, Petar, David Charles De Roure, Razvan Nicolescu, Michael Huth, Rafael Mantilla Montalvo, Stacy Cannady e Peter Burnap: *Future developments in cyber risk assessment for the internet of things*. *Computers in industry*, 102:14–22, 2018. 93
- [105] Módulo Security Solutions SA: *Módulo risk manager*, 2021. <https://www.modulo.com.br/moduloriskmanager/>, acesso em 10 out 2021. 95
- [106] Tribunal Regional do Trabalho da 11ª Região: *Processo de gestão de riscos de tic*, 2018. https://governanca.trt11.jus.br/images/Processo_de_Gest%C3%A3o_de_Riscos.pdf, acesso em 02 out 2021. 95
- [107] Tribunal de Justiça do Estado do Ceará: *Norma de gestão de riscos – metodologia de gestão de riscos de segurança da informação*, 2018. <https://www.tjce.jus.br/wp-content/uploads/2019/09/anexo-vi-portaria-1186-2018-norma-de-gestao-de-risco.pdf>, acesso em 15 jul 2021. 95
- [108] Brasil. Ministério da Saúde. DATASUS: *Metodologia de gestão de riscos do ministério da saúde*, 2015. https://datasus.saude.gov.br/wp-content/uploads/2019/12/MS-Metodologia-de-Gesto-de-Riscos_v20141105.pdf, acesso em 15 set 2021. 95

- [109] Brasil. Tribunal de Contas da União.: *Roteiro de Auditoria de Gestão de Riscos*, 2017. 96, 109, 110
- [110] Chiavenato, Idalberto: *Introdução à Teoria Geral da Administração*. Editora Manoles, Barueri, SP, 2014, ISBN 978-85-204-3792-6. 97
- [111] U.S. Department of Commerce: *National institute of standards and technology*, 2021. <https://www.nist.gov/>, acesso em 30 out 2021. 100
- [112] The MITRE Corporation: *The mitre corporation*, 2021. <https://www.mitre.org/>, acesso em 20 set 2021. 100
- [113] Center for Internet Security - CIS: *Cis critical security controls (cis controls) version 8*, 2021. <https://www.cisecurity.org/controls/v8/>, acesso em 05 out 2021. 103, 104, 105, 106, 107
- [114] National Institute of Standards and Technology - NIST: *Nist special publication 800-53 revision 4 - security and privacy controls for federal information systems and organizations*, 2021. <http://dx.doi.org/10.6028/NIST.SP.800-53r4>, acesso em 02 jul 2021. 103, 106
- [115] Brasil.Secretaria-Geral: *Lei nº 13.709, de 14 de agosto de 2018 - lei geral de proteção de dados pessoais (lgpd)*. 2021. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm, acesso em 01 jul 2021. 104, 105
- [116] Brasil.Secretaria-Geral: *Lei nº 12.965, de 23 de abril de 2014 - estabelece princípios, garantias, direitos e deveres para o uso da internet no brasil*. 2021. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm, acesso em 01 jul 2021. 105
- [117] Brasil. Ministério da Defesa.Comando da Aeronáutica: *Norma de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica (NSCA 7-13)*. 2013. 105, 106, 107, 108
- [118] Brasil. Ministério da Defesa.Comando da Aeronáutica: *Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações no Comando da Aeronáutica (ICA 200-8)*. 2019. 105, 108
- [119] ABNT: *ABNT NBR ISO 22301:2013 - Segurança da sociedade — Sistema de gestão de continuidade de negócios – Requisitos*, 2013. 105, 106
- [120] Brasil. Gabinete de Segurança Institucional.: *Norma Complementar nº 6 da Instrução Normativa nº 1. Gestão de continuidade de negócios em segurança da informação e comunicações*. Norma Complementar nº 6 da Instrução Normativa nº 1, página 7, 2009. 105, 106
- [121] Brasil. Ministério da Defesa.Comando da Aeronáutica: *Gestão de Continuidade dos Serviços nos Elos Especializados do Sistema de Tecnologia da Informação do Comando da Aeronáutica (ICA 7-1)*. 2015. 105, 106

- [122] Brasil. Gabinete de Segurança Institucional.: *Norma Complementar nº 5 da Instrução Normativa nº 1. Criação de equipes de tratamento e resposta a incidentes em redes computacionais - ETIR*. Norma Complementar nº 5 da Instrução Normativa nº1, página 7, 2009. 105
- [123] National Institute of Standards and Technology - NIST: *Nist special publication 800-115 - technical guide to information security testing and assessment*, 2008. <https://csrc.nist.gov/publications/detail/sp/800-115/final>, acesso em 10 jul 2021. 108
- [124] Brasil. Ministério da Defesa. Comando da Aeronáutica: *Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ICA205-47)*. 2015. 108
- [125] Brasil. Tribunal de Contas da União.: *Portal Web Institucional*, 2021. <https://portal.tcu.gov.br/institucional/conheca-o-tcu/competencias/>, acesso em 251 out 2021. 109
- [126] Reguant-Álvarez, Mercedes e Mercè Torrado Fonseca: *El método delphi*. REIRE. Revista d'Innovació i Recerca en Educació, 2016, vol. 9, num. 2, p. 87-102, 2016. 128

Apêndice A

Entrevista estruturada para qualificação dos profissionais do NuCDCAer

Entrevista estruturada para caracterização da amostra dos profissionais de SC/DC do NuCDCAer

Esta entrevista buscou coletar subsídios para a compreensão da composição das equipes como um todo para o entendimento processo de avaliação de riscos cibernéticos para o NuCDCAer. Para isto foi utilizada, preferencialmente a forma estruturada (Vieira, 2009), com questões fechadas, com tabulação dos dados em planilha MS Excel 365.

A amostra, para a obtenção das informações foi composta pelos profissionais da Subdivisão de Segurança da Informação, que estão em atividade no momento da avaliação. Esta amostra não condiz com todo o efetivo da subdivisão em virtude de a organização estar em processo de reorganização e diversas pessoas estarem em atividade estranha ao foco da pesquisa. Foram entrevistadas 30 pessoas no total, para a compreensão da população ativa de técnicos em SC/DC, incluindo-se os líderes e o autor desta pesquisa.

A avaliação desta entrevista produziu uma qualificação do efetivo em termos de conhecimento e experiência profissional e o entendimento do que se necessita em termos educacionais para a consecução das atividades em segurança/defesa cibernética (SC/DC), auxiliando na produção da especificação do processo de avaliação de riscos cibernéticos, especificamente na geração do índice de riscos cibernéticos (IRC).

A finalidade é a identificação e qualificação da amostra da pesquisa para todas as entrevistas ou respostas a questionários subsequentes, baseado no trabalho de Viana (2015), cujo foco foi o de interpretação das necessidades informacionais dos profissionais de segurança cibernética, em instituições da Administração Pública Federal, coincidentemente necessário para a qualificação dos profissionais do NuCDCAer, foco deste estudo atual.

Para este formulário entregue, com 9 perguntas, a necessidade foi somente a da identificação do perfil profissional dos profissionais da SDSI. Não houve identificação pessoal nem de quantidades de profissionais por tipo de perfil, somente os perfis e proporções por nível de atividade/treinamento/capacitação.

Questões oferecidas aos entrevistados:

1. Sexo/gênero:

- a) Feminino b) Masculino

2. Idade:

- a) Até 25 anos b) 25 a 29 anos c) 30 a 39 anos
d) 40 a 49 anos e) Mais de 50 anos

3. Com respeito a sua **experiência profissional** em segurança/defesa cibernética **em geral (incluindo qualquer tempo fora da organização)** em qual alternativa de tempo acumulado, contínuo ou não, o(a) Sr(a) enquadra-se:

- a) 0 a 6 meses b) 6 meses a 2 anos c) 2 a 5 anos
d) 5 a 7 anos e) 7 a 10 anos f) Mais que 10 anos

4. Com respeito a sua **experiência profissional** em segurança/defesa cibernética **na organização** sob pesquisa em qual alternativa de tempo acumulado, contínuo ou não, o(a) Sr(a) enquadra-se:

- a) 0 a 6 meses b) 6 meses a 2 anos c) 2 a 5 anos
d) 5 a 7 anos e) 7 a 10 anos f) Mais que 10 anos

5. Qual a sua **formação educacional/acadêmica mais elevada** concluída?

- a) Ensino Médio b) Graduação c) Pós-graduação Lato Sensu
d) Mestrado e) Doutorado

6. Qual sua **área de formação acadêmica**?

- a) Ciência da computação b) Sistemas de informação c) Tecnologia em processamento de dados
d) Outras formações correlatas a área de TI e) Outras formações

7. Qual sua **educação mais relevante** utilizada em **segurança/defesa cibernética** (SC/DC)?
(em caso de dúvida selecione mais de uma opção)
- a) () Graduação (em área específica de SC/DC)
 - b) () Pós-graduação Lato Sensu (como uma especialização ou MBA na área de SC/DC)
 - c) () Mestrado (profissional/acadêmico na área de SC)
 - d) () Doutorado (em área afim de SC/DC)
 - e) () Certificações (ISO 27001, OSCP, CISSP, CISM, Security+ etc)
 - f) () Cursos de extensão (RNP, CERT, NIC, outros)
8. Para as suas atividades diárias, com reação à segurança/defesa cibernéticas (SC/DC), sua atuação **PRIMÁRIA** melhor se encaixa em qual das seguintes descrições :
(em caso de dúvida selecione mais de uma opção)
- a) () Liderança ou chefia, planejamento ou gestão para alcançar resultados de mais longo prazo (processos estratégicos), sobre gestão de riscos cibernéticos, gestão da continuidade dos negócios ou de TI, definição de políticas, normas ou procedimentos operacionais (níveis estratégico/tático);
 - b) () Operação de sistemas ou atividades voltadas à gestão de riscos e vulnerabilidades, como defesa ativa, testes de penetração etc. (nível operacional/execução);
 - c) () Operação de sistemas ou atividades voltadas à gestão de ameaças, como inteligência de ameaças ou afins (nível operacional/execução);
 - d) () Operação de sistemas ou atividades voltadas à análises de malware ou perícia cibernética (nível operacional/execução);
 - e) () Operação de atividades voltadas à incidentes de segurança cibernéticos em redes de computadores, como rastreamento, triagem, análise, tratamento e resposta (nível operacional/execução).
9. Para as suas atividades diárias, com reação à segurança/defesa cibernéticas, sua atuação **SECUNDÁRIA** melhor se encaixa em qual das seguintes descrições:
(em caso de dúvida selecione mais de uma opção)
- a) () Liderança ou chefia, planejamento ou gestão para alcançar resultados de mais longo prazo (processos estratégicos), sobre gestão de riscos cibernéticos, gestão da continuidade dos negócios ou de TI, definição de políticas, normas ou procedimentos operacionais (níveis estratégico/tático);
 - b) () Operação de sistemas ou atividades voltadas à gestão de riscos e vulnerabilidades, como defesa ativa, testes de penetração etc. (nível operacional/execução);
 - c) () Operação de sistemas ou atividades voltadas à gestão de ameaças, como inteligência de ameaças ou afins (nível operacional/execução);
 - d) () Operação de sistemas ou atividades voltadas a análises de malware ou perícia cibernética (nível operacional/execução);
 - e) () Operação de atividades voltadas à incidentes de segurança cibernéticos em redes de computadores, como rastreamento, triagem, análise, tratamento e resposta (nível operacional/execução).

Análise dos dados demográficos da amostra

Tamanho da amostra 30 participantes (inclusos os líderes de equipe, seção e subdivisão).

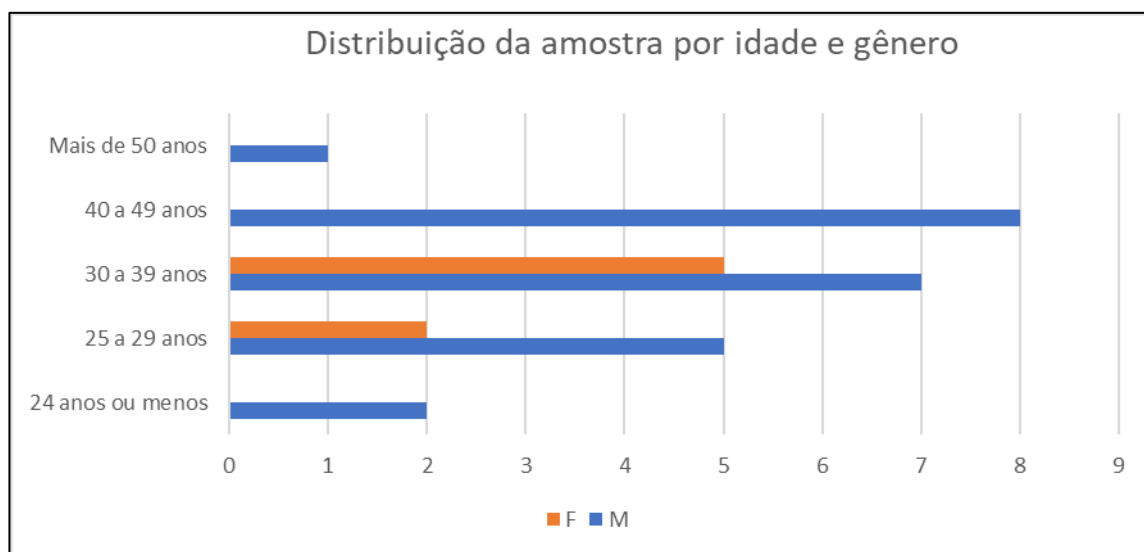


Figura 1 – Distribuição demográfica por idade e gênero

Fonte: autoria própria

Estes dados revelam a predominância do gênero masculino, com exclusividade no início e no final da escala de valores. As duas faixas etárias com maior quantidade de efetivo situam-se no intervalo de 25 a 49 anos, demonstrando que os analistas possuem uma maturidade relativa em termos de idade. Os analistas com menor idade não possuem funções de liderança, ou de decisão nas políticas ou processos.

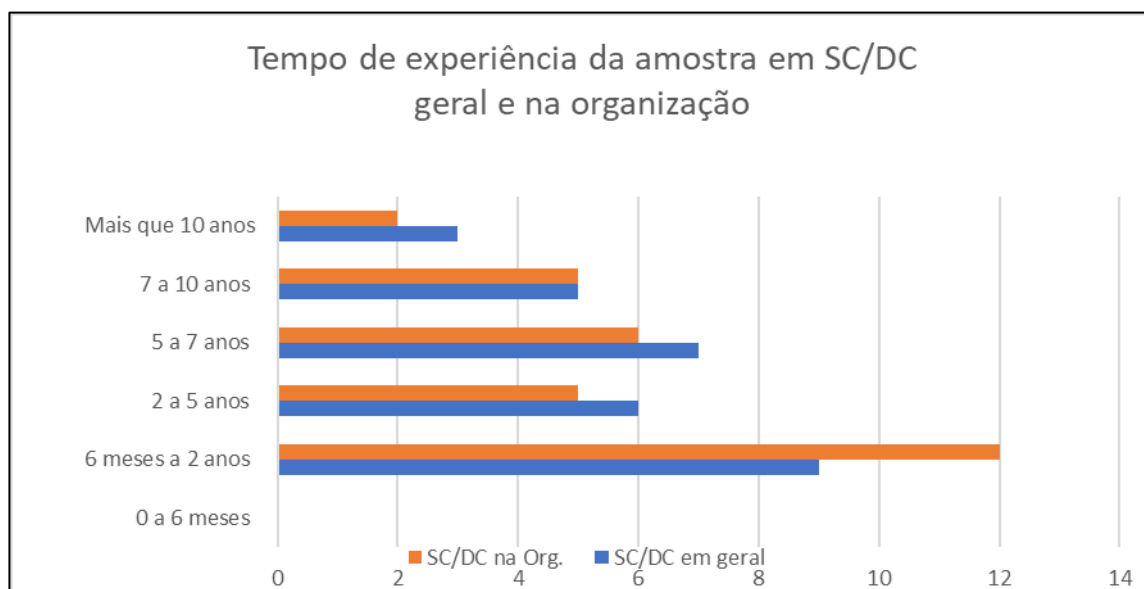


Figura 2 – Distribuição demográfica por experiência profissional em SC/DC

Fonte: autoria própria

O gráfico demonstra que a experiência profissional em SC/DC com maior quantidade de pessoal de forma individual é a faixa de 6 meses a 2 anos de trabalho na área (12 pessoas na organização e 9 em geral), mas observando-se mais a fundo, os profissionais com 2 anos a até mais de 10 anos representam até cerca de 18 pessoas, o que justifica a escolha das equipes para a composição do NuCDCAer.

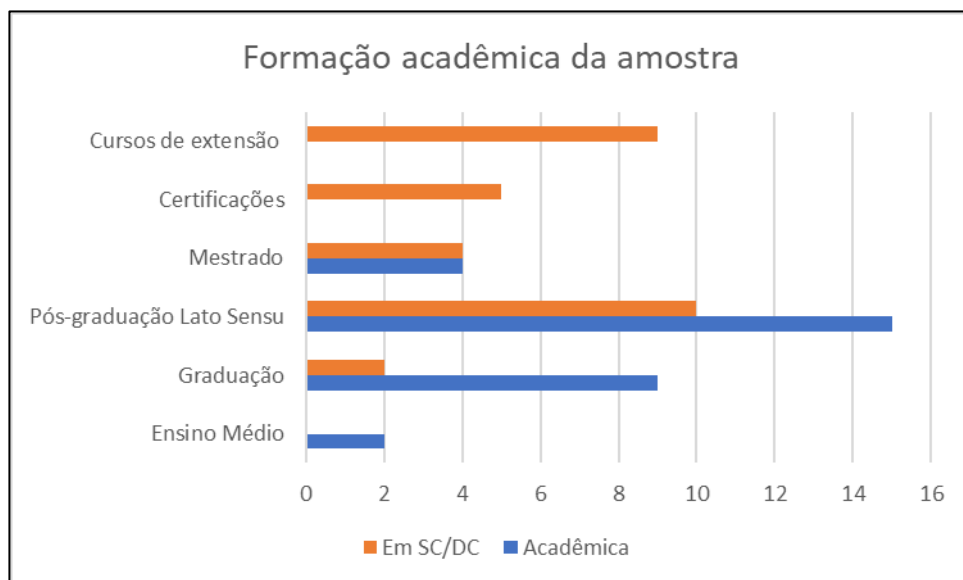


Figura 3 – Distribuição demográfica por nível acadêmico
 Fonte: autoria própria

Quanto à formação acadêmica, e/ou profissional, a maioria absoluta é de pessoas com pós-graduação em nível de especialização na área de SC/DC, mas há uma quantidade considerável de pessoas com graduação acrescida de cursos de extensão e com certificações na área. Há 4 pessoas com nível de mestrado, cerca de 4 outras atualmente cursando (não computadas na amostra, pela escolha de níveis completos, mas nas entrevistas isto foi observado), além de dois profissionais com mestrado e doutorado em andamento (durante a entrevista, mas em pouco tempo depois um deles migrou de profissão, tendo-se retirado do NuCDAer).

Na avaliação das funções foram identificados 10 líderes de equipe, seção e subdivisão em Segurança/Defesa Cibernética, e os gráficos a seguir demonstrarão as análises especificamente voltadas a esta parte da amostra.

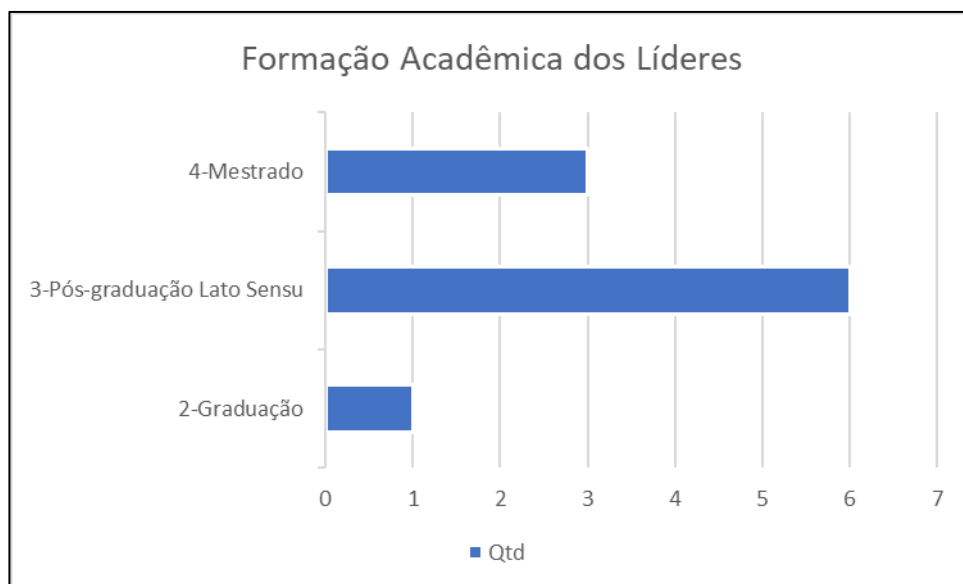


Figura 4 – Distribuição demográfica por nível acadêmico
 Fonte: autoria própria

A formação acadêmica predominante dos líderes continua sendo a pós-graduação lato sensu, mas 3 dos 4 mestres são líderes, enquanto 1 dos líderes possui qualificação acadêmica de graduação.

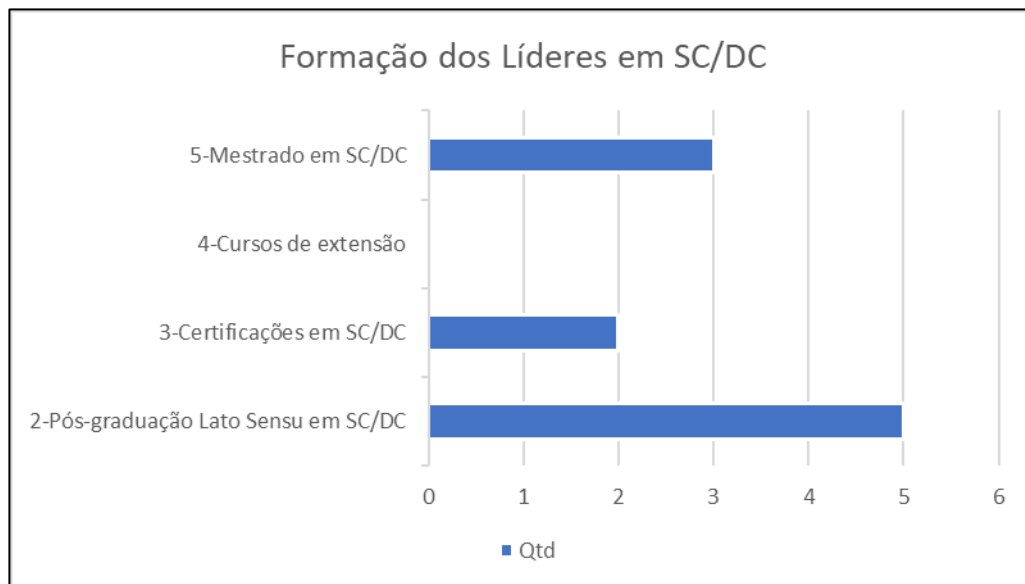


Figura 5 – Distribuição demográfica por formação na área de SC/DC
 Fonte: autoria própria

Para a educação específica em SD/DC quase a totalidade dos especialistas e todos os mestres são formados na área.



Figura 6 – Distribuição demográfica dos líderes por nível experiência profissional em SC/DC
 Fonte: autoria própria

Dentre os 10 líderes 6 possuem mais de 5 anos na área, e a experiência mínima de algum líder é de 6 meses, limitado a 3 pessoas com este nível de experiência.

Os gráficos e as análises feitas revelam que há uma experiência razoável em SC/DC, por profissionais que estão em constante formação evolutiva. O NuCDCAer tem incentivado o treinamento e a capacitação dos executores e dos líderes, oferecendo cursos em conjunto com o ComDCiber sobre defesa/guerra cibernética, além de pós-graduações lato sensu e cursos de extensão em entidades públicas, como o ComDCiber, CERT.br, ENAP, entre outras e em instituições privadas diversas. Todas estas informações sobre educação foram prestadas pelo chefe do NuCDCAer.

Referências:

VIEIRA, Sonia. Como elaborar questionários. In: **Como elaborar questionários**. 2009. p. 159-159.

Vianna, Eduardo Wallier: Análise do comportamento informacional na gestão da segurança cibernética da administração pública federal. Tese de Mestrado, Universidade de Brasília, Brasília, 2015.

Apêndice B

Entrevista semiestruturada para Levantamento dos Processos das Seções do NuCDCAer

Núcleo do Centro de Defesa Cibernética do Comando da Aeronáutica – NuCDCAer
Divisão Técnica
Subdivisão de Segurança da Informação

Entrevista semiestruturada para Gestão de Riscos Cibernéticos da SDSI

(Projeto Integração das Forças Armadas – IFA)

Seção: _____

Entrevistado: _____

Entrevistador(es): _____

Data: ____/____/____

Formato: () Presencial () Videoconferência () Telefone

Este questionário tem a finalidade de estabelecer o contato inicial formal entre a SGSI e as seções da SDSI para identificação das atividades de cada seção, bem como identificar as atividades de interesse dentro do projeto de integração das Forças Armadas – IFA, estabelecido entre o COMAER e o ComDCiber. O projeto visa estabelecer um processo de aquisição de consciência situacional cibernética objetivando a consecução da geração do Nível de Alerta Cibernético (NAC), conforme a Doutrina Militar de Defesa Cibernética (MD31- M-08).

Pergunta 1:

Quais são as macroatividades gerais da seção?

(descreva, se possível com um diagrama, ou forneça informações para a SGSI estabelecer um diagrama preliminar)

Pergunta 2:

Qual o nível de conhecimento da seção acerca do projeto IFA? Se sim, quais atividades entende a seção estar envolvida?

Pergunta 3:

Quais os fatores, segundo o entendimento da seção, são relevantes para avaliar riscos cibernéticos?

Pergunta 4:

Como a seção estabelece a estratégia de levantamento de vulnerabilidades/ameaças dentro de suas funções em segurança cibernética? (autonomia, forma de atendimento de solicitações, escopo, efetua monitoramento ou trabalha sob demanda etc.)

Pergunta 5:

Quais as técnicas de levantamento de vulnerabilidades/ameaças cibernéticas são utilizadas? Em que situações são utilizadas?

Pergunta 6:

Como a seção estabelece a divulgação das atividades em gestão de riscos cibernéticos? (Relatórios, Índices, Avisos/Alertas etc.)

Apêndice C

Entrevista semiestruturada para
entendimento na criação do IRC

Entrevista semiestruturada para subsídio ao entendimento na criação do Índice de Riscos Cibernéticos (IRC):

Esta entrevista buscou coletar subsídios para a compreensão da geração do índice de Riscos Cibernéticos (IRC) para o processo de avaliação de riscos cibernéticos para o NuCDCAer. Segundo Vieira (2009) entrevistas buscam opiniões, atitudes, ideias, juízos em forma de conhecimentos úteis acerca de um tema estabelecido.

Nesta entrevista foi utilizada, preferencialmente a forma semiestruturada (Vieira, 2009), com questões abertas, exceto na coleta dos dados demográficos de interesse para esta pesquisa, quando foram usadas perguntas fechadas, para facilitação da tabulação.

A amostra, para a obtenção das informações acerca do processo de Avaliação de Riscos Cibernéticos (ARCiber) foi composta pelos profissionais com nível de liderança de equipes ou de chefia de estrutura da organização (Divisão, Subdivisão, Seção). Foram entrevistadas 10 pessoas com este perfil. Para a compreensão da população de técnicos em SC/DC foi utilizado todo o efetivo disponível, de 30 pessoas, incluindo-se os líderes e o autor desta pesquisa.

A avaliação desta entrevista produziu uma qualificação do efetivo em termos de conhecimento e experiência profissional e o entendimento do que se necessita em termos informacionais para a consecução das atividades em segurança/defesa cibernética (SC/DC), auxiliando na produção da especificação do processo de avaliação de riscos cibernéticos, especificamente na geração do índice de riscos cibernéticos (IRC).

Considera-se que segurança/defesa cibernéticas encontram-se inseridas no contexto da segurança da informação e pode ser definida como: a preservação da tríade confidencialidade, integridade e disponibilidade da informação no Espaço Cibernético de interesse ao NuCDCAer, incluindo *hardware*, *software*, pessoas, representados pelos ativos e infraestruturas críticas a serem protegidos conforme estabelecido na Doutrina Militar de Defesa cibernética, no âmbito desta organização e na ABNT NBR ISO/IEC 27032:2015, em um âmbito mais abrangente, como pode ser observado nas Figuras 1 e 2.

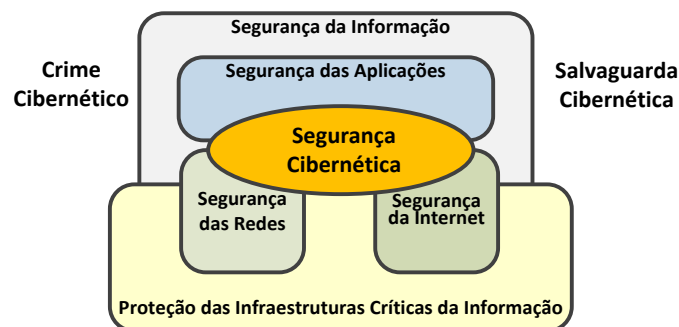


Figura 1: Relacionamento entre segurança cibernética e outras seguranças

Fonte: ABNT NBR ISO/IEC 27032:2015

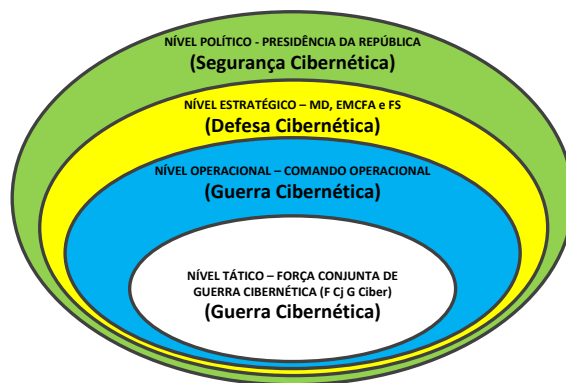


Figura 2-Níveis de decisão e atores no Espaço Cibernético

Fonte: Doutrina Militar de Defesa Cibernética

A entrevista foi dividida em três partes realizadas em 3 reuniões individuais e 2 coletivas para obtenção de ideias centrais por critério de pesquisa:

1ª parte:

A finalidade é a identificação da necessidade de aquisição/manipulação das informações para o processo de avaliação dos riscos cibernéticos, bem como compreender não só o foco do trabalho da organização, como suas necessidades e dificuldades, além de permitir conhecer o nível de conhecimento e experiência da força de trabalho disponível.

Identificação das dependências e necessidades informacionais, bem como as buscas pelas informações para a consecução das atividades em SC/DC.

2ª Parte:

Finalidade de identificar os elementos do processo de gestão de riscos (frameworks, cenários/controles e escalas de avaliação dos controles e dos riscos).

Bloco A – Identificação da criticidade estratégica dos ativos para a organização

Bloco B – Identificação dos padrões para o processo de avaliação de riscos (frameworks)

Bloco C – Identificação dos agrupamentos de controles/controles para avaliação dos riscos cibernéticos

3ª Parte:

Estabelecimento das fórmulas de cálculo e dos resultados esperados.

Estes dados pessoais foram anônimos e servem para subsidiar o entendimento de como se processa a segurança/defesa cibernética para a organização, de acordo com o entendimento de seus profissionais e consequentemente auxiliar no desenvolvimento do processo de análise/gestão dos riscos cibernéticos em função das diversas atividades identificadas.

Parte 1 - Esta parte refere-se às informações sobre a identificação dos respondentes das entrevistas e questionários e das relações com as informações necessárias.

a) Por quê a informação é uma commodity para a atividade do NuCDCAer?

b) Há uma definição clara sobre o contexto informacional para as atividades da organização?

c) Por favor, cite 3 ou mais palavras que imediatamente lhe vem à mente em termos de fontes de informação que entende como confiáveis ou úteis para a consecução dos objetivos da atuação da organização ou de sua atividade.

d) Poderia discorrer, em poucas palavras como se processa a busca pelas informações em sua atividade (início, modo, utilização, dificuldades etc.)?

Parte 2: Identificação dos elementos do processo de gestão de riscos (níveis de criticidade dos ativos, frameworks, cenários/controles, escalas de avaliação dos controles e dos riscos);

Durante as reuniões preliminares e informais para definição dos processos de avaliação de riscos, identificou-se que os riscos seriam analisados em função do impacto causado por possíveis ameaças ao explorar vulnerabilidades, levando-se em conta o valor estratégico do ativo para a organização que o suporta ou depende.

Para isso se faz necessário que o ativo tenha o seu valor estratégico identificado, além do uso de padrões ou métodos consagrados de segurança cibernética para a normalização das análises/avaliações de risco cibernéticos. As pesquisas e as conversações preliminares levaram à identificação de frameworks como os seguintes: NIST Cybersecurity Framework, MITRE Att&ck, MITRE D3fend e Lockheed Martin Cyber Kill Chain. Cada um deles possui características quanto à identificação dos procedimentos e técnicas usados para ataque cibernéticos, com a finalidade de entendimento dos padrões das ameaças e como se pode proteger o espaço cibernético.

Para esta parte da pesquisa objetiva-se a deliberação desse tipo de padronização, para que os processos do NuCDCAer sejam alinhados à linguagem e padrões de mercado, com a finalidade de serem compreendidos pelos demais componentes de defesa nacional aos quais o NuCDCAer está relacionado. Há como facilitar o treinamento e a capacitação dos integrantes desta organização, por meio da contratação de empresas que prestam este tipo de serviço, por usar técnicas que são padrão de mercado.

Bloco A – Identificação da criticidade estratégica dos ativos para a organização

a) Para que o risco aos ativos seja convenientemente estabelecido, se faz necessária a compreensão do valor do ativo para os objetivos estratégicos da organização analisada. Este valor nada tem a ver com o valor financeiro de aquisição do mesmo e sim do quão dependentes os processos estratégicos estão deste ativo. O Sr(a) poderia classificar os ativos em uma escala de criticidade estratégica prática?

b) Há alguma outra informação ou observação que deseja compartilhar?

Bloco B – Identificação dos padrões para o processo de avaliação de riscos (frameworks)

a) Para a composição do processo de avaliação de riscos o Sr(a) conhece algum framework de segurança cibernética que deveria ser usado em nossos processos? Não há necessidade de se limitar aos já citados, bem como eles não precisam ser únicos ou independentes.

b) O Sr(a) poderia fornecer alguma característica especial (frameworks) que o(s) torne(m) útil(eis) ao processo de avaliação dos riscos da organização, como seus padrões ou relacionamentos com outros frameworks?

c) Há alguma outra informação que julgue pertinente divulgar para auxiliar na diagramação dos processos de avaliação de riscos?

Bloco C – Identificação dos critérios/cenários/controles para avaliação dos riscos cibernéticos

a) Após a identificação dos possíveis frameworks a serem usados, o Sr(a) identifica possíveis agrupamentos de controles que sirvam para estabelecer os temas básicos para a criação de controles de mitigação de riscos cibernéticos (ex.: proteção de aplicações, resiliência cibernética)?

b) Após a identificação de agrupamento de controles, há a necessidade de se estabelecerem os controles que permitirão a análise e a avaliação dos riscos cibernéticos de forma granular. O Sr(a) poderia citar controles individuais, dentro dos agrupamentos que permitam analisar o risco e estabelecer uma redução do mesmo face a este controle idealizado? Nesta fase bastam que os controles sejam identificados, ficando a escala de avaliação para o próximo momento.

c) Há alguma outra informação ou observação que deseja compartilhar?

Bloco D – Identificação das escalas de avaliação para critérios/cenários/controles

a) Para cada controle identificado se faz necessário estabelecer um critério de intensidade do mesmo em relação à redução do risco (escala de avaliação). O Sr(a) poderia identificar as escalas (qualitativas) que podem ser usadas para inquirir a presença, ausência totais ou parciais e as características do controle frente ao risco a ser analisado.

b) Para cada escala criada, se faz necessário estabelecer valores para que haja uma identificação quantitativa da redução pela presença ou aumento pela ausência do controle comparado ao risco inquirido.

c) Há alguma outra informação ou observação que deseja compartilhar?

Parte 3: Estabelecimento das fórmulas de cálculo e dos resultados esperados.

Tão importante quanto o processo e os controles de análise/avaliação dos riscos, necessita-se de fórmulas que possam corroborar a identificação e o cálculo do índice de riscos cibernéticos (IRC) no ativo a ser analisado e dos resultados esperados.

- a) O Sr(a) poderia identificar os valores e as relações entre estes valores que podem auxiliar a criar os valores de risco calculado?
-

- b) O Sr(a) poderia identificar as relações válidas entre os valores calculados e os fatores que podem auxiliar a calcular o índice de riscos cibernéticos (IRC)?
-

- c) Há alguma outra informação ou observação que deseja compartilhar?
-

Referências:

VIEIRA, Sonia. Como elaborar questionários. In: **Como elaborar questionários**. 2009. p. 159-159.

Apêndice D

Resultado da entrevista
semiestruturada para análise dos
grupos de controle e controles para
avaliação dos riscos

Resultado da análise e referenciamento dos controles para avaliação de riscos cibernéticos

Agrupamentos	Controles	Escala	Referências (Att&ck, D3fend, CIS Top 20 etc.)	Matriz MITRE D3fend	Matriz NIST CSF
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Entrada das Vulnerabilidades</p>	<p style="text-align: center;">Criticidade da Vulnerabilidade</p> <p>(Informação obtida no relatório de vulnerabilidades refletem o impacto da vulnerabilidade analisada)</p>	<p>*Aspecto Obrigatório (Escala padrão CVSS reduzida para graus de 1 a 5)</p> <p>5 = Crítica 4 = Alta 3 = Média 1 = Baixa</p>	<p>ABNT NBR ISO/IEC 27001:2013 (A.12.6, A.14.2.3, A.16.1.3)</p> <p>CIS Control #7 (Continuous Vulnerability Management) (https://www.cisecurity.org/controls/cis-controls-list/)</p> <p>CVSS (Base Metrics) (https://www.first.org/cvss/user-guide/) (O grupo de métrica Base é composto pelas características intrínsecas de uma vulnerabilidade que são constantes ao longo do tempo e nos ambientes dos usuários. Este grupo é composto de dois conjuntos de métricas: as métricas de exploração (Exploitability) e as métricas de impacto (Impact).)</p> <p>Nist Cybersecurity Framework V 1.1 – Identificar (ID), Proteger (PR) e Detectar (DE), nas subcategorias:</p> <ul style="list-style-type: none"> •ID.RA-1 – Necessidade de identificação e documentação das vulnerabilidades; •ID.RA-2 – Obtenção sobre ameaças cibernéticas (que serão convertidas em vulnerabilidades que poderão ser exploradas) recebidas de fóruns especializados e de fontes de compartilhamento de notícias; •ID.RA-3 – Identificação e documentação de ameaças internas e externas; •PR.IP-12 – Necessidade de desenvolvimento e implementação de um plano de gerenciamento de vulnerabilidades; e •DE.CM-8 – Necessidade de realização de varreduras de vulnerabilidades. 	DETECTAR	IDENTIFICAR / PROTEGER
	<p style="text-align: center;">Tempo da Vulnerabilidade</p> <p>(Tempo de existência, descoberta confirmada ou maturidade do ecossistema da vulnerabilidade e dos controles)</p>	<p>*Aspecto Obrigatório</p> <p>5 = Existência confirmada, exploits funcional sem patch de remediação 4 = Existência confirmada, Exploits não totalmente funcionais ou baixo nível de remediação 3 = Existência confirmada, exploits não confirmados, patches de remediação temporários ou com algum nível de remediação 2 = Existência da vulnerabilidade confirmada, mas de baixo nível de impacto, sem exploits publicados ou patch de remediação oficial disponível 1 = Vulnerabilidade não confirmada.</p>	<p>CVSS (Temporal Metrics) (https://www.first.org/cvss/user-guide/)</p> <p>NIST Special Publication 800-53 Revision 4 [RA-5] – Escaneamento de Vulnerabilidades</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.12.6)</p> <p>Nist Cybersecurity Framework V 1.1 – Identificar (ID), Proteger (PR), nas subcategorias:</p> <ul style="list-style-type: none"> •ID.RA-1 – Necessidade de identificação e documentação das vulnerabilidades; •PR.IP-12: Um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado. 		
<p style="text-align: center;">Limitação no escopo da análise</p> <p>(Existe alguma limitação no escopo da análise de vulnerabilidades (PenTest) em virtude do ambiente de Avaliação (produção , homologação ou teste, grau de sigilo, permissão do proprietário ou autoridade etc.))</p>	<p>*Aspecto Obrigatório</p> <p>5 = Sim, houve limitação da análise de vulnerabilidades. 1 = Não houve limitação ao teste de vulnerabilidade ou penetração.</p>	<p>Nist Cybersecurity Framework V 1.1 –Proteger (PR) e Detectar (DE), nas subcategorias:</p> <ul style="list-style-type: none"> •PR.DS-7: O(s) ambiente(s) de desenvolvimento e teste é separado do ambiente de produção; •DE.CM-8 – Necessidade de realização de varreduras de vulnerabilidades. <p>CIS Control #18 (Penetration Testing) (https://www.cisecurity.org/controls/cis-controls-list/)</p>			

Agrupamentos	Aspectos	Escala	Referências (Att&ck, D3fend, CyBOK, CIS Top 20 etc.)	Matriz MITRE D3fend	Matriz NIST CSF
<p style="text-align: center;">Aspectos/Implicações Legais (Dependente do Contexto)</p> <p>LGPD, Marco Civil e artigos que interpretam impactos legais. Impactos legais internacionais pelo uso da infraestrutura em ataques cibernéticos aos Estados.</p>	<p style="text-align: center;">Impactos por Aspectos Legais</p> <p>(Responsabilizações/ Risco de Judicialização / sanções penais diversas por descumprimento de leis ou violação de direitos - Privacidade)</p>	<p>5 = Alto / Nunca foi avaliado (processos e sanções de alto custo à instituição) 3 = Médio (Multas ou danos à imagem da instituição pela judicialização) 1 = Irrelevante possibilidade de judicialização ou sanções econômicas ou legais 0 = Eliminar aspecto da análise</p>	<p>ABNT NBR ISO/IEC 27001:2013 (A.18)</p> <p>LEI Nº 13.709 (LGPD)</p> <p>Nist Cybersecurity Framework V 1.1 – Identificar (ID), na subcategoria: •ID.GV-3 – As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos;</p>	<p>Não há referência no MITRE D3fend</p>	<p>IDENTIFICAR</p>
	<p style="text-align: center;">Limitações Contratuais</p> <p>(Limitadores ou impedimentos de uso de boas práticas de segurança da informação em virtude de contratos ou acordos firmados) (Proibições, Sigilo, Privacidade etc.)</p>	<p>5 = Há registros contratuais que impedem ações de boas práticas de segurança 3 = Há registros contratuais que limitam ações de boas práticas de segurança 1 = Não há registros contratuais de impedam ou limitem boas práticas de segurança 0 = Eliminar aspecto da análise</p>	<p>Obs.: Verificar LEI Nº 13.709 (LGPD)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.18)</p> <p>NIST Special Publication 800-53 Revision 4 [AR-1; AR-2; AR-4; AR-5; AR-6; AR-7]</p> <p>Nist Cybersecurity Framework V 1.1 – Identificar (ID), nas subcategorias: •ID.GV-3 – As funções e responsabilidades de segurança cibernética são coordenadas e alinhadas com funções internas e parceiros externos; •ID.SC-3 - Os contratos com fornecedores e parceiros terceirizados são usados para implementar medidas apropriadas projetadas para atender aos objetivos do programa de segurança cibernética de uma organização e do Plano de Gerenciamento de Riscos da Cadeia de Suprimentos Cibernéticos</p>		
	<p style="text-align: center;">Gestão de Logs</p> <p>(Há política e armazenamento de logs de forma segura e de acordo com as disposições legais (quantidade, tempo de retenção, proteção dos registros, sincronização de tempo para validação))</p>	<p>*Aspecto Obrigatório</p> <p>5 = Não / Não há armazenamento ou política de armazenamento de qualquer log de ativo, nem proteção destes registros pelos tempos legais (marco civil) 4 = Não / Há política de armazenamento de logs, mas não há efetiva guarda de logs de todos os ativos importantes ou proteção destes registros pelos tempos legais (marco civil) 3 = Não / Há política de armazenamento de logs dos ativos importantes, mas não há proteção destes registros 1 = Sim / há política e armazenamento seguro dos registros importantes pelos tempos legais (marco civil)</p>	<p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (Anexo B, item 1.33)</p> <p>ICA 200-8/2008 – Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.12.4)</p> <p>Obs.: Verificar LEI Nº 13.709 (LGPD)</p> <p>LEI Nº 12.965/14 (Marco Civil da Internet) (Art. 10, Art. 11, Art. 13)</p> <p>CIS Control #8 (Audit Log Management) (https://www.cisecurity.org/controls/cis-controls-list/)</p> <p>Nist Cybersecurity Framework V 1.1 – Proteger (PR), na subcategoria: •PR.PT-1 - Os registros de auditoria/registo são determinados, documentados, implementados e revisados de acordo com a política.</p>		

Agrupamentos	Aspectos	Escala	Referências (Att&ck, D3fend, CyBOK, CIS Top 20 etc.)	Matriz MITRE D3fend	Matriz NIST CSF
Ações de Reposta / Continuidade dos negócios	<p>Impactos por Tempo de Recuperação</p> <p>Há informações de tempo máximo de parada ou de perda aceitável dos ativos críticos sob GCN? (Dependente de redundâncias diversas, planos de contingência, processos formais de reação a incidentes)</p>	<p>5 = Alto / Não é medido / Não há qualquer redundância ou processo que reduza interrupções) 3 = Médio / Há alguma redundância ou processo de redução de tempo de recuperação, mas há risco de o tempo ser medianamente elevado 1 = Há redundância e/ou processos de resposta imediata a incidentes que possam impactar em tempo de recuperação 0 = Remover aspecto da análise</p>	<p>ABNT NBR ISO/IEC 27001:2013 (A.17)</p> <p>ABNT NBR ISO/IEC 22301 - 2013 - Segurança da Sociedade - Sistema de Gestão de Continuidade dos Negócios</p> <p>NC 06/IN01/DSIC/GSIPR (4.1.4 - Tempo Objetivo de Recuperação)</p> <p>ICA7-1-Gestão de Continuidade dos Serviços nos Elos Especializados do Sistema de Tecnologia da Informação do Comando da Aeronáutica (3.1.3)</p> <p>Nist Cybersecurity Framework V 1.1 – Identificar (ID), na subcategoria: •ID.RA-4 – Potenciais impactos no negócio e probabilidades são identificados na organização;</p>	<p>Não há referência no MITRE D3fend (continuidade não se refere exatamente a riscos cibernéticos, trata-se do negócio em si)</p>	<p>IDENTIFICAR</p>
	<p>Resposta a Incidentes - ETIR</p> <p>(Possui Equipe de Tratamento de Incidentes de Rede (ETIR) ou equipe com capacitação em gestão de incidentes de rede na Organização em que a aplicação, ativo ou serviço estão hospedados)</p>	<p>*Aspecto Obrigatório</p> <p>5 = Não possui ETIR formal ou ou equipe de resposta a incidentes de rede treinada formalizada. 1 = Sim, possui ETIR ou equipe de resposta a incidentes de rede treinada formalizada.</p>	<p>NC05/IN01/DSIC/GSIPR- Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR (6, 7, 8)</p> <p>NC08/IN01/DSIC/GSIPR- Gestão de ETIR: Diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal (7.2, 7.3, 8)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.16)</p> <p>CIS Control #17 (Incident Response Management) (https://www.cisecurity.org/controls/cis-controls-list/) (17.1)</p> <p>NIST Special Publication 800-53 Revision 4 [IR-10]</p> <p>Nist Cybersecurity Framework V 1.1 –identificar (ID), detectar (DE) e responder (RS), nas subcategorias: •ID.RA-6: As respostas ao risco são identificadas e priorizadas; •DE.AE-1: Uma linha de base de operações de rede e fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada; •DE.AE-2: Os eventos detectados são analisados para compreender os alvos e métodos de ataque; •DE.AE-3: Os dados da ocorrência são coletados e correlacionados a partir de várias fontes e sensores; •DE.AE-4: O impacto dos eventos é determinado; •DE.AE-5: Os limites de alerta de incidentes são estabelecidos; •RS.AN-3: Há realização de investigações; •RS.AN-4: Os incidentes são categorizados de forma consistente com os planos de resposta; •RS.CO-2: Os incidentes são informados de acordo com os critérios estabelecidos; •RS.CO-3: As informações são compartilhadas de acordo com os planos de resposta; •RC.RP-1: O Plano de recuperação é executado durante ou após um incidente de segurança cibernética.</p>		<p>IDENTIFICAR / DETECTAR / RESPONEDR</p>

Agrupamentos	Aspectos	Escala	Referências (Att&ck, D3fend, CyBOK, CIS Top 20 etc.)	Matriz MITRE D3fend	Matriz NIST CSF
Ações de Reposta / Continuidade dos negócios	<p>Plano de Continuidade (Existe planejamento de continuidade dos serviços ou negócios (redundância - Site Secundário, planos de contingência etc.))</p>	<p>*Aspecto Obrigatório 5 = Não há qualquer planejamento de continuidade dos negócios ou serviços 4 = Há rudimentos de planejamento de continuidade, sem formalização, ou como iniciativa isolada de alguns setores; 3 = Há um planejamento parcial de continuidade dos negócios ou serviços (incompleto, faltam elementos ou testagem) 2 = Há planejamento completo de continuidade, mas falta uma testagem eficaz; 1 = Há planejamento completo de continuidade dos negócios ou serviços, inclusive testagem.</p>	<p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.11)</p> <p>ICA7-1-Gestão de Continuidade dos Serviços nos Elos Especializados do Sistema de Tecnologia da Informação do Comando da Aeronáutica (3.1.1)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.17)</p> <p>ABNT NBR ISO/IEC 22301 - 2013 - Segurança da Sociedade - Sistema de Gestão de Continuidade dos Negócios</p> <p>NC 06/IN01/DSIC/GSIPIR (5 -PROCEDIMENTOS)</p> <p>CIS Control #11 (Data Recovery) (https://www.cisecurity.org/controls/cis-controls-list/) (11.1, 11.5)</p> <p>NIST Special Publication 800-53 Revision 4 [CP-1; CP-2; PE-17]</p> <p>Nist Cybersecurity Framework V 1.1 – proteger (PR) e recuperar (RC), nas subcategorias: •PR.IP-9: Planos de resposta a incidentes e continuidade de negócios e planos de recuperação de incidentes e de desastres estão em vigor e gerenciados •PR.IP-10: Planos de recuperação e resposta são testados; •RC.RP-1: O Plano de recuperação é executado durante ou após um incidente de segurança cibernética.</p>	<p>Não há referência no MITRE D3fend (continuidade não se refere exatamente a riscos cibernéticos, trata-se do negócio em si)</p>	<p>PROTEGER / RECUPERAR</p>
	<p>Gestão de Backup (Há backup para os dados e/ou serviços virtualizados (Máq. Virtuais))</p>	<p>5 = Não há qualquer backup de dados ou de ambiente virtual) 4 = Não, só há backups de parte dos dados ou sistemas virtuais, mas estão desatualizados ou não foram testados 3 = Não, só há backups de parte dos dados ou sistemas virtuais, atualizados, mas sem registros de testes com eficácia 2 = Sim, há backups dos dados ou sistemas virtuais importantes, atualizados, mas sem registros de testes com eficácia 1 = Sim, há backups dos dados ou sistemas virtuais importantes, atualizados e testados com eficácia 0 = Remover aspecto da análise</p>	<p>ABNT NBR ISO/IEC 27001:2013 (A.12.3)</p> <p>CIS Control #03 (Data Protection) (https://www.cisecurity.org/controls/cis-controls-list/)</p> <p>CIS Control #11 (Data Recovery) (https://www.cisecurity.org/controls/cis-controls-list/)</p> <p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.11 e Anexo J, itens f, g, h, i, j)</p> <p>NIST Special Publication 800-53 Revision 4 [CP-9; CP-10]</p> <p>Nist Cybersecurity Framework V 1.1 – proteger (PR), na subcategoria: •PR.IP-4: Os Backups de informações são realizados, conservados e testados.</p>		

Agrupamentos	Aspectos	Escala	Referências (Att&ck, D3fend, CyBOK, CIS Top 20 etc.)	Matriz MITRE D3fend	Matriz NIST CSF
Proteção de Perímetro da Rede	<p>Presença de Firewall de Borda (Há proteção da rede por Firewall de Borda(uso de DMZ ou equivalente))</p>	<p>5 = Não (ou não atualizado/configurado corretamente) 1 = Sim (atualizado/configurado) 0 = Remover aspecto da análise</p>	<p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.3 e Anexos E)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.13)</p> <p>ABNT NBR ISO/IEC 27032:2015 (11.4.2.3)</p> <p>Nist Cybersecurity Framework V 1.1 – proteger (PR), na subcategoria: •PR.AC-5: A integridade da rede é protegida.</p>	ISOLAR	DETECTAR / PROTEGER
	<p>Presença de IPS/IDS (Há proteção da rede por IPS detecção e reação a ameaças de rede)</p>	<p>5 = Não (ou não atualizado/configurado corretamente) 1 = Sim (atualizado/configurado) 0 = Remover aspecto da análise</p>	<p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.3 e Anexos E)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.13)</p> <p>ABNT NBR ISO/IEC 27032:2015 (11.4.2.3)</p> <p>CIS Control #13 (Network Monitoring and Defense) (https://www.cisecurity.org/controls/cis-controls-list/) (13.2, 13.3, 13.7, 13.8)</p> <p>Nist Cybersecurity Framework V 1.1 –Identificar (ID), Detectar (DE), na subcategoria: •DE.CM-1: A rede é monitorada para detectar potenciais incidentes de segurança cibernética.</p>		
Proteção da Aplicação	<p>Presença de Proxy Reverso (Há proteção das Aplicações por Proxy Reverso)</p>	<p>5 = Não 1 = Sim 0 = Remover aspecto da análise</p>	<p>ABNT NBR ISO/IEC 27001:2013 (A.13)</p> <p>ABNT NBR ISO/IEC 27032:2015 (12.4)</p> <p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.3 e Anexos D)</p> <p>Nist Cybersecurity Framework V 1.1 –Identificar (ID), Detectar (DE), na subcategoria: •DE.CM-1: A rede é monitorada para detectar potenciais incidentes de segurança cibernética.</p>		
	<p>Presença de Firewall de Aplicação web (Há proteção das Aplicações por WAF – (Web Application Firewall))</p>	<p>5 = Não existe (ou não atualizado/configurado corretamente) 3 = Existe, mas não é bem configurado ou não é atualizado/revisado com frequência 1 = Sim (atualizado/configurado) 0 = Remover aspecto da análise</p>	<p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.3 e Anexos D)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.13)</p> <p>ABNT NBR ISO/IEC 27032:2015 (12.4)</p> <p>CIS Control #13 (Network Monitoring and Defense) (https://www.cisecurity.org/controls/cis-controls-list/) (13.10)</p> <p>Nist Cybersecurity Framework V 1.1 –Identificar (ID), Detectar (DE), na subcategoria: •DE.CM-1: A rede é monitorada para detectar potenciais incidentes de segurança cibernética.</p>		

Agrupamentos	Aspectos	Escala	Referências (Att&ck, D3fend, CyBOK, CIS Top 20 etc.)	Matriz MITRE D3fend	Matriz NIST CSF
Proteção de Acesso ao sistema ou serviço	<p style="text-align: center;">Privilégios desnecessários ativos</p> <p>(Há contas de usuários com privilégios administrativos que não necessitem deste nível de acesso)</p>	<p>5 = Sim há contas com privilégios desnecessários ou não foi investigado/não foi possível investigar 1 = Não há contas com perfil administrativo além das estritamente necessárias 0 = Remover aspecto da análise</p>	<p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (Anexo B, item 1.27)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.9.2, A.9.4)</p> <p>CIS Control #5 (Account Management) (https://www.cisecurity.org/controls/cis-controls-list/) (5.4)</p> <p>NIST Special Publication 800-53 Revision 4 [AC-2; AC-3; (1)(8)] AC-6(1)(2)(5);]</p> <p>Nist Cybersecurity Framework V 1.1 – proteger (PR), na subcategoria: • PR.AC-1: Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados.</p>	DESPEJAR	PROTEGER
	<p style="text-align: center;">Contas Ativas Desnecessárias</p> <p>(Há contas ativas de usuários que se encontram inativos ou desligados da organização (Desligados, afastados ou em férias))</p>	<p>5 = Sim há contas desnecessárias ativas/ Não foi investigado / Não há processo de desativação de contas de usuários por motivos de afastamento ou desligamento; 1 = Não há contas de usuários comuns que se encontram afastados ou desligados / há processo eficaz de desativação de contas sem uso 0 = Remover aspecto da análise</p>	<p>NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (Anexo A, itens 3 e 4; Anexo B,)</p> <p>ABNT NBR ISO/IEC 27001:2013 (A.9.2, A.9.4)</p> <p>CIS Control #5 (Account Management) (https://www.cisecurity.org/controls/cis-controls-list/) (5.3)</p> <p>NIST Special Publication 800-53 Revision 4 [AC-2; AC-6(1)(2)(5);]</p> <p>Nist Cybersecurity Framework V 1.1 – proteger (PR), na subcategoria: • PR.AC-1: Identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados.</p>		

Agrupamentos	Aspectos	Escala	Referências	Matriz MITRE D3fend	Matriz NIST CSF
Proteção do Ativo / Serviço	Uso de Criptografia (Há uso de criptografia no uso dos serviços, comunicações ou aplicações)	5 = Sistema necessita criptografia em múltiplos níveis e serviços e não é fornecido 3 = Sistema necessita criptografia em múltiplos níveis e serviços e é fornecido parcialmente 1=Sistema necessita de criptografia e é fornecido adequadamente 0 = Sistema não necessita de criptografia / Remover aspecto da análise	NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (Anexo C, itens d, e) ABNT NBR ISO/IEC 27001:2013 (A.10) NIST Special Publication 800-53 Revision 4 [IA-7] Nist Cybersecurity Framework V 1.1 – proteger (PR), nas subcategorias: •PR.DS-1: Os dados em repouso são protegidos; •PR.DS-2: Os dados em trânsito são protegidos.	ENDURECER	PROTEGER
	Presença de Portas abertas desnecessárias (Há portas de rede ou serviços (TCP/UDP) abertos além das necessidades da(s) aplicação(ões), ativo(s) ou serviço(incluindo acesso remoto))	5 = Sim / Não foi avaliado 1 = Ativo avaliado sem registros de portas desnecessárias abertas 0 = Remover aspecto da análise	ABNT NBR ISO/IEC 27032:2015 (9.4.3) Nist Cybersecurity Framework V 1.1 – proteger (PR), na subcategoria: •PR.AC-3: O acesso remoto é gerenciado.		ISOLAR
	Nível de Exposição do ativo (Amplitude da disponibilidade do ativo em termos de redes que aumentem ou reduzam exposição a ataques)	*Aspecto Obrigatório 5 = Disponível via Internet (acessível a ataques externos/outsider) 3 = Disponível via Intranet (acessível a ataques de insiders ou comprometimento de gateways externos/Internet/Extranet) 1 = Disponível via Rede Segregada / Ativo de uso isolado ou sem conexão de rede (necessidade de acesso via insider pela rede ou acesso físico ao ativo)	ABNT NBR ISO/IEC 27001:2013 (A.12.1.4) Apesar de não exatamente observar a exposição do ativo, a publicação NIST SP 800-115 exhibe a execução do PENTEST feito dentro e fora do perímetro da rede que hospeda o ativo. (item 2.4). LM Ciber Kill Chain - as fases do ataque Reconnaissance and Delivery são facilitadas de acordo com a exposição do ativo.	Não há referência no MITRE D3fend	PROTEGER
	Homologação de Sigilo (O sistema que manipula dados sigilosos foi homologado pela inteligência) (a justificativa é em função de sermos do governo federal e esta é uma característica de sistemas que não é testado pelas metodologias comuns)	5 = Não, o sistema tramita ou armazena dados sigilosos e nunca foi homologado por órgão de inteligência responsável 1 = Sim, o sistema tramita e/ou armazena dados sigilosos e foi homologado por órgão de inteligência responsável 0 = O Sistema não manipula dados sigilosos	ICA205-47-Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS) (3.1.2, 4.5, 5.7, 6.3, 6.5) ICA 200-8/2008 – Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações (1.5, 3.1) ABNT NBR ISO/IEC 27001:2013 (A.8.2) Nist Cybersecurity Framework V 1.1 – proteger (PR), na subcategoria: •PR.DS-5: As proteções contra vazamentos de dados são implementadas	DETECTAR	PROTEGER
	Proteção contra malwares (Há proteção dos ativos por software antivírus ou contra códigos maliciosos do tipo adware, spyware, cavalo-de-tróia (trojans, worms, backdoors, keyloggers, bots, botnets, rootkit e outros padronizado pela organização))	5 = Não há qualquer proteção por software contra códigos maliciosos 3 = Há uma proteção parcial por software contra alguns tipos de códigos maliciosos 1 = Sim, há proteção por software contra códigos maliciosos 0 = Remover aspecto da análise	NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.3 e Anexo D). ABNT NBR ISO/IEC 27001:2013 (A.12.2) NIST Special Publication 800-53 Revision 4 [SI-3]. Nist Cybersecurity Framework V 1.1 – proteger (PR) e detectar (DE), nas subcategorias: •PR.DS-8: Mecanismos de verificação de integridade são usados para verificar a integridade do hardware; •DE.CM-4: Código malicioso é detectado.	Não há referência no MITRE D3fend	PROTEGER
	Proteção física dos ativos (Há proteção física dos ativos de rede e dos recursos computacionais mais importantes (acesso, energia, climatização, fogo, monitoramento, cabeamento etc.))	*Aspecto Obrigatório 5 = Não há proteção física adequada para os ativos importantes 3 = Há uma proteção física parcial, não eficaz aos ativos importantes 1 = Sim, há proteção física adequada aos principais ativos	NSCA7-13-Segurança da Informação e Defesa Cibernética nas Organizações do COMAER (3.1). ABNT NBR ISO/IEC 27001:2013 (A.11.1, A.11.2) NIST Special Publication 800-53 Revision 4 [PE-1; PE-3; PE-6; PE-9; PE-11; PE-13; PE-14; PE-15] Nist Cybersecurity Framework V 1.1 – proteger (PR), na subcategoria: •PR.AC-2: O acesso físico aos ativos é gerenciado e protegido.	Não há referência no MITRE D3fend	PROTEGER

Apêndice E

Resumo e análise da entrevista estruturada sobre a validação da planilha de cálculo do IRC sob o método DELPHI para a etapa 6

Técnica Delphi aplicada à etapa 6

(Validação da Ferramenta Computacional via pesquisa estruturada)

Conforme já explicitado na metodologia, foi escolhida a técnica Delphi para a avaliação dos controles utilizados para a análise das vulnerabilidades durante a avaliação dos riscos cibernéticos (ARCiber). A ferramenta foi desenvolvida em formato de planilha para avaliação do processo criado, com sua utilização implementada na fase de homologação da ferramenta de uso corrente RSA Archer, que, em virtude de sua interface fragmentada, não permite uma visão completa do processo de forma prática e didática da ARCiber.

Foi utilizada a aplicação web WELPHI, uma solução comercial, por subscrição mensal, de uma empresa baseada em Portugal, a qual implementa a técnica Delphi via web de forma prática e rápida, oferecendo a interface para criação dos textos e questionários, recepção das respostas e questionários, definição dos cálculos de aceitação/rejeição dos argumentos e exibição das estatísticas básicas dos questionários, com possibilidade de múltiplas rodadas e envio seletivo via e-mail.

Este apêndice contém cada texto e pergunta oferecidos, as estatísticas de respostas, os comentários e as análises dos comentários que levantaram dúvidas ou críticas. Ao final é apresentado um resumo com as estatísticas das respostas em formato de tabela e as justificativas ou análises para os resultados obtidos.

RODADA 1

Texto da mensagem via E-mail enviada aos respondentes:

Assunto: O Sr/ Sra. foi convidado a participar de um questionário sobre a ferramenta de avaliação de riscos para a SGSI (NuCDCAer)

Mensagem:

Caro(a) convidado(a), foi autorizado pelo Chefe do NuCDCAer a emissão deste questionário.

A função desta atividade é avaliar os controles de uma ferramenta de cálculo de riscos prototipada em formato de planilha a qual serve de base para a implementação da gestão de riscos cibernéticos no âmbito do NuCDCAer, via ferramenta RSA Archer e consequentemente avaliar o processo de Avaliação de Riscos Cibernéticos (ARCiber) desenvolvido pela equipe da SGSI com participação de diversos integrantes do NuCDCAer.

Há links para esta planilha que servirá como protótipo de avaliação da metodologia, nas versões para Microsoft Excel e Libre Office Calc, além de um manual elucidativo para o uso da ferramenta. Solicita-se que haja um uso básico da ferramenta para avaliação dos controles que servirão para avaliar se nosso ambiente do NuCDCAer consegue mitigar vulnerabilidades por meio de controles. O questionário está implementado na ferramenta web Welphi, que operacionaliza a metodologia Delphi em versão web. As respostas às 25 questões servirão de avaliação para determinar se há algum consenso dos especialistas convidados, como o (a) Sr.(a) acerca de cada controle, e caso não haja, o controle será removido. Haverá, provavelmente, a necessidade de pelo menos mais uma rodada de respostas, para a confirmação das respostas que foram aceitas sem um alto valor de consenso e as que necessitam de mais alguma discussão. Por favor, para cada pergunta há um campo de comentário, que se solicita seja preenchido, caso necessário, com uma opinião, comentário, crítica ou sugestão sobre a questão/controlado, pois servirá de base para a rodada posterior e melhor avaliação do controle.

A equipe da SGSI estará à disposição para elucidar eventuais dúvidas que surgirem, em virtude de ser um processo novo e complexo, o qual demanda intercâmbio entre as equipes de nossa organização em sua fase de estruturação.

Em resumo, o Welphi é um sistema de questionários online que implementa o método Delphi, através de rodadas em que, além das suas respostas às questões colocadas, é possível introduzir comentários que serão compartilhados com os restantes participantes, de forma anônima, de forma a haver troca de argumentos e assim caminhar no sentido de um consenso sobre os controles analisados.

Por favor siga o link abaixo para iniciar a sua resposta ao questionário:

Link de acesso: [Questionário Welphi](#)

Links adicionais para suporte:

- Link para a planilha na versão em MS-Excel: [Planilha em Excel](#)
- Link para a planilha na versão em Libre office Calc: [Planilha em Calc](#)
- Manual de uso da planilha: [Manual de Uso](#)
- Link para todos os arquivos: [Arquivos de instruções e planilhas \(Excel e Calc\)](#)

Se é a sua primeira participação em um questionário Welphi, ser-lhe-á solicitado que crie uma senha para que possa acessar a este, ou a quaisquer outros questionários em que seja convidado a participar nesta plataforma. Sempre que quiser acessar ao seu questionário deverá seguir o link acima e utilizar o seu endereço de e-mail e a senha recém-criada para entrar.

Obrigado pelo seu tempo e disposição em ajudar.

A Equipe da SGSI

Texto introdutório da rodada 1 **(acessado ao abrir o Welphi para responder ao questionário)**

Bem-vindo ao questionário de avaliação da ferramenta e do processo de Avaliação de Riscos Cibernéticos desenvolvida na SGTI, em implementação experimental via RSA Archer

A finalidade do questionário é o de avaliar a ferramenta computacional (planilha) para o processo de avaliação de riscos cibernéticos (ARCiber), cujo foco e escopo coincidem totalmente com o meu trabalho de mestrado, para o qual estas informações serão de extrema valia, bem como para a implementação do processo de forma eficaz em nossas atividades cotidianas no NuCDCAer.

Esta ferramenta configura-se em uma forma didática de compreensão do processo ARCiber e de avaliação dos conceitos de gestão de riscos cibernéticos. Sua implementação final se dará na ferramenta RSA Archer, mas a planilha serve como um protótipo de validação dos controles e do método em si. Cada controle foi escolhido em função do uso de frameworks de risco como o NIST Cybersecurity Framework, CIS Controls, Normas ISO 27001, 27002, 27005, 27032, 22301 e 31000, além de normativos FAB. A lista dos 22 controles a serem avaliados encontra-se distribuída pelas perguntas da avaliação, além de 03 perguntas sobre a interface de uso da ferramenta.

Links adicionais para suporte:

- Link para a planilha na versão em MS-Excel: [Planilha em Excel](#)
- Link para a planilha na versão em Libre office Calc: [Planilha em Calc](#)
- Manual de uso da planilha: [Manual de Uso](#)
- Link para todos os arquivos: [Arquivos de instruções e planilhas \(Excel e Calc\)](#)

O processo do método Delphi de validação dos controles necessita por volta de 2 rodadas de respostas dos especialistas em Segurança/Defesa Cibernética para que os controles possam obter um consenso mínimo e serem considerados coerentes para serem efetivamente utilizados em nossos trabalhos cotidianos no NuCDCAer, logo há a possibilidade de lhe ser solicitada nova participação, dependendo da dinâmica do processo. Para cada pergunta há um comentário que é de suma importância, caso haja qualquer análise, crítica ou sugestão sobre as respostas escolhidas ou sobre os controles analisados. Após a primeira rodada os controles terão suas respostas positivas ou negativas analisadas e os que tiverem pontuação muito baixa tendem a ser eliminados, e os com pontuação elevada serão automaticamente aceitos e os com pontuação mediana continuam no processo, mas receberão melhorias em seus textos de acordo com os comentários recebidos que poderão dar uma nova visão à avaliação do controle em virtude das análises prévias. Por favor, seja o(a) mais crítico(a) possível, para que haja coerência de respostas e precisão na análise.

Solicito sua ajuda neste trabalho, pois configura muito além de um trabalho acadêmico, e o processo de ARCiber estudado e desenhado já está influenciando na implementação do RSA Archer, mas falta a avaliação e validação dos controles e das fórmulas de cálculo do Índice de Riscos Cibernéticos.

Antes das perguntas, há a indicação dos grupos de controles, os quais são divisões lógicas das avaliações, com suas definições e embasamentos nos frameworks já referenciados.

Obrigado pela sua disponibilidade.

Questões da rodada 1

Grupo de controles: Entrada das vulnerabilidades.

Controle: Criticidade da vulnerabilidade.

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Entrada de Vulnerabilidades	Criticidade da Vulnerabilidade	Informação obtida no relatório de vulnerabilidades do ativo. Refletem o impacto original (bruto) da vulnerabilidade a ser analisada	CIS Control #7, CVSS (Base Metrics), Nist Cybersecurity Framework V 1.1 (ID.RA-1, ID.RA-2, ID.RA-3, PR.IP-12, DE.CM-8)

Pergunta 1:

Você concorda que para **Entrada das vulnerabilidades**, o **cadastro das criticidades das vulnerabilidades** por meio de relatórios de vulnerabilidades do ativo (pentests ou scans de rede), ou de relatórios externos que indiquem vulnerabilidades para o tipo de ativo com valores definidos pela escala do CVSS seja uma forma eficaz de entrada de dados para analisar as vulnerabilidades dos ativos do ambiente do NuCDCAer?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 1:

Texto da pergunta 1	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Entrada das vulnerabilidades , o cadastro das criticidades das vulnerabilidades por meio de relatórios de vulnerabilidades do ativo (pentests ou scans de rede), ou de relatórios externos que indiquem vulnerabilidades para o tipo de ativo com valores definidos pela escala do CVSS seja uma forma eficaz de entrada de dados para analisar as vulnerabilidades dos ativos do ambiente do NuCDCAer?	20	60%	40%	0%	0%	Aprovada

Comentários enviados para a pergunta 1:

Id.	Resposta	Comentário
1	Concordo	Achei que faltou uma contextualização sobre os grupos de controle, algo que explicasse quais as etapas estamos falando inicialmente. Outra sugestão é inicialmente a qualificação do pesquisador (analisador), tipo você tem qual formação, quanto tempo na área de segurança, possui conhecimentos em gestão de riscos, etc. Para que, depois, possa pesar as análises de acordo com o grupo ou nível de conhecimento do avaliador. Também tive dificuldade em entender o que é o cadastramento de vulnerabilidades, pois é um cadastramento via uma referência ou tabela ou é um processo de análise de um especialista? o relatório de vulnerabilidades gera a criticidade? A forma de questionário em Escala de Likert utiliza AFIRMAÇÕES e portanto, se vc concorda ou não. Ou, seja: A escala Likert costuma ser apresentada como uma espécie de tabela de classificação. Afirmativas são apresentadas e o respondente é convidado a emitir o seu grau de concordância com aquela frase. (Fonte: https://mindminers.com/blog/entenda-o-que-e-escala-likert/) Então essa pergunta: "Você concorda que para Entrada das vulnerabilidades, o cadastramento das criticidades das vulnerabilidades por meio de relatórios de vulnerabilidades do ativo (pentests ou scans de rede), ou de relatórios externos que indiquem vulnerabilidades para o tipo de ativo com valores definidos pela escala do CVSS seja uma forma eficaz de entrada de dados para analisar as vulnerabilidades dos ativos do ambiente do NuCDCAer? " Deveria ser algo como (sugestão): (introdução) No processo de gestão de riscos, que possui as fases A, B, C e XYZ, na fase de "Entrada das vulnerabilidades", o cadastramento das criticidades das vulnerabilidades por meio de relatórios de vulnerabilidades do ativo (pentests ou scans de rede), ou de relatórios externos que indiquem vulnerabilidades para o tipo de ativo com valores definidos pela escala do CVSS Esse processo então: "É uma forma eficaz de entrada de dados para analisar as vulnerabilidades dos ativos do ambiente do NuCDCAer" -> concordo , discordo ...
2	Concordo	Acredito ser uma fonte importante de vulnerabilidade do ativo. Esse controle junto a outras informações, como a criticidade do ativo, pode gerar o valor do risco de um ataque a esse ativo.

3	Concordo totalmente	<p>Boa parte das vulnerabilidades possuem ampla documentação a respeito do nível de criticidade da vulnerabilidade em si. "Sistema de Pontuação de Vulnerabilidade Comum (CVSS) O Common Vulnerability Scoring System (CVSS) é usado para classificar a severidade e o risco de segurança do sistema de computador. CVSS é uma estrutura aberta que consiste nos grupos de métricas a seguir: Base Temporal Ambiental Base O intervalo de severidade de pontuação de base é de 0 a 10 e representa as características inerentes da vulnerabilidade. A pontuação de base tem a maior relevância na pontuação CVSS final e pode ser dividida ainda mais nas subpontuações a seguir: Impacto A subpontuação de impacto representa as métricas para impacto de confidencialidade, impacto de integridade e impacto de disponibilidade de uma vulnerabilidade explorada com sucesso. Explorabilidade A subpontuação de explorabilidade representa as métricas para Vetor de acesso, Complexidade de acesso e Autenticação e mede como a vulnerabilidade é acessada, a complexidade do ataque e o número de vezes que um invasor deve autenticar para explorar com sucesso uma vulnerabilidade. Temporal A pontuação temporal representa as características de uma ameaça de vulnerabilidade que muda ao longo do tempo e consiste nas métricas a seguir: Explorabilidade A disponibilidade de técnicas ou códigos que podem ser usados para explorar a vulnerabilidade, que muda ao longo do tempo. Nível de Correção O nível de correção que está disponível para uma vulnerabilidade. Segurança do Relatório O nível de confiança na existência da vulnerabilidade e a credibilidade de seus detalhes técnicos. Ambiental A pontuação ambiental representa as características da vulnerabilidade que são impactadas pelo ambiente do usuário. Configure as métricas ambientais a seguir para destacar as vulnerabilidades de ativos importantes ou críticos, aplicando métricas ambientais mais altas. Aplique as pontuações mais altas para os ativos mais importantes, pois as perdas que estão associadas a esses ativos têm consequências maiores para a organização. Potencial de dano indireto (CDP) O potencial para perda de vida ou de ativos físicos por dano ou furto desse ativo, ou para perda econômica de produtividade ou de renda. Distribuição de destino (TD) A proporção de sistemas vulneráveis no ambiente do seu usuário. Requisito de Confidencialidade (CR) O nível de impacto na perda de confidencialidade quando uma vulnerabilidade é explorada nesse ativo. Requisito de integridade (IR) Essa métrica indica o nível de impacto na perda de integridade quando uma vulnerabilidade é explorada com sucesso nesse ativo. Requisito de disponibilidade (AR) O nível de impacto na disponibilidade do ativo quando uma vulnerabilidade é explorada com sucesso nesse ativo." Fonte: https://www.ibm.com/docs/pt-br/qradar-on-cloud?topic=vulnerabilities-common-vulnerability-scoring-system-cvss</p>
4	Concordo totalmente	<p>Acredito que a criticidade da vulnerabilidade é de fundamental importância para a priorização das atividades de correção de vulnerabilidades.</p>

Avaliação dos comentários.

Para o comentário nº 1, único que trouxe alguma crítica, apesar de o respondente concordar com o controle, indica que este avaliador não leu o manual que acompanha a pesquisa (vários respondentes indicaram não o terem lido), cujos links estão nos dois textos. Este avaliador consultou a equipe da SGSI e lhe foi indicado o manual. Ele também está em um processo acadêmico de Doutorado, e o comentário reflete dúvidas acadêmicas, normalmente não discutidas durante o processo de respostas, pois já foram anteriormente avaliadas por outros profissionais envolvidos na pesquisa, e justificadas na parte de metodologia da pesquisa, quando houve o desenvolvimento do questionário. Os demais comentários somente reforçam as respostas dadas.

Grupo de controles: Análise da Vulnerabilidade.

Controles:

1. Tempo da Vulnerabilidade
2. Limitação no escopo da análise

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Análise da Vulnerabilidade	Tempo da Vulnerabilidade	Analisa o tempo de existência, descoberta confirmada ou maturidade do ecossistema da vulnerabilidade e dos controles	CVSS (Temporal Metrics), NIST Special Publication 800-53 Revision 4 (RA-5), ABNT NBR ISO/IEC 27001:2013 (A.12.6), Nist Cybersecurity Framework V 1.1 (ID.RA-1, PR.IP-12)
	Limitação no escopo da análise	Investiga se houve alguma limitação no escopo da análise de vulnerabilidades (PenTest) em virtude do ambiente de Avaliação (produção, homologação ou teste, grau de sigilo, permissão do proprietário ou autoridade etc)	Nist Cybersecurity Framework V 1.1 (PR.DS-7, DE.CM-8), CIS Control #18

Pergunta 2:

Você concorda que para **Análise da Vulnerabilidade**, o **tempo de existência de uma vulnerabilidade** é um fator importante para a análise do ambiente em risco a ponto de ser considerado um controle que deva constar em uma ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 2:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Análise da Vulnerabilidade , o tempo de existência de uma vulnerabilidade é um fator importante para a análise do ambiente em risco a ponto de ser considerado um controle que deva constar em uma ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	Aprovada

Comentários enviados para a pergunta 2:

Id.	Resposta	Comentário
1	Concordo totalmente	Concordo totalmente, pois vulnerabilidades novas (0 day) em sua maioria não possui path de correção disponível e estará em análise a exposição que a vulnerabilidade poderá causar. Esses fatores elevam a criticidade. Portanto deverá ser considerado o tempo de existência da vulnerabilidade.
2	Concordo totalmente	Quanto maior o tempo da vulnerabilidade, maior será conhecimento da comunidade hacker a respeito da vulnerabilidade e mais formas/técnicas de exploração serão usadas/cridas para que o atacante consiga explorar.
3	Concordo	Sim, pois conforme o tempo, zero day ou vulnerabilidade antiga, pode aumentar o risco de existir um exploit.
4	Concordo	O tempo de existência da vulnerabilidade é importante para inferir sobre a existência de exploits públicos capazes de explorar aquela vulnerabilidade, o que impacta o nível de criticidade. O escopo da vulnerabilidade também é importante pois tem impacto direto no nível de criticidade da vulnerabilidade.
5	Concordo totalmente	Acredito que o nível de exposição do ativo também deva ser algo relevante, pois a depender se o ativo está exposto na internet as chances de este já ter sido explorado aumenta.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Pergunta 3:

Você concorda que para **Análise da Vulnerabilidade**, uma **limitação do escopo da análise de riscos**, como o ativo estar em um ambiente de produção, homologação ou desenvolvimento, ou haver indicação de impossibilidade de análise completa em função de sigilo ou permissão de autoridade competente configura um fator relevante para a existência deste controle constar em uma ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 3:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Análise da Vulnerabilidade , uma limitação do escopo da análise de riscos , como o ativo estar em um ambiente de produção, homologação ou desenvolvimento, ou haver indicação de impossibilidade de análise completa em função de sigilo ou permissão de autoridade competente configura um fator relevante para a existência deste controle constar em uma ferramenta de análise de riscos cibernéticos?	20	55%	40%	5%	0%	Aprovada

Comentários enviados para a pergunta 3:

Id.	Resposta	Comentário
1	Concordo	Nesse caso, acho que seria interessante diferenciar os termos análise com outros sinônimos: Análise de vulnerabilidade, a análise de riscos, ...como o ativo estar em um ambiente... análise completa em função ...ferramenta de análise de riscos cibernéticos... Seria algo como: Restrições de acesso do controle ou da ferramenta no sistema alvo.
2	Concordo totalmente	Concordo totalmente, pois ativos em produção terão criticidade maior do que os que constam em ambiente de homologação e teste, devido ao impacto que poderá causar. Esse é um fator que deve ser considerado. Porém ativos vulneráveis em ambientes de teste também podem comprometer a rede.
3	Concordo totalmente	Quanto mais completo o teste da equipe de pentest, maior o conhecimento a respeito das vulnerabilidades das aplicações, sendo assim maior conhecimento para tomar a decisão a respeito de como a vulnerabilidade será mitigada.
4	Concordo	Entendo que na grande maioria das vezes é inviável testes em produção, sendo o teste em ambiente de homologação ser o mais viável.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Grupo de controles: Aspectos/Implicações Legais.

Controles:

1. Impactos por Aspectos Legais
2. Limitações Contratuais
3. Gestão de Logs

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Aspectos/Implicações Legais	Impactos por Aspectos Legais	Investiga se há possibilidade de responsabilizações/ risco de judicialização / sanções penais diversas por descumprimento de leis ou violação de direitos - Privacidade	ABNT NBR ISO/IEC 27001:2013 (A.18), Lei nº 13.709 (LGPD), Nist Cybersecurity Framework V 1.1 (ID.GV-3).
	Limitações Contratuais	Observa se há limitadores ou impedimentos de uso de boas práticas de segurança da informação em virtude de contratos ou acordos firmados (Proibições, Sigilo, Privacidade etc.)	ABNT NBR ISO/IEC 27001:2013 (A.18), Lei nº 13.709 (LGPD), NIST Special Publication 800-53 Revision 4 (AR-1; AR-2; AR-4; AR-5; AR-6; AR-7), Nist Cybersecurity Framework V 1.1 (ID.GV-3, ID.SC-3).
	Gestão de Logs	Investiga se há política e armazenamento de logs de forma segura e de acordo com as disposições legais (quantidade, tempo de retenção, proteção dos registros, sincronização de tempo para validação).	NSCA7-13 (Anexo B, item 1.33), ICA 200-8/2008, ABNT NBR ISO/IEC 27001:2013 (A.12.4), Lei nº 12.965/14 (Marco Civil da Inter-net) (Art. 10, Art. 11, Art. 13), CIS Control #8, Nist Cybersecurity Framework V 1.1 (PR.PT-1)

Pergunta 4:

Você concorda que para **Aspectos/Implicações Legais**, possíveis **impactos por aspectos legais** que uma vulnerabilidade explorada possa ocasionar à organização é um fator importante para a análise do ambiente em risco a ponto de ser considerado um controle que deva constar em uma ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 4:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Aspectos/Implicações Legais , possíveis impactos por aspectos legais que uma vulnerabilidade explorada possa ocasionar à organização é um fator importante para a análise do ambiente em risco a ponto de ser considerado um controle que deva constar em uma ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	Aprovada

Comentários enviados para a pergunta 4:

Id.	Resposta	Comentário
1	Concordo totalmente	É muito importante o registro dessas informações em ferramenta de análise de riscos cibernéticos, pois através dela será possível compreender os riscos em questão e sua necessidade de mitigação.
2	Concordo	Sim, pois devemos agir dentro dos controles das leis.
3	Concordo totalmente	Juntamente com o nível de exposição do ativo.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Pergunta 5:

Você concorda que para **Aspectos/Implicações Legais**, possíveis **limitações contratuais** possam impedir o uso de boas práticas de segurança cibernética a ponto de ser necessária a existência de um controle para evidenciar estas dúvidas e assim constar (controle) em uma ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 5:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Aspectos/Implicações Legais , possíveis limitações contratuais possam impedir o uso de boas práticas de segurança cibernética a ponto de ser necessária a existência de um controle para evidenciar estas dúvidas e assim constar (controle) em uma ferramenta de análise de riscos cibernéticos?	20	30%	55%	15%	0%	Aprovada

Comentários enviados para a pergunta 5:

Id.	Resposta	Comentário
1	Discordo	Não entendi bem essa pergunta.
2	Concordo	Esses quesitos devem ser muito bem controlados e que seus riscos aceitos pela direção.
3	Concordo	Sim, pois devemos agir dentro do acordo contratual.
4	Discordo	Acredito que os acordos contratuais devem seguir as necessidades da FAB no quesito segurança da informação. E não o inverso, ou seja, os controles de segurança da informação não devem se adaptar aos acordos contratuais, e sim os acordos contratuais devem ser feitos para a tender às necessidades de segurança da informação.
5	Concordo	Nesse ponto acredito que os contratos devem ser mais bem elaborados para que situações como essa sejam evitadas.

Avaliação dos comentários.

O comentário nº 1 sugere que o respondente não observou o manual, que explica o controle em si, que procura evidenciar brechas que podem existir em contratos, as quais podem limitar a atuação de boas práticas, como a proibição de certos procedimentos de análise de riscos, limitações de acesso etc. sendo o comentário nº 5 uma resposta plausível para esta dúvida.

O comentário nº 4 reflete uma ação correta, mas não houve o entendimento da real utilidade do controle, que é a de estabelecer um checklist para identificar eventuais fraquezas na elaboração de contratos ou de acordos entre partes que envolvam as ações da FAB em segurança cibernética. Após exame deste comentário, a equipe da SGSI identificou que não há uma real discordância do que foi comentado e do que foi questionado, somente uma divergência teórica de opiniões. O controle aparenta ter validade prática como item de identificação de fraquezas contratuais.

Pergunta 6:

Você concorda que para **Aspectos/Implicações Legais**, a **gestão de logs (de acesso à rede e de ativos de rede diversos)** constitui um controle que deve ser observado e incluído em análises de vulnerabilidades do ambiente em risco como um aspecto com implicações legais e como tal deve constar em na ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 6:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Aspectos/Implicações Legais , a gestão de logs (de acesso à rede e de ativos de rede diversos) constitui um controle que deve ser observado e incluído em análises de vulnerabilidades do ambiente em risco como um aspecto com implicações legais e como tal deve constar em na ferramenta de análise de riscos cibernéticos?	20	50%	40%	10%	0%	Aprovada

Comentários enviados para a pergunta 6:

Id.	Resposta	Comentário
1	Concordo	Não sei bem se essa gestão de logs é um controle, ou se é um processo a ser realizado.
2	Concordo totalmente	Os logs são fontes de informações muito importantes a respeito do ativo.
3	Concordo	Deverá ser observado a política de seleção e armazenamento de logs, fundamental para investigações de incidentes.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Grupo de controles: Ações de Reposta / Continuidade dos negócios.

Controles:

1. Impactos por Tempo de Recuperação
2. Resposta a Incidentes - ETIR
3. Plano de Continuidade
4. Gestão de Backup

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Ações de Reposta / Continuidade dos negócios	Impactos por Tempo de Recuperação	Analisa se há informações de tempo máximo de parada ou de perda aceitável dos ativos críticos sob Gestão da Continuidade dos Negócios (GCN).	ABNT NBR ISO/IEC 27001:2013 (A.17), ABNT NBR ISO/IEC 22301 - 2013, NC 06/TN01/DSIC/GSIPR (4.1.4), ICA7-1 (3.1.3), Nist Cybersecurity Framework V 1.1 (ID.RA-4).
	Resposta a Incidentes - ETIR	Observa se há alguma equipe de tratamento de incidentes de rede (ETIR) ou alguma equipe ou profissional(is) com capacitação em gestão de incidentes de rede na organização em que a aplicação, ativo ou serviço estão hospedados.	NC05/TN01/DSIC/GSIPR (6, 7, 8), NC08/TN01/DSIC/GSIPR (7.2, 7.3, 8), ABNT NBR ISO/IEC 27001:2013 (A.16), CIS Control #17, NIST Special Publication 800-53 Revision 4 (IR-10), Nist Cybersecurity Framework V 1.1 (ID.RA-6, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS.AN-3, RS.AN-4, RS.CO-2, RS.CO-3, RC.RP-1)
	Plano de Continuidade	Investiga se existe planejamento de continuidade dos serviços ou negócios (redundância -site secundário, planos de contingência, de gestão de crises etc.)	NSCA7-13 (3.11), ICA7-1 (3.1.1), ABNT NBR ISO/IEC 27001:2013 (A.17), ABNT NBR ISO/IEC 22301 - 2013, NC 06/TN01/DSIC/GSIPR (5), CIS Control #11, NIST Special Publication 800-53 Revision 4 (CP-1; CP-2; PE-17), Nist Cybersecurity Framework V 1.1 (PR.IP-9, PR.IP-10, RC.RP-1).
	Gestão de-Backup	Analisa se há backup para os dados e/ou serviços virtualizados e como são geridos.	ABNT NBR ISO/IEC 27001:2013 (A.12.3), CIS Control (#03, #11), NSCA7-13 (3.11 e Anexo J, itens f, g, h, i, j), NIST Special Publication 800-53 Revision 4 (CP-9; CP-10), Nist Cybersecurity Framework V 1.1 (PR.IP-4)

Pergunta 7:

Você concorda que para **Ações de Reposta / Continuidade dos negócios**, um processo de identificação de possíveis **impactos por tempo de recuperação (BIA – Business Impact Analysis)** como elemento (controle) preventivo para mitigação de impactos por incidentes com os ativos críticos da organização constitui um controle que deve ser incluído em análises de vulnerabilidades do ambiente em risco e deve constar na ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 7:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Ações de Reposta / Continuidade dos negócios , um processo de identificação de possíveis impactos por tempo de recuperação (BIA – Business Impact Analysis) como elemento (controle) preventivo para mitigação de impactos por incidentes com os ativos críticos da organização constitui um controle que deve ser incluído em análises de vulnerabilidades do ambiente em risco e deve constar na ferramenta de análise de riscos cibernéticos?	20	60%	30%	5%	5%	Aprovada

Comentários enviados para a pergunta 7:

Id.	Resposta	Comentário
1	Concordo totalmente	Avaliar subdividir o controle por tempo de parada.
2	Concordo	Concordo que deve ser observada a criticidade dos ativos sob a ótica da Gestão de Continuidade do Negócio.
3	Concordo totalmente	Existem ativos extremamente sensíveis, onde um longo tempo de parada pode causar impacto negativo à organização.
4	Discordo totalmente	Aqui realmente não está claro o que se quer saber.

Avaliação dos comentários.

Para o comentário nº 4 o comentário pode indicar que o respondente não compreendeu as implicações da BIA, análise de impacto nos negócios, nos processos de repostas ou continuidade dos negócios em incidentes cibernéticos. As equipes são multidisciplinares e nem todos são especialistas em todas as áreas avaliadas. De acordo com a estatística de respostas, esta foi a única discordância com a pergunta.

Pergunta 8:

Você concorda que para **Ações de Reposta / Continuidade dos negócios**, a observação sobre a existência de alguma **equipe de tratamento de incidentes de rede (ETIR) ou alguma equipe ou profissional(is) com capacitação em gestão de incidentes de rede** na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 8:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Ações de Reposta / Continuidade dos negócios , a observação sobre a existência de alguma equipe de tratamento de incidentes de rede (ETIR) ou alguma equipe ou profissional(is) com capacitação em gestão de incidentes de rede na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	60%	35%	5%	0%	Aprovada

Comentários enviados para a pergunta 8:

Id.	Resposta	Comentário
1	Concordo totalmente	No caso, não só ETIR, mas equipe de suporte/segurança em geral, mas só isso também não, pois também deveria identificar de forma automatizada de alguma forma. Pois, possuir uma equipe não quer dizer que está sendo efetiva, por isso ferramentas automatizadas são importantes.
2	Concordo	A garantia da eficácia depende muito do nível da maturidade da equipe.
3	Concordo totalmente	A existência de uma equipe de Tratamento de Incidentes impacta diretamente no nível de degradação dos serviços de TI, no período de restauração dos serviços e na quantidade de reincidência dos ataques cibernéticos, sendo então de fundamental importância na classificação do risco.
4	Concordo totalmente	Uma equipe de tratamento de incidentes pronta e qualificada pode ser fator decisivo para o rápido restabelecimento do ativo.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Pergunta 9:

Você concorda que para **Ações de Recuperação / Continuidade dos negócios**, a observação sobre a existência de **planos ou planejamento da continuidade dos negócios (contingência, redundâncias, gestão de crises etc.)** na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 9:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Ações de Recuperação / Continuidade dos negócios , a observação sobre a existência de planos ou planejamento da continuidade dos negócios (contingência, redundâncias, gestão de crises etc.) na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	Aprovada

Comentários enviados para a pergunta 9:

Id.	Resposta	Comentário
1	Concordo totalmente	Sim, assim como o tempo de atualização desses planos também são importantes (caso haja mudanças nos serviços ativos etc).
2	Concordo	Não é possível garantir a eficácia na mitigação de riscos cibernéticos.
3	Concordo totalmente	Um plano de continuidade de negócio existente direciona melhor ações a serem tomadas.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Pergunta 10:

Você concorda que para **Ações de Recuperação / Continuidade dos negócios**, a observação sobre a existência de **gestão de backups (planejamento, confecção, proteção e testagem)** na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 10:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Ações de Recuperação / Continuidade dos negócios , a observação sobre a existência de gestão de backups (planejamento, confecção, proteção e testagem) na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	60%	35%	5%	0%	Aprovada

Comentários enviados para a pergunta 10:

Id.	Resposta	Comentário
1	Concordo totalmente	Isso não é uma parte dos outros planos? continuidade, etc?
2	Concordo	Difícil garantir a eficácia operacional quando necessita do backup.
3	Concordo totalmente	A existência de uma gestão de eficaz de backups é de fundamental importância para mitigar riscos e deve sim ser incluída na análise de riscos.
4	Concordo totalmente	No atual cenário cibernético a gestão de backup se tornou imprescindível.

Avaliação dos comentários.

O comentário nº 1 apesar de parecer discordar, reflete, na verdade, uma crítica que corrobora o entendimento. Os backups realmente fazem parte de outros planos, mas devem ter uma avaliação independente, dada sua importância estratégica.

Grupo de controles: Proteção do Perímetro da Rede.

Controles:

1. Presença de Firewall de Borda
2. Presença de IPS/IDS

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Proteção de Perímetro da Rede	Presença de Firewall de Borda	Analisa se há proteção da rede por Firewall de Borda(uso de DMZ ou equivalente).	NSCA7-13 (3.3 e Anexos E), ABNT NBR ISO/IEC 27001:2013 (A.13), ABNT NBR ISO/IEC 27032:2015 (11.4.2.3), Nist Cybersecurity Framework V 1.1 (PR.AC-5).
	Presença de IPS/IDS	Investiga se há proteção da rede por IPS ou IDS, detecção e reação a ameaças de rede ou tráfego anômalo.	NSCA7-13 (3.3 e Anexos E), ABNT NBR ISO/IEC 27001:2013 (A.13), ABNT NBR ISO/IEC 27032:2015 (11.4.2.3), CIS Control #13, Nist Cybersecurity Framework V 1.1 (DE.CM-1).

Pergunta 11:

Você concorda que para **proteção do perímetro da rede** sob a responsabilidade da organização, a **presença de um firewall de borda (ou similar, para separação de tráfego entre as redes internas e externas da organização/criação da DMZ)** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 11:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para proteção do perímetro da rede sob a responsabilidade da organização, a presença de um firewall de borda (ou similar, para separação de tráfego entre as redes internas e externas da organização/criação da DMZ) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	Aprovada

Comentários enviados para a pergunta 11:

Id.	Resposta	Comentário
1	Concordo	Concordo em parte, visto que a atualização e a manutenção das regras são tão importantes quanto, pois novamente, pode não estar sendo efetivo. Passando uma falsa noção de segurança, simplesmente por ter a ferramenta.
2	Concordo	Só a presença não seria o ideal. O ideal seria não só existir, mas estar bem configurado. Teria que definir uma métrica para refletir o "bem configurado".
3	Concordo totalmente	Firewall de borda é o primeiro nível de proteção, sendo consideração fundamental e até básico. A inexistência de um simples firewall de borda afeta em muito o nível de criticidade das vulnerabilidades.
4	Concordo totalmente	Tanto a conscientização dos usuários/efetivos, quanto a aplicação de mecanismos de segurança reduzem consideravelmente a superfície de ataque.

Avaliação dos comentários.

Para os 4 comentários, em virtude de ser uma área de maior conhecimento dos especialistas, há muita especificação sobre as atividades a serem avaliadas. Ao se observar o conjunto de controles com suas escalas de avaliação, pode-se compreender que as sugestões já haviam sido acatadas, o que sugere que os comentários foram efetivados pelos executores que não participaram da definição das escalas de avaliação, mas demonstram maturidade no assunto.

Pergunta 12:

Você concorda que para **proteção do perímetro da rede** sob a responsabilidade da organização, a **presença de IPS e/ou IDS** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 12:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para proteção do perímetro da rede sob a responsabilidade da organização, a presença de IPS e/ou IDS constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	Aprovada

Comentários enviados para a pergunta 12:

Id.	Resposta	Comentário
1	Concordo	A presença de firewall, IDS e IPS são nível de ferramentas com a mesma finalidade de proteção de borda.
2	Concordo	Só a presença não seria o ideal. O ideal seria não só existir, mas estar bem configurado. Teria que definir uma métrica para refletir o "bem configurado".
3	Concordo totalmente	Tanto a conscientização dos usuários/efetivos, quanto a aplicação de ferramentas de segurança reduzem consideravelmente a superfície de ataque.

Avaliação dos comentários.

Os comentários refletem exatamente a mesma maturidade analisada pelos comentários da questão 11..

Grupo de controles: Proteção da Aplicação.

Controles:

1. Presença de Proxy Reverso
2. Presença de Firewall de Aplicação web

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Proteção da Aplicação	Presença de Proxy Reverso	Verifica se há proteção das Aplicações por Proxy Reverso	NSCA7-13 (3.3 e Anexos D), ABNT NBR ISO/IEC 27001:2013 (A.13), ABNT NBR ISO/IEC 27032:2015 (12.4), Nist Cybersecurity Framework V 1.1 (DE.CM-1).
	Presença de Firewall de Aplicação web	Observa se há proteção das Aplicações por WAF – (Web Application Firewall)	NSCA7-13 (3.3 e Anexos D), ABNT NBR ISO/IEC 27001:2013 (A.13), ABNT NBR ISO/IEC 27032:2015 (12.4), CIS Control #13, Nist Cybersecurity Framework V 1.1 (DE.CM-1).

Pergunta 13:

Você concorda que para **proteção das aplicações** sob a responsabilidade da organização, a **presença de um proxy reverso** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 13:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para proteção das aplicações sob a responsabilidade da organização, a presença de um proxy reverso constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	45%	45%	10%	0%	Aprovada

Comentários enviados para a pergunta 13:

Id.	Resposta	Comentário
1	Concordo totalmente	A aplicação de ferramentas de segurança reduz consideravelmente a superfície de ataque.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corrobora as respostas dadas.

Pergunta 14:

Você concorda que para **proteção das aplicações** sob a responsabilidade da organização, a **presença de um firewall de aplicações web (WAF em inglês)** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 14:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para proteção das aplicações sob a responsabilidade da organização, a presença de um firewall de aplicações web (WAF em inglês) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	60%	40%	0%	0%	Aprovada

Comentários enviados para a pergunta 14:

Id.	Resposta	Comentário
1	Concordo totalmente	A aplicação de ferramentas de segurança reduz consideravelmente a superfície de ataque.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corrobora as respostas dadas.

Grupo de controles: Proteção do acesso ao sistema ou serviço.

Controles:

1. Presença de privilégios desnecessários ativos
2. Presença de contas desnecessárias ativas

Pergunta 15:

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Proteção do Acesso ao sistema ou serviço	Presença de privilégios desnecessários ativos	Investiga se há contas de usuários com privilégios administrativos que não necessitem deste nível de acesso.	NSCA7-13 (Anexo B, item 1.27), ABNT NBR ISO/IEC 27001:2013 (A.9.2, A.9.4), CIS Control #5, NIST Special Publication 800-53 Revision 4 (AC-2; AC-3, AC-6), Nist Cybersecurity Framework V 1.1 (PR.AC-1).
	Presença de contas desnecessárias ativas	Observa se há contas ativas de usuários que se encontram inativos ou desligados da organização (Desligados, afastados ou em férias).	NSCA7-13 (Anexo A, itens 3 e 4; Anexo B,), ABNT NBR ISO/IEC 27001:2013 (A.9.2, A.9.4), CIS Control #5, NIST Special Publication 800-53 Revision 4 (AC-2; AC-6), Nist Cybersecurity Framework V 1.1 (PR.AC-1).

Você concorda que para **proteção do acesso ao sistema ou serviço** sob a responsabilidade da organização, a investigação sobre a **presença de privilégios desnecessários ativos** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 15:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para proteção do acesso ao sistema ou serviço sob a responsabilidade da organização, a investigação sobre a presença de privilégios desnecessários ativos constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	70%	25%	5%	0%	Aprovada

Comentários enviados para a pergunta 15:

	Resposta	Comentário
1	Concordo totalmente	Tudo isso faz parte de um processo: Controle de Acessos e gestão de senhas ou cofre de senhas. Existem ferramentas e soluções no mercado para fazer essa gestão. Ou seja, o controle seria algo como: Controle de Acesso e de gestão de senhas.
2	Discordo	A avaliação/verificação desse controle pode ser muito complexa e subjetiva, deixando a análise inviável.
3	Concordo totalmente	Ressalva de que o ideal seria a "ausência" e não a "presença".
4	Concordo totalmente	Contas com privilégios desnecessários aumentam a probabilidade de escalação de privilégio por um agente mal-intencionado.

Avaliação dos comentários.

O comentário 2 foi a única discordância neste quesito avaliado. A análise está correta e foi objeto de discussão quando da definição do controle. O grupo de analistas que discutiu a criação do controle chegou a um consenso semelhante, mas optou por manter o controle em virtude de ser um ponto importante a ser avaliado para mitigar riscos, os procedimentos operacionais de verificação de privilégios acima do necessário ativo, prescrevendo a manutenção de privilégios estritamente necessários às atividades.

Pergunta 16:

Você concorda que para **proteção do acesso ao sistema ou serviço** sob a responsabilidade da organização, a investigação sobre a **presença de contas desnecessárias ativas** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 16:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para proteção do acesso ao sistema ou serviço sob a responsabilidade da organização, a investigação sobre a presença de contas desnecessárias ativas constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	70%	25%	5%	0%	Aprovada

Comentários enviados para a pergunta 16:

Id.	Resposta	Comentário
1	Discordo	A avaliação/verificação desse controle pode ser muito complexa e subjetiva, deixando a análise inviável.
2	Concordo totalmente	Ressalva de que o ideal seria a "ausência" e não a "presença".
3	Concordo totalmente	Concordo totalmente, para os casos de desligamento de usuários ou afastamento por longo período.
4	Concordo totalmente	Contas sem uso aumentam a superfície de ataque por um agente mal-intencionado.

Avaliação dos comentários.

O significado destes comentários e suas justificativas são exatamente os mesmos da pergunta 15.

Grupo de controles: Proteção do Ativo / Serviço.

Controles:

1. Uso de Criptografia
2. Presença de portas de rede desnecessárias abertas
3. Nível de Exposição do ativo
4. Homologação de Sigilo
5. Proteção contra malwares
6. Proteção física dos ativos

Grupo de Controles	Controle	Caracterização	Origem do Controle (Embasamento)
Proteção do Ativo / Serviço	Uso de Criptografia	Investiga se há uso de criptografia no uso dos serviços, comunicações ou aplicações de forma coerente e eficaz.	NSCA7-13 (Anexo C, itens d, e), ABNT NBR ISO/IEC 27001:2013 (A.10), NIST Special Publication 800-53 Revision 4 (IA-7) Nist Cybersecurity Framework V 1.1 (PR.DS-1, PR.DS-2).
	Presença de Portas abertas desnecessárias	Verifica se há portas de rede ou serviços (TCP/UDP) abertos além das necessidades da(s) aplicação(ões), ativo(s) ou serviços (incluindo acesso remoto)	ABNT NBR ISO/IEC 27032:2015 (9.4.3), Nist Cybersecurity Framework V 1.1 (PR.AC-3).
	Nível de Exposição do ativo	Observa a amplitude da disponibilidade do ativo em termos de redes que aumentem ou reduzam exposição a ataques	ABNT NBR ISO/IEC 27001:2013 (A.12.1.4), NIST SP 800-115 (item 2.4), LM Ciber Kill Chain – (Reconnaissance and Delivery são facilitadas de acordo com a exposição do ativo).
	Homologação de Sigilo	Identifica se o sistema que manipula dados sigilosos foi homologado pela inteligência, se for o caso.	ICA205-47 (3.1.2, 4.5, 5.7, 6.3, 6.5), ICA 200-8/2008 (1.5, 3.1), ABNT NBR ISO/IEC 27001:2013 (A.8.2), Nist Cybersecurity Framework V 1.1 (PR.DS-5).
	Proteção contra malwares	Investiga se há proteção dos ativos por software antivírus ou contra códigos maliciosos do tipo adware, spyware, cavalo-de-tróia (trojans, worms, backdoors, keyloggers, bots, botnets, rootkit e outros padronizado pela organização)	NSCA7-13 (3.3 e Anexo D), ABNT NBR ISO/IEC 27001:2013 (A.12.2), NIST Special Publication 800-53 Revision 4 (SI-3), Nist Cybersecurity Framework V 1.1 (PR.DS-8, DE.CM-4).
	Proteção física dos ativos	Observa se há proteção física dos ativos de rede e dos recursos computacionais mais importantes (acesso, energia, climatização, fogo, monitoramento, cabeamento etc.)	NSCA7-13 (3.1), ABNT NBR ISO/IEC 27001:2013 (A.11.1, A.11.2), NIST Special Publication 800-53 Revision 4 (PE-1; PE-3; PE-6; PE-9; PE-11; PE-13; PE-14; PE-15), Nist Cybersecurity Framework V 1.1 (PR.AC-2).

Pergunta 17:

Você concorda que para **Proteção do Ativo / Serviço** sob a responsabilidade da organização, a investigação sobre o **uso efetivo de criptografia** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 17:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre o uso efetivo de criptografia constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	55%	40%	5%	0%	Aprovada

Comentários enviados para a pergunta 17:

Id.	Resposta	Comentário
1	Discordo	Controle subjetivo (definir coerente e eficaz). Talvez ajustar esse controle para "Avalia a obrigatoriedade de uso de criptografia no uso do serviço e investiga se o tipo criptografia utilizado é coerente e eficaz".
2	Concordo	Somente para os casos em que a confidencialidade é relevante. Para sistemas em que esse requisito de SI não é necessário, a criptografia não é relevante.
3	Concordo	A depender do nível de criticidade das informações trafegadas naquele ativo.
4	Concordo totalmente	O uso de criptografia reduz consideravelmente a interceptação da informação por ataques, com por exemplo o man-in-the-middle.

Avaliação dos comentários.

Para o comentário nº 1, única discordância da questão é justificado pela determinação, pelos especialistas que definiram os controles, para que se fizesse efetiva a verificação de criptografia em atividades que assim o exigissem. Como já foi explicado, os controles servem exatamente como um checklist de segurança, não somente como um cálculo de valor de risco ou mitigação. Sua ausência em caso de necessidade aumenta o nível de exposição ao risco. Além disso, se o sistema não exige criptografia, há o recurso de estabelecer a escala "não se aplica" ao controle e eliminá-lo do cálculo.

Pergunta 18:

Você concorda que para **Proteção do Ativo / Serviço** sob a responsabilidade da organização, a investigação sobre a **presença de portas de rede desnecessárias abertas** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 18:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a presença de portas de rede desnecessárias abertas constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	75%	25%	0%	0%	Aprovada

Comentários enviados para a pergunta 18:

Id.	Resposta	Comentário
1	Concordo totalmente	Se essas são desnecessárias então não deve ser controlada e sim corrigida.
2	Concordo totalmente	Portas desnecessárias abertas aumentam a superfície de ataque por um agente mal-intencionado.

Avaliação dos comentários.

Comentário e justificativa similar à da questão 17. Não se trata de controlar a quantidade de portas abertas e sim de se verificar se há alguma, e isso estabelece um valor de risco maior, ou menor se as mesmas forem fechadas, logo o controle serve como um checklist de mitigação.

Pergunta 19:

Você concorda que para **Proteção do Ativo / Serviço** sob a responsabilidade da organização, a investigação sobre o **Nível de Exposição do ativo (como estar fisicamente em uma rede segregada, intranet ou na Internet)** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 19:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre o Nível de Exposição do ativo (como estar fisicamente em uma rede segregada, intranet ou na Internet) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	75%	25%	0%	0%	Aprovada

Comentários enviados para a pergunta 19:

	Resposta	Comentário
1	Concordo totalmente	Quanto mais exposto um ativo crítico, maior será a probabilidade de o ataque causar um dano maior.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Pergunta 20:

Você concorda que para **Proteção do Ativo / Serviço** sob a responsabilidade da organização, a investigação sobre a **Homologação de Sigilo (por órgão de inteligência que possa auditar e certificar)**, para sistemas que manipulem informações com grau de sigilo constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 20:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a Homologação de Sigilo (por órgão de inteligência que possa auditar e certificar) , para sistemas que manipulem informações com grau de sigilo constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	55%	35%	10%	0%	Aprovada

Comentários enviados para a pergunta 20:

Id.	Resposta	Comentário
1	Concordo totalmente	Não entendi bem essa. Homologação de sigilo? auditar?
2	Discordo	Verificar se na FAB existe hoje alguma norma que demanda isso.
3	Concordo	Relevante nos casos em que a confidencialidade é importante.
4	Concordo	Ativos/Sistemas críticos devem ser testados/homologados antes de ser colocado em produção.

Avaliação dos comentários.

Os comentários nº 1 e 2 refletem dúvidas de integrantes que não estão familiarizados com desenvolvimento de software, pois no caso específico da FAB e dos órgãos governamentais, os softwares que armazenam, tratam ou tramitam dados sigilosos devem passar por auditoria prévia de órgãos de inteligência para verificação de conformidade com os preceitos definidos pelas normas de inteligência (sigilosas) que existem tanto na FAB como em outros órgãos governamentais. O controle se justifica em virtude da compliance devida. Não houve divergências entre os analistas quando da criação do controle.

Pergunta 21:

Você concorda que para **Proteção do Ativo / Serviço** sob a responsabilidade da organização, a investigação sobre a **presença de proteção contra malwares (como vírus, spywares, trojans, backdoors etc.)** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 21:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a presença de proteção contra malwares (como vírus, spywares, trojans, backdoors etc.) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	75%	25%	0%	0%	Aprovada

Comentários enviados para a pergunta 21:

Id.	Resposta	Comentário
1	Concordo totalmente	A proteção contra malware é um fator importante para evitar ataques cibernéticos.

Avaliação dos comentários.

Nenhum comentário necessita de avaliação, pois somente corroboram as respostas dadas.

Pergunta 22:

Você concorda que para **Proteção do Ativo / Serviço** sob a responsabilidade da organização, a investigação sobre a **Proteção física dos ativos (acesso físico, energia, climatização, monitoramento, cabeamento etc.)** constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 22:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a Proteção física dos ativos (acesso físico, energia, climatização, monitoramento, cabeamento etc.) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	Aprovada

Comentários enviados para a pergunta 22:

Resposta	Comentário
Não houve comentários para esta pergunta.	

Grupo de controles: Avaliação da interface da ferramenta computacional para ARCiber.

Controles:

1. Validade da escala da eficácia dos controles (TCU) para as escalas dos controles
2. Facilidade do uso da ferramenta
3. Utilidade/validade percebida da ferramenta

Tabela 1 - Definição da Eficácia dos Controles (TCU)

Nível de Confiança ou eficácia do controle (NC)	Situação do Controle Existente	Multiplicador do Risco Inerente	Valores para a seleção qualitativa do nível do controle ¹ .
Inexistente NC = 0%	Ausência completa de controle ou controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1,00	5
Fraca NC = 20%	Controle deixa de atender ao requisito de mitigação de riscos em sua maior parte. Apoiado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual havendo confiança no conhecimento das pessoas.	0,80	4
Mediana NC = 40%	Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	0,60	3
Satisfatória NC = 60%	Controle normatizado e embora passível de aperfeiçoamento, está sustentado por ferramentas adequadas e mitiga o risco razoavelmente.	0,40	2
Forte NC = 80%	Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrado num nível de “melhor prática”.	0,20	1

Fonte: adaptado de Brasil.TCU(2017)

Pergunta 23:

Para o uso da ferramenta computacional para ARCiber e a comparação das vulnerabilidades com os controles e a consequente avaliação da mitigação dos riscos inerentes (brutos, via CVSS), necessita-se de escalas padronizadas. As escalas usadas na ferramenta receberam padronização de eficácia por uma escala desenvolvida pelo TCU, conforme a Tabela 1 contida no enunciado desta página. Você concorda que as escalas usadas nos controles da ferramenta foram eficazes em permitir a avaliação da mitigação dos riscos?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 23:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Para o uso da ferramenta computacional para ARCiber e a comparação das vulnerabilidades com os controles e a consequente avaliação da mitigação dos riscos inerentes (brutos, via CVSS), necessita-se de escalas padronizadas. As escalas usadas na ferramenta receberam padronização de eficácia por uma escala desenvolvida pelo TCU, conforme a Tabela 1 contida no enunciado desta página. Você concorda que as escalas usadas nos controles da ferramenta foram eficazes em permitir a avaliação da mitigação dos riscos?	20	30%	60%	0%	10%	Aprovada

Comentários enviados para a pergunta 23:

Id.	Resposta	Comentário
1	Concordo	Não entendi muito a padronização de eficácia com a tabela, precisa esclarecer ou fazer uma contextualização melhor nessa. Assim como, o termo “foram eficazes” está inadequado visto a pergunta seria se estivéssemos analisando um caso passado em que foi feito isso. Nesse, seria: está completa a graduação de níveis, ou mesmo, essa graduação atende a todas as possibilidades, ou algo assim.
2	Discordo totalmente	Por que os valores para seleção qualitativa estão inversos ao nível de eficácia do controle? Sugiro colocar de 1 a 5 (e não de 5 a 1)
3	Discordo totalmente	Não uso a ferramenta
4	Concordo	É importante frisar a respeito da escala desenvolvida pelo TCU, que deve ser avaliada de acordo com a realidade de cada organização. Mas a escala em questão possui coerência de critério.
5	Concordo	Acredito que as escalas padronizadas podem dar uma direção na avaliação da mitigação dos riscos. No entanto, deve haver espaço para tratamento de exceções de acordo com o cenário.

Avaliação dos comentários.

Os comentários refletem que o manual não foi suficientemente lido. Primeiramente os controles e seus fatores multiplicadores refletem o grau de risco, ou seja, de falta de proteção, por isso os valores de 5 a 1, pois o valor 5 corresponde a uma proteção nula pelos controles e o valor 1 à proteção máxima possível (80%) pelo controle. O usuário não precisa conhecer esta metodologia, pois foi usada para embasar cada controle à sua necessidade de linguagem. Exemplificando, para um controle de backup, uma proteção máxima (1) exige que o backup exista, esteja completo, atualizado e testado, e nível 5, como inexistente, diferente de um controle como o de criptografia, cuja escala é binária (existe [1] e não existe mesmo sendo necessário [5]). Logo esta análise da escala não configura um controle e consistiu em uma testagem da conscientização dos futuros usuários no padrão das escalas adotadas. O valor de 90% de aceitação refletiu que a grande maioria compreendeu esta parte do processo.

O comentário nº 3 reflete somente que o respondente não observou as instruções do questionário, e pertence a uma equipe que não necessitará utilizar rotineiramente este processo de avaliação de riscos.

Pergunta 24:

Durante o uso da ferramenta computacional para ARCiber você avalia que foi de utilização fácil e/ou intuitiva?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 24:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Durante o uso da ferramenta computacional para ARCiber você avalia que foi de utilização fácil e/ou intuitiva?	20	25%	60%	5%	10%	Aprovada

Comentários enviados para a pergunta 24:

Id.	Resposta	Comentário
1	Discordo	Desconheço a ferramenta
2	Concordo	Não utilizei, mas deveria ser mais específica, tipo: ao utilizar o Archer, na inserção de XYZ, ou mesmo, na gestão de riscos a ferramenta atende todas as necessidades? ou algo assim.
3	Discordo totalmente	Qual ferramenta computacional para ARCiber? Não compreendi a pergunta.
4	Discordo totalmente	Não uso a ferramenta
5	Concordo	Após breve explicação e compreensão do manual foi possível compreendê-la.

Avaliação dos comentários.

Os comentários nº 1 e 4 refletem somente que o respondente não observou as instruções do questionário, e pertence a uma equipe que não necessitará utilizar rotineiramente este processo de avaliação de riscos. O comentário nº 2 reflete a

ansiedade no uso do Archer, e será respondido quando a ferramenta estiver plenamente operante e incorporada aos processos do NuCDCAer.

Pergunta 25:

Durante o uso da ferramenta computacional para ARCiber você avalia que a ferramenta possui utilidade/validade para a gestão de riscos do NuCDCAer?

Respostas oferecidas: () Concordo totalmente () Concordo () Discordo () Discordo totalmente

Resultado da primeira rodada para a pergunta 25:

Texto da questão	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	Resultado para esta questão
Durante o uso da ferramenta computacional para ARCiber você avalia que a ferramenta possui utilidade/validade para a gestão de riscos do NuCDCAer?	20	45%	40%	5%	10%	Aprovada

Comentários enviados para a pergunta 25:

Id.	Resposta	Comentário
1	Concordo	Imagino que sim né?
2	Discordo totalmente	Qual ferramenta computacional para ARCiber? Não compreendia a pergunta.
3	Discordo totalmente	Não uso a ferramenta

Avaliação dos comentários.

Os comentários nº 2 e 3 refletem somente que o respondente não observou as instruções do questionário, e pertence a uma equipe que não necessitará utilizar rotineiramente este processo de avaliação de riscos.

Texto de agradecimento da Rodada1

Obrigado, seu questionário está completo.

Esta foi a primeira rodada, pois necessitaremos de sua ajuda mais uma vez. Nosso trabalho como profissionais de segurança/defesa cibernéticas é de grande importância para a FAB, e para nosso país. Fazemos nossa parte e juntos podemos sempre mais.

Mais uma vez, obrigado pela sua participação.

Resumo e análise da Rodada 1

Fórmula de aprovação/reprovação do consenso de cada questão:

- Respostas POSITIVAS (aceitação): Concordo totalmente, Concordo.
- Respostas NEGATIVAS (rejeição): Discordo totalmente, Discordo.

Resultado para cada questão:

- **Aprovação:** %Concordo totalmente + %Concordo \geq 80%
- **Reprovação:** %Discordo totalmente + %Discordo $>$ 50% ou %Concordo totalmente + %Concordo $<$ 50%
- **Sujeito à revisão em outra rodada:** 80% $>$ (%Concordo totalmente + %Concordo) \geq 50%

Nº da Pergunta	Texto da pergunta	Total de respondentes	Concordo totalmente	Concordo	Discordo	Discordo totalmente	%Aprovação	%Reprovação	Resultado para esta questão
1	Você concorda que para Entrada das vulnerabilidades, o cadastramento das criticidades das vulnerabilidades por meio de relatórios de vulnerabilidades do ativo (pentests ou scans de rede), ou de relatórios externos que indiquem vulnerabilidades para o tipo de ativo com valores definidos pela escala do CVSS seja uma forma eficaz de entrada de dados para analisar as vulnerabilidades dos ativos do ambiente do NuCDCAer?	20	60%	40%	0%	0%	100%	0%	Aprovada
2	Você concorda que para Análise da Vulnerabilidade, o tempo de existência de uma vulnerabilidade é um fator importante para a análise do ambiente em risco a ponto de ser considerado um controle que deva constar em uma ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	100%	0%	Aprovada
3	Você concorda que para Análise da Vulnerabilidade, uma limitação do escopo da análise de riscos, como o ativo estar em um ambiente de produção, homologação ou desenvolvimento, ou haver indicação de impossibilidade de análise completa em função de sigilo ou permissão de autoridade competente configura um fator relevante para a existência deste controle constar em uma ferramenta de análise de riscos cibernéticos?	20	55%	40%	5%	0%	95%	5%	Aprovada
4	Você concorda que para Aspectos/Implicações Legais, possíveis impactos por aspectos legais que uma vulnerabilidade explorada possa ocasionar à organização é um fator importante para a análise do ambiente em risco a ponto de ser considerado um controle que deva constar em uma ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	100%	0%	Aprovada
5	Você concorda que para Aspectos/Implicações Legais, possíveis limitações contratuais possam impedir o uso de boas práticas de segurança cibernética a ponto de ser necessária a existência de um controle para evidenciar estas dúvidas e assim constar (controle) em uma ferramenta de análise de riscos cibernéticos?	20	30%	55%	15%	0%	85%	15%	Aprovada
6	Você concorda que para Aspectos/Implicações Legais, a gestão de logs (de acesso à rede e de ativos de rede diversos) constitui um controle que deve ser observado e incluído em análises de vulnerabilidades do ambiente em risco como um aspecto com implicações legais e como tal deve constar em na ferramenta de análise de riscos cibernéticos?	20	50%	40%	10%	0%	90%	10%	Aprovada
7	Você concorda que para Ações de Reposta / Continuidade dos negócios, um processo de identificação de possíveis impactos por tempo de recuperação (BIA – Business Impact Analysis) como elemento (controle) preventivo para mitigação de impactos por incidentes com os ativos críticos da organização constitui um controle que deve ser incluído em análises de vulnerabilidades do ambiente em risco e deve constar na ferramenta de análise de riscos cibernéticos?	20	60%	30%	5%	5%	90%	10%	Aprovada
8	Você concorda que para Ações de Reposta / Continuidade dos negócios, a observação sobre a existência de alguma equipe de tratamento de incidentes de rede (ETIR) ou alguma equipe ou profissional(is) com capacitação em gestão de incidentes de rede na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	60%	35%	5%	0%	95%	5%	Aprovada

9	Você concorda que para Ações de Reposta / Continuidade dos negócios, a observação sobre a existência de planos ou planejamento da continuidade dos negócios (contingência, redundâncias, gestão de crises etc.) na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	100%	0%	Aprovada
10	Você concorda que para Ações de Reposta / Continuidade dos negócios, a observação sobre a existência de gestão de backups (planejamento, confecção, proteção e testagem) na organização em que a aplicação, ativo ou serviço estão hospedados constitui um controle eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	60%	35%	5%	0%	95%	5%	Aprovada
11	Você concorda que para proteção do perímetro da rede sob a responsabilidade da organização, a presença de um firewall de borda (ou similar, para separação de tráfego entre as redes internas e externas da organização/criação da DMZ) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	100%	0%	Aprovada
12	Você concorda que para proteção do perímetro da rede sob a responsabilidade da organização, a presença de IPS e/ou IDS constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	100%	0%	Aprovada
13	Você concorda que para proteção das aplicações sob a responsabilidade da organização, a presença de um proxy reverso constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	45%	45%	10%	0%	90%	10%	Aprovada
14	Você concorda que para proteção das aplicações sob a responsabilidade da organização, a presença de um firewall de aplicações web (WAF em inglês) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	60%	40%	0%	0%	100%	0%	Aprovada
15	Você concorda que para proteção do acesso ao sistema ou serviço sob a responsabilidade da organização, a investigação sobre a presença de privilégios desnecessários ativos constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	70%	25%	5%	0%	95%	5%	Aprovada
16	Você concorda que para proteção do acesso ao sistema ou serviço sob a responsabilidade da organização, a investigação sobre a presença de contas desnecessárias ativas constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	70%	25%	5%	0%	95%	5%	Aprovada
17	Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre o uso efetivo de criptografia constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	55%	40%	5%	0%	95%	5%	Aprovada
18	Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a presença de portas de rede desnecessárias abertas constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	75%	25%	0%	0%	100%	0%	Aprovada
19	Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre o Nível de Exposição do ativo (como estar fisicamente em uma rede segregada, intranet ou na Internet) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	75%	25%	0%	0%	100%	0%	Aprovada

20	Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a Homologação de Sigilo (por órgão de inteligência que possa auditar e certificar), para sistemas que manipulem informações com grau de sigilo constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	55%	35%	10%	0%	90%	10%	Aprovada
21	Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a presença de proteção contra malwares (como vírus, spywares, trojans, backdoors etc.) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	75%	25%	0%	0%	100%	0%	Aprovada
22	Você concorda que para Proteção do Ativo / Serviço sob a responsabilidade da organização, a investigação sobre a Proteção física dos ativos (acesso físico, energia, climatização, monitoramento, cabeamento etc.) constitui um controle mínimo eficaz para mitigação de riscos cibernéticos que deve ser incluído em análises de vulnerabilidades via ferramenta de análise de riscos cibernéticos?	20	65%	35%	0%	0%	100%	0%	Aprovada
23	Para o uso da ferramenta computacional para ARCiber e a comparação das vulnerabilidades com os controles e a consequente avaliação da mitigação dos riscos inerentes (brutos, via CVSS), necessita-se de escalas padronizadas. As escalas usadas na ferramenta receberam padronização de eficácia por uma escala desenvolvida pelo TCU, conforme a Tabela 1 contida no enunciado desta página. Você concorda que as escalas usadas nos controles da ferramenta foram eficazes em permitir a avaliação da mitigação dos riscos?	20	30%	60%	0%	10%	90%	10%	Aprovada
24	Durante o uso da ferramenta computacional para ARCiber você avalia que foi de utilização fácil e/ou intuitiva?	20	25%	60%	5%	10%	85%	15%	Aprovada
25	Durante o uso da ferramenta computacional para ARCiber você avalia que a ferramenta possui utilidade/validade para a gestão de riscos do NuCDCAer?	20	45%	40%	5%	10%	85%	15%	Aprovada

Análise dos resultados da rodada 1 (e do processo do método Delphi)

A grande aprovação dos controles da ferramenta foi avaliada pela equipe da SGI e chegou-se à conclusão que diversos fatores levaram a este resultado de consenso em uma única rodada. São eles:

- Capacitação da grande maioria em segurança/defesa cibernética, dependente direta da gestão de riscos;
- Apesar de alguns respondentes ainda terem pouca experiência nos processos de avaliação de riscos cibernéticos em função de suas atividades cotidianas em outros processos da área, por terem participado de algumas entrevistas, foram instruídos sobre as técnicas e tiveram aumento de suas maturidades neste quesito, de forma suficiente para a compreensão das necessidades de controles;
- Curiosidade do efetivo no processo em virtude do início de implantação do RSA Archer, cuja metodologia de gestão de riscos cibernéticos foi derivada do processo de ARCIBER desenvolvido;
- Necessidade demonstrada pelo efetivo em tornar o RSA Archer uma ferramenta centralizadora de dados para os processos de segurança/defesa cibernética;
- Foco na estruturação do NuCDCAer, com o efetivo se dedicando ao trabalho de aprendizado e planejamento das funções básicas e avançadas de segurança/defesa cibernética, o que pode explicar a boa vontade e presteza nas respostas sobre o processo de avaliação de riscos cibernéticos (ARCIBER), evidenciado pela ferramenta em formato prototipado em planilha MS Excel e LibreOffice Calc;
- Juntamente com o convite para o questionário, foram enviados textos explicativos, links para a ferramenta nas duas plataformas (Microsoft e Libre Office), além do manual de uso da ferramenta, para eventuais dúvidas sobre assuntos não usuais de algumas seções;
- Algumas respostas negativas evidenciam que alguns respondentes não leram alguns textos, nem abriram a ferramenta, ou seja, foram direto ao link do questionário, apesar de a maioria ter feito uso dela durante o planejamento e construção.

Apêndice F

Artigos publicados durante o período do PPCA

Artigos publicados durante o período do PPCA

Artigos completos publicados em periódicos

Farias, Priscila de Araújo ; de Lima, Cleber Mitchell ; Monteiro, Simone Borges Simão ; Reis, Ana Carla Bittencourt . Proposta de um Método para Priorização de Projetos de Infraestrutura de TI. Revista Ibérica de Sistemas e Tecnologias de Informação RISTI (PORTO), n. E27, p. 763-776, 2020. ISSN: 1646-9895.

Capítulos de livros publicados

Costa, João Paulo Vieira ; de Lima, Cleber Mitchell ; Almeida, Newton Franklin ; Chaim, Ricardo Matos ; Souza, João Carlos Félix . Model for Dynamics Credit Risk Characterization and Profit Inference in Credit Card Fintechs. Advances in Intelligent Systems and Computing. 1ed.: Springer International Publishing, 2021, v. 1367, p. 411-421. DOI: 10.1007/978-3-030-72660-7_40

Trabalhos completos publicados em anais de congressos

de Oliveira, Jose Fabio ; de Lima, Cleber Mitchell ; Almeida, Newton Franklin ; Mariano, Ari Melo ; Bittencourt Reis, Ana Carla ; da Silva, Joao Mello . Costs influence and mediating effect of corporate risk management on organizational performance: a study applied to the Brazilian Public Service. In: 2021 16th Iberian Conference on Information Systems and Technologies (CISTI), 2021, Chaves. 2021 16th Iberian Conference on Information Systems and Technologies (CISTI). Red Hook: IEEE, 2021. p. 1. DOI: 10.23919/CISTI52073.2021.9476392

Proposta de um Método para Priorização de Projetos de Infraestrutura de TI

Priscilla de Araújo Farias, Cléber Mitchell de Lima, Simone Borges Simão Monteiro, Ana Carla Bittencourt Reis

priscillafarias.eng@gmail.com, clebermitchell@gmail.com, simoneborges@unb.br,
anacarlabr@unb.br

Universidade de Brasília, Brasília, Distrito Federal, Brasil

Pages: 763–776

Resumo: O gerenciamento de portfólio de projetos tornou-se um desafio para as diversas organizações, uma vez constatada a necessidade de selecionar adequadamente os investimentos a serem realizados, no intuito de garantir que os objetivos estratégicos sejam alcançados de maneira mais eficiente. Dessa forma, este estudo propõe um método para a priorização de projetos utilizando uma matriz de qualidade baseada na ferramenta *fuzzy* QFD (*Quality Function Development*) e na técnica no PROMETHEE II. O método proposto foi aplicado no processo de gestão de portfólio de projetos de infraestrutura de Tecnologia da Informação do Centro Integrado de Telemática do Exército. Os resultados demonstram a aplicabilidade do método no cenário selecionado, de forma a melhorar o atual processo existente e possibilitar um adequado emprego dos recursos humanos e financeiros.

Palavras-chave: Gerenciamento de Portfólio; Seleção de Projetos; Matriz *Fuzzy* QFD; PROMETHEE II.






Proposal of a prioritizing method for IT infrastructure projects

Abstract: The management process of project portfolio has become a challenge for several organizations, since there is a need to properly select investments to be performed, aiming to ensure that the strategic objectives are achieved more efficiently. Therefore, this study proposes a method for project prioritization using a quality matrix based on the fuzzy QFD (*Quality Function Development*) tool and on the technique PROMETHEE II. The proposed method was applied to the Information Technology infrastructure project portfolio management process of Army Integrated Center for Telematics. The results demonstrate the applicability of the method within the selected scenario, in order to improve the current process and to enable a proper use of human and financial resources.

Keywords: Portfolio Management; Project Selection; Fuzzy QFD Matrix; PROMETHEE II.



Model for Dynamics Credit Risk Characterization and Profit Inference in Credit Card Fintechs

João Paulo Vieira Costa^() , Cleber Mitchell de Lima^() ,
Newton Franklin Almeida^() , Ricardo Matos Chaim^() ,
and João Carlos Félix Souza^() 

University of Brasília, Brasília, Brazil
{190135042, 190132311, 190133031}@aluno.unb.br,
{ricardoc, jocafs}@unb.br

Abstract. Fintechs have gained strong momentum in recent years showing high growth rates and very significant turnover. Agile, differentiated and technological services, including credit cards, are successfully facing traditional banking services. In this article, a case study in the Brazilian financial market, System Dynamics simulates the adoption of technology and products of these new banking services. The modeling adopts regulatory parameters of the Central Bank of Brazil, regarding customer portfolio, credit portfolio of the revolving revenue, credit loss provisioning, and default rate. The focus is mapping credit risk dynamics in Brazilian markets to support decision of managers and investors. The results, obtained from the simulations, showed positive and growing profits when we use variables with similar values to those of the current scenario. Additionally, action on interest rates on revolving credit rates affects the profitability of these projects. The presented system can be used to support investment evaluation and or managers decision in this area.

Keywords: Fintech · System dynamics · Credit card · Credit risk

1 Introduction

The credit market represents the financial market segment where institutions raise funds from sectors that have resources available and offer loans to sectors or customers in need. Hence, they are remunerated by the difference between what is lent and what is received (spread) [1]. Usually, these are operations with a limited and short term, for emergency actions and have the characteristic of having a legal order and contractual formalization. Understanding its dynamics is essential for the smooth functioning of the gears of any country's economy and its interaction with others.

Understanding the difficulties in calculating risks inherent to this dynamic is a major factor, according to Wenzler [2], for which it is possible to price them accurately, provided that the appropriate structural model is adopted. With the use of a correct modeling it is possible to reduce risks and uncertainties, which is a necessary fact to be taken into

Influência dos custos e o efeito mediador do gerenciamento de riscos corporativos no desempenho organizacional: um estudo no Serviço Público Brasileiro

Costs influence and mediating effect of corporate risk management on organizational performance: a study applied to the Brazilian Public Service

José Fábio de Oliveira, Cleber Mitchell de Lima, Newton Franklin Almeida,

Ari Melo Mariano, Ana Carla Bittencourt Reis e João Mello da Silva

Universidade de Brasília

Brasília, Brasil

oliveira.jose@aluno.unb.br, cleber.lima@aluno.unb.br, newton.almeida@aluno.unb.br,
arimariano@unb.br, anacarlabr@unb.br e joaomello@unb.br

Resumo — O objetivo deste estudo exploratório foi avaliar o efeito mediador do Gerenciamento de Riscos Corporativos no desempenho das instituições públicas brasileiras. Para alcançar o objetivo foi realizada uma pesquisa do tipo exploratória, com abordagem quantitativa via equações estruturais. Um questionário foi aplicado para 139 funcionários públicos de 15 diferentes organizações públicas do governo. Os resultados identificaram um efeito mediador significativo do Gerenciamento de Riscos Corporativos na relação entre estratégias de negócio e o desempenho das instituições públicas brasileiras, e uma relação direta de 13,3%. Sendo assim, as instituições devem dedicar-se a gestão de riscos corporativos como fator potencializador de suas estratégias de negócio. Examinando o Gerenciamento de Riscos, observou-se que ele foi explicado em 32,1%, sendo as variáveis que mais impactam são a liderança de custo, seguida da diferenciação.

Palavras Chave – *PLS-SEM; Gerenciamento de Riscos Corporativos; Desempenho organizacional; Setor público.*

Abstract - The objective of this exploratory study was to evaluate the mediating effect of Corporate Risk Management on the performance of Brazilian public institutions. To achieve the objective, an exploratory research was carried out, with a quantitative approach via structural equations. A questionnaire was applied to 139 civil servants from 15 different public government organizations. The results identified a significant mediating effect of Corporate Risk Management in the relationship between business strategies and the performance of Brazilian public institutions, and a direct ratio of 13.3%. Therefore, institutions must dedicate themselves to corporate risk management as a factor that enhances their business strategies. Examining Risk Management, it was observed that it was explained in 32.1%, with the variables that most impact being cost leadership, followed by differentiation.

Keywords - *PLS-SEM; enterprise risk management; compliance; organizational performance; Public sector.*

I. INTRODUÇÃO

As pressões por eficiência no setor público se intensificaram desde a crise financeira global de 2008, com orçamentos em declínio e aumento da demanda por serviços públicos de qualidade. Desde então, os governos estão em busca de economias significativas de custos, com a reorganização institucional [1]. Contudo, essa reorganização governamental pode acarretar a geração de eventos não planejados ou incertos, caracterizados por riscos, os quais são o efeito da incerteza nos objetivos da organização, conforme definição da norma ISO 31000 [2] e podem variar em natureza, gravidade e consequência. A necessidade de mitigar os efeitos da incerteza não é recente, como é observado por Power [3], o qual chama atenção para uma expansão nos discursos de risco que ocorrem desde a década de 1990.

Segundo o COSO [4] o Gerenciamento de Riscos Corporativos (GRC) é um conjunto formado pela cultura, capacidades e práticas, integradas com o estabelecimento de estratégias e desempenho do qual as organizações dependem para gerenciar riscos na criação, preservação e realização de valor. O GRC surgiu como um novo paradigma para gerenciar o portfólio de riscos, que as organizações enfrentam, segundo Beasley [5]. Ele destaca que os formuladores de políticas continuam a se concentrar em mecanismos para melhorar a governança corporativa e a gestão de riscos. Apesar de o GRC