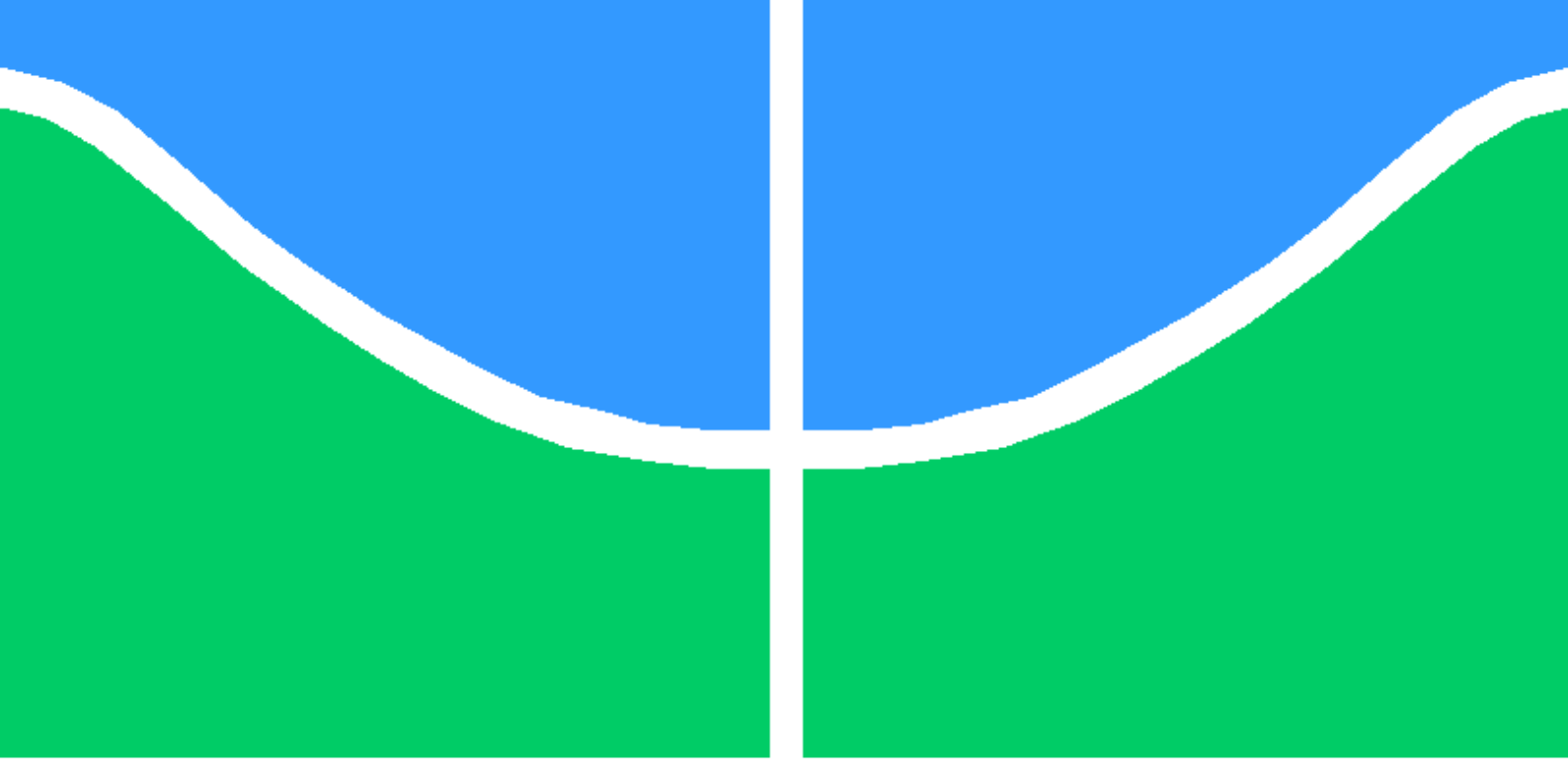

TRABALHO DE GRADUAÇÃO

ESTUDO COMPARATIVO ENTRE REGULAMENTAÇÕES GOVERNAMENTAIS E NORMAS SOCIOTÉCNICAS VIGENTES REFERENTES À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Ivy Stefany Vieira Flores

Priscila Natividade Morhy

Brasília, julho de 2013

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

ESTUDO COMPARATIVO ENTRE REGULAMENTAÇÕES GOVERNAMENTAIS E NORMAS SOCIOTÉCNICAS VIGENTES REFERENTES À GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Ivy Stefany Vieira Flores

Priscila Natividade Morhy

Relatório submetido ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Dr. Edgard Costa Oliveira (Orientador) _____
Universidade de Brasília

Prof. Me. José Edil Guimarães de Medeiros _____
Universidade de Brasília

Prof. Dr. Rafael Timóteo de Sousa Jr _____
Universidade de Brasília

Dedicatórias

Dedico este trabalho, primeiramente, aos meus pais pelo exemplo, força e incentivo dados e pela confiança que sempre tiveram em mim.
Aos demais familiares e namorado pelo apoio incondicional.
A todos que fizeram destes anos de graduação uma caminhada gratificante.
Em especial dedico ao meu Avô João Pedro que durante toda sua vida me fez sentir uma pessoa especial, renovando a minha fé em mim a cada desafio

Priscila Natividade Morhy

A dedicatória deste trabalho é dividida em três partes:
Ao meu tio Neto, por ter despertado em mim o interesse pela engenharia.
À Thiffany, que sempre acreditou na minha capacidade de criar o que eu quisesse.
À minha família, porto seguro e fonte inesgotável de força.

Ivy Stefany Vieira Flores

Agradecimentos

Aos meus pais, pelo amor maior que o infinito e a entrega incondicional. Vocês sempre fizeram de tudo para que eu fosse feliz; espero que a conclusão desta etapa faça com que sintam ao menos um décimo da felicidade que eu sinto por ser filha de vocês. E aos meus irmãos, que desde que eu consigo me lembrar cuidaram de mim e me apoiaram. Amo muito vocês! Obrigada por tudo.

Ao Íkaro, meu companheiro, amor, anjo e porto seguro, que me torna uma pessoa melhor e me faz inacreditavelmente feliz. Obrigada pela paciência, pelos sorrisos de sol, por me animar quando eu achava que nada ia dar certo, pelo carinho e por milhares de outras coisas que jamais caberiam aqui.

Aos meus amigos e primos - que compreenderam minha ausência nos últimos tempos, estiveram ao meu lado sempre que precisei, me divertiram, me fizeram sorrir e torceram por mim - o meu mais sincero agradecimento.

À Priscila, parceira de projeto final e de curso, que se tornou uma amiga ao longo destes 5 anos e meio: conseguimos! Obrigada por dividir comigo o peso que um trabalho como este pode ter, com certeza foi muito mais fácil (e divertido) escrevê-lo com você.

Ao professor Edgard, por ter aceitado prontamente o desafio de nos orientar, pelas ideias, colaboração e entusiasmo demonstrado ao longo do último ano: obrigada! Agradeço também a todos os professores da Universidade de Brasília que participaram da minha formação e me auxiliaram no processo de construção do conhecimento.

Ivy Stefany Vieira Flores

Agradeço aos meus pais por serem meu maior exemplo de perseverança e terem me ajudado a chegar até aqui sempre com muito amor, compreensão e apoio. Sem vocês, nada disso seria possível!
Ao Bruno pela paciência, incentivo, bom humor, carinho e abraços confortantes nestes meses de intensa produção.
À Ivy pela parceria, amizade, apoio, descontração e confiança em desenvolver comigo este Projeto Final.
Ao Professor Edgard de Oliveira Costa por aceitar o convite de nos orientar e nos auxiliar no amadurecimento das ideias que geraram este trabalho. Temos em você um grande "amigo-orientador".
À Tia Meire pela dedicação e auxílio nos momentos de dúvidas.
E a todos aqueles que torceram por mim e estiveram ao meu lado.

Priscila Natividade Morhy

RESUMO

Este projeto de graduação tem o objetivo de aproximar a Administração Pública Federal das práticas vigentes adotadas internacionalmente no âmbito da Gestão de Riscos de Segurança da Informação. Pensando nisso, foi realizado um estudo comparativo entre conceitos e processos apresentados pelas regulamentações governamentais - Instrução Normativa 01 DSIC/GSIPR, Norma Complementar 02 DSIC/GSIPR e Norma Complementar 04 DSIC/GSIPR - e pelas normas sociotécnicas vigentes - ABNT ISO GUIA 73:2009 e ABNT NBR ISO/IEC 27005:2011. Para a análise terminológica foi desenvolvido um questionário aplicado a especialistas da área de Segurança da Informação. Já a análise dos processos foi feita com base em pesquisa bibliográfica exploratória e análise documental. Ao final, são propostas sugestões de alinhamento de processos e harmonização dos conceitos.

Palavras-chave: Gestão de Riscos de Segurança da Informação, Normas Sociotécnicas, Regulamentações Governamentais, Administração Pública Federal, ABNT.

ABSTRACT

This graduation project aims to approximate the Brazilian Federal Public Administration to the current practices internationally adopted concerning Information Security Risk Management. Considering this, a comparative study was performed between concepts and processes introduced by governmental regulations - Instrução Normativa 01 DSIC/GSIPR, Norma Complementar 02 DSIC/GSIPR and Norma Complementar 04 DSIC/GSIPR - and current sociotechnical standards - ABNT ISO Guia 73:2009 and ABNT NBR ISO/IEC 27005:2011. For the terminological analysis a questionnaire had been developed and applied to Information Security experts. Regarding the processual analysis, an exploratory bibliographic research and a documental analysis had been done. Finally, processual alignment and conceptual harmonization recommendations are suggested.

Keywords: Information Security Risk Management, Sociotechnical Standards, Governmental Regulations, Brazilian Federal Public Administration, ABNT.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

Siglas

ABNT	Associação Brasileira de Normas Técnicas
ABNT 27005	ABNT NBR ISO/IEC 27005:2011
APF	Administração Pública Federal
CEE	Comissão de Estudo Especial
CTIR.GOV	Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal
DSIC	Departamento de Segurança da Informação e Comunicações
GR	Gestão de riscos
GRSI	Gestão de riscos de segurança da informação
GRSIC	Gestão de riscos de segurança da informação e comunicações
GSIPR	Gabinete de Segurança Institucional da Presidência da República
Guia 73	ABNT ISO GUIA 73:2009
IEC	International Electrotechnical Commission
IN	Instrução Normativa
ISO	International Organization for Standardization
MP	Ministério do Planejamento, Orçamento e Gestão
NBR	Norma Brasileira
NC	Norma Complementar
PDCA	Metodologia "Plan-Do-Check-Act"
PNS	Plano de Normalização Setorial
POSIC	Política de Segurança da Informação e Comunições
SGSI	Sistema de gestão de segurança da informação
SI	Segurança da informação
SIC	Segurança da informação e comunicações
SLTI	Secretaria de Logística e Tecnologia da Informação
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação

1 INTRODUÇÃO

1.1 DEFINIÇÃO DO PROBLEMA

Analisando detalhadamente as regulamentações voltadas aos órgãos da Administração Pública Federal - IN 01 e normas complementares - apoiadas principalmente nas normas ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005, nota-se uma disparidade em relação ao conjunto de normas elaboradas recentemente pela ABNT ISO.

Em 2009 a ABNT publicou a norma de gestão de riscos ABNT NBR ISO 31000 e a revisão de seu vocabulário ABNT ISO Guia 73 e à luz dessas duas publicações, em 2011, revisou a norma específica para gestão de riscos de segurança da informação, ABNT NBR ISO/IEC 27005. Devido aos novos padrões estabelecidos pela ABNT em 2011, surgiram diferenças de conceitos e de processos entre as propostas do governo e a normatização vigente.

Segundo um levantamento feito pelo Tribunal de Contas da União em 2012 visando a situação da governança de tecnologia da informação na Administração Pública Federal, 49% dos órgãos/entidades dos 350 selecionados como amostra de pesquisa informaram que não possuem equipe designada para gerenciar a segurança da informação e que apenas 10% realizam análise de riscos (BRASIL, 2012a). Esses dados apontam uma possível disfunção da gestão de riscos em segurança da informação na APF e a falta de aderência às regulamentações do GSIPR.

Nossa proposta é revisar as regulamentações feitas pelo GSIPR e as normas vigentes da ABNT com a intenção de compará-las e alinhá-las.

1.2 JUSTIFICATIVA

Considera-se informação como sendo o conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado. É possível observar que tudo que é desenvolvido dentro de uma organização, seja ela pública ou privada, está cada vez mais ligado a este conceito. Com o passar dos anos, a informação tornou-se um bem econômico ou ativo organizacional e as maneiras de obter, lidar e utilizar a informação passaram a ser objeto de pesquisa visando potencializar os benefícios inerentes a este ativo (LORENS, 2007). Neste contexto, surgiu então a necessidade de manter esta informação segura, inclusive como um modo de proteger a organização. Visando solucionar esta necessidade, a segurança da informação se apresenta como uma área do conhecimento com o objetivo de atribuir à informação os princípios de confidencialidade, disponibilidade, autenticidade e integridade.

Mais recentemente, a segurança da informação tem sido vista como uma extensão da gestão de riscos. Existem duas principais normas vigentes a esse respeito: uma que trata da gestão de riscos, ABNT NBR ISO 31000:2009 e uma que se referencia a gestão de riscos, mais especificamente, aplicada à segurança da informação, ABNT NBR ISO/IEC 27005:2011.

Observando o resultado de um levantamento realizado pelo TCU em 2012 e também que as normas nas quais as referências governamentais se baseiam estão desatualizadas, percebemos uma oportunidade de melhoria das regulamentações do governo através de uma revisão sob a ótica das novas normas ABNT ISO. Nesta monografia fazemos esta comparação analisando as regulamentações governamentais e as normas da ABNT ISO, separando as diferenças entre elas e propondo uma maneira de equipará-las.

1.3 OBJETIVOS DA PESQUISA

1.3.1 Objetivo Geral

O objetivo principal desta pesquisa é a comparação das regulamentações governamentais e normas sociotécnicas vigentes referentes à gestão de riscos de segurança da informação. Esta comparação, terminológica e de processos, identifica as diferenças e ajuda no alinhamento entre os dois modelos.

1.3.2 Objetivos Específicos

a) Analisar os conceitos e os processos referentes à gestão de riscos de segurança da informação presentes nas regulamentações governamentais e normas vigentes da ABNT;

b) Identificar as diferenças, e seus possíveis aspectos negativos, entre as regulamentações do governo e as normas vigentes da ABNT;

c) Propor medidas de uniformização dos processos e harmonização dos conceitos que alinhem as regulamentações do governo e as normas vigentes da ABNT.

1.4 METODOLOGIA

O desenvolvimento da pesquisa se deu em cinco partes: levantamento e pesquisa bibliográfica exploratória, análise documental, análise terminológica com questionário, análise de processos com fluxogramas e descrição de soluções. Para a primeira parte, o método escolhido abrange pesquisa junto as seguintes fontes de informação:

a) Normas ABNT NBR ISO;

b) Instruções normativas e normas complementares;

c) Monografias, dissertações e estudos de caso;

d) Acórdão 2585/2012 do Tribunal de Contas da União.

Na segunda parte, a análise documental é feita por meio de comparações, fichamentos e tabulações que ajudam a evidenciar as diferenças buscadas no objetivo específico (b).

Com base no procedimento de harmonização de conceitos visto na ABNT NBR 13790:1997 foi elaborada uma análise terminológica com o objetivo de aproximar os glossários utilizados pela ABNT ISO GUIA 73, Instrução Normativa GSI/PR n^o 01 e Norma Complementar 04/IN01/DSIC /GSIPR. A análise terminológica estuda os conceitos apresentados, ou seja: termos e definições.

Optou-se pela aplicação de um questionário aos especialistas da área de segurança da informação para auxiliar na comparação entre os conceitos empregadas pela Administração Pública Federal e pela ABNT. Esta escolha se deu pela preocupação em manter a isonomia nas decisões pertinentes aos conceitos. O questionário foi formulado após observação de termos presentes nos objetos de estudo e que podem gerar ambiguidade ou dúvida quanto ao seu emprego. Existem certos fenômenos na língua portuguesa, relações semânticas entre as palavras, que elucidam tais ocorrências. São eles:

Polissemia - Termo que possui mais de um significado. (MORENO, 2009)

Homonímia - Termos diferentes, com origens e significados distintos, que possuem a mesma configuração fonológica e ortográfica. (MORENO, 2009)

Sinonímia - Termos diferentes que tem exatamente o mesmo significado, significado semelhante ou aproximado.

Em nossa análise terminológica apresentada no capítulo 4 são detectados dois desses fenômenos: polissemia e sinonímia.

O grau de equivalência dos conceitos também é colocado em questão e o entrevistado pode escolher entre as opções totalmente equivalentes, parcialmente equivalentes ou nada equivalentes ao responder a pesquisa. A opção "equivalentes"abrange termos que não necessariamente são os mesmos, mas cuja definição tem o mesmo significado, como ocorre por exemplo na sinonímia. Já a opção "parcialmente equivalentes"trata de conceitos cujas definições, embora distintas, buscam atingir o mesmo propósito. O significado não chega a ser o mesmo, mas a ideia por trás do conceito é similar. Por fim a opção "não equivalentes"se refere a conceitos que, utilizando o mesmo termo ou não, tem objetivos e significados distintos e a ideia por trás da definição de cada um deles é divergente. Um exemplo são os termos polissêmicos.

As fontes dos conceitos a serem julgados são citadas no enunciado do questionário, não estando presentes no momento em que são descritos nos itens. Esta medida previne a influência

da fonte na escolha do entrevistado. O questionário aplicado consta no Anexo I desta pesquisa e os resultados obtidos no Anexo II. A partir dos resultados foram criados gráficos utilizando a ferramenta Microsoft Office Excel Professional 2010.

Em termos de análise de processos, foi feita uma breve descrição de cada etapa dos processos de GRSI da ABNT NBR ISO/IEC 27005:2011 e Norma Complementar 04/IN01/DSIC/GSIPR. A partir desta descrição, utilizou-se o software Microsoft Office Visio Professional 2007 para desenhar fluxogramas das etapas. Com base nos fluxogramas e nas descrições previamente desenvolvidas, a comparação entre os processos foi feita no Capítulo 4 desta monografia.

Na última parte, com base nos resultados obtidos, são descritas sugestões para reduzir o problema apontado.

2 REVISÃO BIBLIOGRÁFICA

Para uma melhor compreensão do estudo comparativo aqui desenvolvido é necessário rever alguns conceitos básicos pertinentes à gestão de riscos de segurança da informação, bem como os órgãos responsáveis pela elaboração de normas e regulamentações que envolvem este tema.

2.1 SEGURANÇA DA INFORMAÇÃO

2.1.1 Conceito

A informação está cada vez mais sendo considerada um ativo de grande importância para empresas e instituições, pois os avanços tecnológicos das últimas décadas fizeram com que houvesse um crescimento imensurável da quantidade de informações trocadas e armazenadas bem como o aumento da importância do seu conteúdo. Tendo isto em vista a preocupação em manter estes ativos a salvo de acessos não controlados virou uma necessidade para continuidade operacional de uma empresa. O segmento segurança da informação surge deste contexto: uma área específica do estudo e proteção dos ativos de informação.

Muito mais do que uma área de estudo, o conceito de segurança de informação assumiu um significado próprio e deve ser discutido para melhor assimilação desta pesquisa. Existem na literatura especializada vários conceitos do que a segurança da informação *faz*, mas não do que ela é de fato, resultando em diversas abordagens.

Sêmola (2003) define segurança da informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. Sêmola discorre ainda sobre uma ambiguidade existente quando se utiliza a expressão "segurança da informação":

- Segurança como "meio": prática adotada para tornar um ambiente mais seguro;

- Segurança como "fim": resultado de uma prática adotada, um objetivo a ser alcançado.

Já Anderson (2003) apresenta seu próprio conceito em seu artigo *Why we need a new definition of information security*: "Um sentimento bem fundamentado da garantia de que os controles e riscos da informação estão bem equilibrados".

A ABNT (2005) trata de segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio.

Beal (2004) aborda a segurança de informação como um processo onde medidas de proteção são necessárias para manter as informações a salvo de ameaças contra sua integridade, disponibilidade e confidencialidade.

Tem-se também o foco em segurança da informação a partir de seus objetivos. Segundo Zapater e Suzuki (2003), o objetivo da SI é garantir a confidencialidade, integridade e a disponibilidade dos ativos de informação de uma corporação independente da forma ou meio em que são compartilhados ou armazenados, digital ou impresso. Pressupondo que a SI é a responsável pela identificação das diversas vulnerabilidades e pela gestão de riscos associados a estes ativos diversos.

Para continuidade da pesquisa, utilizou-se a definição que consta na norma ABNT NBR ISO/IEC 27001, que diz que segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas. (ABNT, 2006)

2.1.2 Atributos

Dentro da segurança da informação existem atributos básicos considerados essenciais para que exista proteção dos ativos de informação. Eles estão interligados, se completam e, muitas vezes, se confundem. Encontram-se na literatura do tema variações em relação à quantia de atributos: na maioria são considerados três - confidencialidade, integridade e disponibilidade. Sêmola (2003) fala destes três principais parâmetros e elucida ainda a existência da autenticidade como aspecto associado à segurança da informação. Para esta pesquisa considera-se que são quatro os atributos considerados essenciais ao falarmos de SI. São eles:

a) Confidencialidade: está associada à ideia de acesso restrito à determinada informação. Diretamente ligada à privacidade, é o princípio que garante limitação de acesso, ou seja, somente pessoas autorizadas a obter tal informação estarão aptas a fazê-lo.

b) Autenticidade: é a garantia de que a fonte da informação será inalterada, mantendo assim seu conteúdo atribuído sempre ao autor legítimo.

c) Integridade: é o princípio relacionado à prevenção do conteúdo da informação durante seu ciclo de vida. Está focado na preocupação com a gravação, alteração e/ou destruição de ativos.

d) Disponibilidade: zela pela disponibilidade dos ativos de informação quando usuários legítimos tiverem a necessidade de acessá-los.

2.2 GESTÃO DE RISCOS

2.2.1 O que é risco

A palavra "risco"é amplamente utilizada em diversos contextos, por exemplo, risco de vida, risco de incêndio, riscos de queda, risco de tempestades, entre outros. Em geral, relaciona-se o termo à ideia de "chance de algo acontecer", conceito que não está totalmente errado, no entanto, merece ser mais discutido para continuidade desta pesquisa.

Ao falar de risco no contexto de organizações, pode-se utilizar a seguinte definição: "riscos é a probabilidade de uma ameaça explorar vulnerabilidades para causar perdas ou danos a um ativo ou grupo de ativos da organização". (OLIVEIRA, 2001)

Pode-se ainda partir para o conceito de risco do sistema sociotécnico: efeito da incerteza nos objetivos. (ABNT, 2009a)

No contexto mais específico de segurança da informação, foi estabelecido que para esta pesquisa, considera-se "risco"o efeito de uma potencial ameaça aos ativos de informação.

2.2.2 O que é gestão de riscos

Vivemos todos os dias sob ameaças, probabilidades de que algo saia fora do planejado. Por exemplo, ao atravessar uma rua nos expomos a um potencial atropelamento, ou ao praticar um esporte podemos, por um esforço a mais, ganhar uma distensão. No entanto não deixamos de fazer determinadas atividades apenas por serem passivas de riscos, o que fazemos é encontrar maneiras de contorná-los, como olhar para os lados antes da travessia de uma rua, ou não exagerar ao fazer um esporte.

Em uma empresa/órgão não é diferente, sua operacionalidade está o tempo inteiro sob riscos potenciais. A gestão de riscos é então a maneira encontrada por ela para administrar estes riscos e diminuí-los.

De acordo com a definição vista em ABNT - Guia 73 - gestão de Riscos (GR) são atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. (2009)

Mas pode-se dizer mais do termo GR, pois ele engloba todo o processo e estrutura envolvidos na gerência da incerteza dos objetivos visando a melhor tomada de decisão e aproveitamento de oportunidades.

O objetivo do gerenciamento de riscos dentro de uma empresa ou órgão não é a eliminação total dos mesmos, mas sim uma melhor compreensão deles para minimizar os impactos negativos em caso de sua ocorrência.

No entanto, o processo de gestão de riscos assume algumas variações dependendo do grupo de interesse onde ele será implementado: financeiro, político, social, saúde, etc. Nesta pesquisa

o grupo de interesse é o de segurança da informação e dentro deste enfoque o conceito de gestão de riscos é:

> Conjunto de processos que permite às organizações identificar e implementar as medidas de proteção necessárias para diminuir os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos. (BEAL, 2004)

A existência de um processo de GR voltado especificamente para segurança da informação é um grande importância dentro de uma empresa/órgão pois existem complexidades e desafios intrínsecos à área que necessitam de um tratamento especial.

2.2.3 Componentes da gestão de riscos

Para ser possível melhor entendimento da gestão de riscos, é preciso estabelecer alguns termos importantes porém confusos entre si. Tem-se pela ABNT (2009a) quatro principais conceitos relacionados à gestão de riscos:

a) Estrutura da gestão de riscos: conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento análise crítica e melhoria contínua da gestão de riscos através de toda a organização.

b) Política de gestão de riscos: declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos.

c) Plano de gestão de riscos: esquema dentro da estrutura de gestão de riscos que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos.

d) Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

A partir das definições pode-se estabelecer sucintamente uma relação entre elas da seguinte maneira: a estrutura da gestão de riscos possui um conjunto de componentes, dentre eles a política e o plano de GR. A política entra como fundamento e o plano como arranjo organizacional. Além disto, existe o processo de GR em si, que é a aplicação sistemática da estrutura.

2.2.4 Gestão de riscos de segurança da informação: um processo

Um processo é um conjunto de atividades ou tarefas executados de acordo com regras, procedimentos ou funções organizacionais para transformar as entradas do processo nas saídas desejadas (VIANA, 2010). Com base neste conceito, pode-se discutir a gestão de riscos de segurança da informação (GRSI) como um processo.

Sabe-se ainda que todo processo precisa de uma documentação para formalizar a descrição de suas entradas, saídas, atividades intermediárias, ferramentas e técnicas. O processo de GRSI foi formalizado e está disponível na Norma ABNT NBR ISO/IEC 27005:2011.

A Figura 2.1 nos mostra o esquema do processo de GRSI segundo a ABNT que estabelece o uso desta estrutura em qualquer organização como um todo. Observa-se ainda o caráter contínuo e iterativo do processo, justificada pela minimização de tempo e esforço na identificação dos riscos de alto impacto.

O processo de GRSI definido na Fig. 2.1 pode ser descrito da seguinte maneira: é feito um estabelecimento de contexto onde são definidas as premissas dos riscos. Após isto, é colocado em ação o processo de avaliação de riscos dividido em identificação, análise e avaliação dos riscos. Neste ponto é feita uma reflexão a respeito das informações obtidas: se elas são satisfatórias para o tratamento eficaz do risco, segue-se para o a fase de tratamento do risco; caso contrário uma nova definição de contexto é feita e o processo de avaliação de riscos é retomado.

A fase de tratamento do risco estabelece uma maneira eficaz de reduzir o risco a um valor aceitável. Nela ainda avalia-se o tratamento selecionado: satisfatório ou não perante o nível de risco residual aceito pela empresa. Se satisfatório, segue-se para a próxima etapa; se não satisfatório pode-se revisar o tratamento selecionado ou voltar para o começo do processo na fase de definição do contexto.

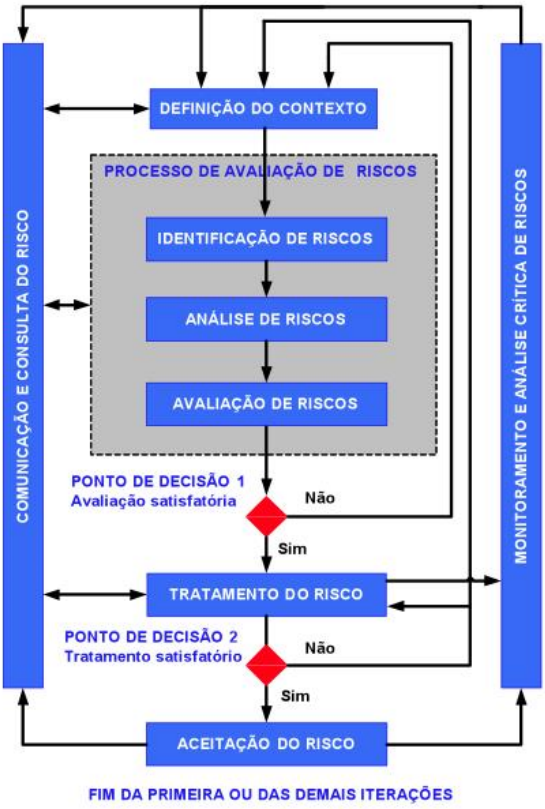

Figura 2.1: Processo de gestão de riscos de segurança da informação (ABNT, 2011)

A última fase do processo é a aceitação do risco onde os riscos residuais são aceitos e incorporados ao sistema de gestão de segurança da informação (SGSI) da empresa.

O SGSI de uma empresa é a parte do sistema de gestão da mesma responsável pela implementação da gestão de riscos de segurança da informação. Segundo ele é possível separar o processo de GRSI em fases como demonstra a Tabela 2.1.

Tabela 2.1: O processo de gestão de riscos de segurança da informação em fases segundo o processo do SGSI. (ABNT, 2011)

Processo do SGSI	**Processo de gestão de riscos de segurança da informação**
Planejar	Definição do contexto, processo de avaliação de riscos, definição do plano de tratamento de riscos e aceitação do risco
Executar	Implementação do plano de tratamento de risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de riscos de segurança da Informação

Como todo processo, o de GRSI possui formalização. Diz-se que ele tem como entrada todas as informações necessárias para definição de contexto da GRSI; como atividades intermediárias as ações de estabelecimento de contextos externo e interno e as diretrizes de implementação onde o propósito da GRSI é definido; e como saída a especificação dos critérios básicos, escopo e limites da GRSI e a definição dos responsáveis pelo andamento da implementação do processo.

2.3 A ADMINISTRAÇÃO PÚBLICA FEDERAL

2.3.1 Responsabilidade

O termo Administração Pública Federal (APF), ou simplesmente Administração Pública, é definido e organizado na Constituição Federal de 1988, Título III, em um capítulo específico. A Constituição detalha mais o termo no artigo 37 onde define que a APF direta e indireta de qualquer do Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedeça aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Além da classificação como direta e indireta, a Administração Pública Federal pode ser dividida em objetiva e subjetiva. De Moraes (2001) nos ajuda a defini-las como:

- Administração Pública Federal Objetiva: diz respeito à atividade administrativa imediata do Estado. Constitui dos serviços integrados na estrutura administrativa da Presidência da República e dos Ministérios.

- Administração Pública Federal Subjetiva: é o conjunto de órgãos e de pessoas jurídicas aos quais a lei atribui o exercício da função administrativa do Estado e compreende as seguintes entidades: autarquias, empresas públicas, sociedades de economia mista, fundações públicas e entidades dotadas de personalidade jurídica.

O aspecto subjetivo é o que será interessante para este estudo pois o termo APF aqui fará alusão, principalmente, aos órgãos públicos de qualquer Poder da República e em qualquer esfera federativa que possuam responsabilidade administrativa.

2.3.2 Gabinete de Segurança Institucional da Presidência da República e a gestão de riscos de segurança da informação

A preocupação com a questão da segurança tem sido uma constante no governo federal. Em 1930, durante o governo do Presidente Getúlio Vargas foi criado o Estado-Maior do Governo Provisório, órgão responsável pela segurança. Ao longo das décadas este órgão passou por diversas transformações, até que em 08 de maio de 2006 o Governo Federal aprovou através do Decreto n^o 5772 a Estrutura Regimental do Gabinete de Segurança Institucional da Presidência da República - GSIPR. Dentro da estrutura do GSIPR, criou o Departamento de Segurança da Informação e Comunicações - DSIC. Este decreto foi revogado por outro, o Decreto n^o 7411, de 29 de dezembro de 2010:

> O Gabinete de Segurança Institucional é um órgão essencial da Presidência da República e tem como área de competência os seguintes assuntos:
> - assistência direta e imediata ao Presidente da República no desempenho de suas atribuições;
> - prevenção da ocorrência e articulação de gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional;
> - assessoramento pessoal ao Presidente da República em assuntos militares e de segurança;
> - coordenação das atividades de inteligência federal e de segurança da informação;
> - segurança pessoal do Chefe de Estado, do Vice-Presidente da República e dos respectivos familiares, dos titulares dos órgãos essenciais da Presidência da República e de outras autoridades ou personalidades quando determinado pelo Presidente da República, assegurado o exercício do poder de polícia; e
> - segurança dos palácios presidenciais e das residências do Presidente da República e do Vice-Presidente da República, assegurado o poder de polícia. (BRASIL, 2010)

Assim, o GSIPR tem como atribuições a assistência direta e imediata ao Presidente da República, prevenção e articulação de gerenciamento de crises, assessoramento pessoal ao Presidente

da República em assuntos militares e de segurança, coordenação de atividades de inteligência e de segurança da informação e, finalmente, a segurança pessoal de autoridades, familiares e personalidades quando determinado pelo Presidente da República.

O Decreto n^o 7411 ainda determina uma estrutura organizacional para o GSIPR, definindo como órgãos de assistência direta e imediata ao Ministro de Estado o Gabinete e a Secretaria Executiva. Abaixo da Secretaria Executiva está o Departamento de Segurança da Informação e Comunicações. O DSIC é o departamento ao qual estão relacionadas as questões de segurança da informação e comunicações.

Segundo a Instrução Normativa GSI/PR n^o 01 de 13 de junho de 2008, compete ao Departamento de Segurança da Informação e Comunicações:

> I - planejar e coordenar as atividades de segurança da informação e comunicações na Administração Pública Federal, direta e indireta;
> II - estabelecer as normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta;
> III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal, direta e indireta, denominado CTIR.GOV;
> IV - elaborar e implementar programas destinados à conscientização e à capacitação dos recursos humanos em segurança da informação e comunicações;
> V - orientar a condução da Política de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;
> VI - propor programa orçamentário específico para as ações de segurança da informação e comunicações. (BRASIL, 2008a)

Portanto, o DSIC tem como função o planejamento e a coordenação das atividades de segurança da informação e comunicações na APF, estabelecimento de normas para implementação da gestão de segurança da informação e comunicações pelos órgãos e entidades da APF, operacionalização e manutenção de centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da APF, elaboração e implementação de programas à conscientização e capacitação dos recursos humanos em segurança da informação e comunicações e orientação da condução da política de segurança da informação e comunicações na APF.

Todas as orientações elaboradas pelo DSIC estão na forma de instrução normativa e normas complementares. Para melhor compreendermos o que são estas orientações precisamos primeiro entender o que é uma instrução normativa. Muitas vezes um órgão administrativo necessita interpretar as leis vigentes, criando atos administrativos. Assim, a Instrução Normativa é expedida no sentido de interpretar a lei, sendo hierarquicamente inferior à Constituição Federal, às leis complementares e ordinárias e aos decretos presidenciais. A Instrução Normativa, portanto, não

é uma lei, mas "ato regulamentador de autoridade pública"(BRASIL, 2012b, p. 109), que não pode ampliar ou inovar os termos da legislação.

A gestão de riscos de segurança da informação é abordada na Norma Complementar 04/DSIC/GSIPR de 14 de agosto de 2009 - Gestão de Riscos de Segurança da Informação e Comunicações, que estabelece as diretrizes gerais do processo de gestão de riscos de segurança da informação e comunicações nos órgãos da Administração Pública Federal, direta e indireta.

O processo de gestão de riscos de segurança da informação e comunicações - GRSIC deve considerar a estrutura do órgão ou entidade da APF, bem como seus objetivos, processos e requisitos legais. Este processo está embasado no modelo denominado PDCA (Plan-Do-Check-Act) e ilustrado na Fig. 2.2:

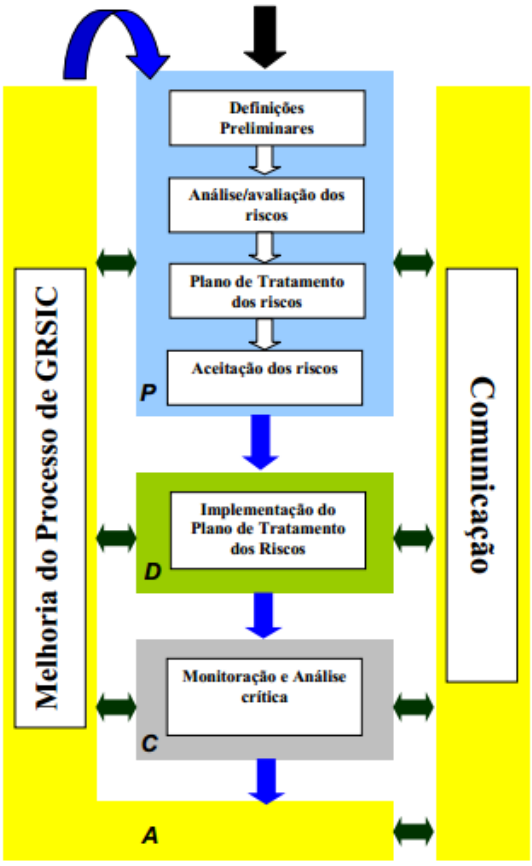

Figura 2.2: Processo de gestão de riscos de segurança da informação e comunicações. (BRASIL, 2013)

O processo explicitado na Fig. 2.2 está dividido em quatro etapas: planejamento, execução, verificação e ação. Na fase de planejamento, deve-se fazer uma análise da organização visando estruturar o processo de GRSIC, definir um escopo de aplicação para este processo. Em seguida, é preciso identificar os riscos, avalia-los de acordo com os critérios de prioridade estabelecidos

pelo órgão ou entidade e posteriormente determinar as formas de tratamento destes riscos. Por fim, verifica-se o resultado do processo executado, aceitando os riscos ou submetendo-os à nova avaliação. Na etapa de execução, aplica-se as ações de segurança da informação e comunicações que constam no plano de tratamento de riscos. Verifica-se a eficácia do processo através de monitoração e análise crítica e caso o resultado seja insatisfatório devem ser feitas melhorias de GRSIC. É essencial que todas as partes envolvidas e interessadas compartilhem informações sobre todas as fases.

Este processo se assemelha com o descrito no tópico 2.2.4 deste trabalho - Gestão de riscos de segurança da informação: um processo. Veremos com mais detalhes nos capítulos seguintes as diferenças entre eles e as consequências destas diferenças.

2.3.3 Situação atual da gestão de riscos de segurança da informação na Administração Pública Federal

Em 2007, o Tribunal de Contas da União realizou um levantamento com o intuito de acompanhar a situação de governança de tecnologia da informação (TI) na Administração Pública Federal, resultando no Acórdão 1.603/2008-TCU-Plenário. Esta avaliação continuou sendo feita nos anos posteriores e em 2012 foram divulgados no Acórdão 2585/2012 os resultados do terceiro levantamento, que contou com a participação de 350 instituições da APF.

No que se refere à segurança da informação, a figura 2.3 ilustra a situação atual nos órgãos da APF, mostrando os dados dos anos de 2010 e 2012. Para esta questão foram utilizadas como critérios principais a Instrução Normativa n^o 1/2008 do GSIPR, a ABNT NBR ISO/IEC 27002:2005 (gestão de segurança da informação) e a NBR ISO/IEC 27005 (gestão de riscos da segurança da informação) (BRASIL, 2012a)

Baseando-se na Fig 2.3, nota-se uma situação intermediária com relação ao gerenciamento de segurança da informação e política de segurança da informação: 51% dos órgãos que participaram do levantamento possuem equipe designada para gerenciar a segurança da informação e 45% tem uma política de segurança da informação. Destaca-se também o baixo nível de maturidade da gestão de riscos na APF, uma vez que somente 24% dos órgãos pesquisados mantém inventário dos ativos de informação e 17% possuem processo de classificação das informações. No entanto, o fator mais preocupante é que 90% das instituições não realizam análise de riscos.

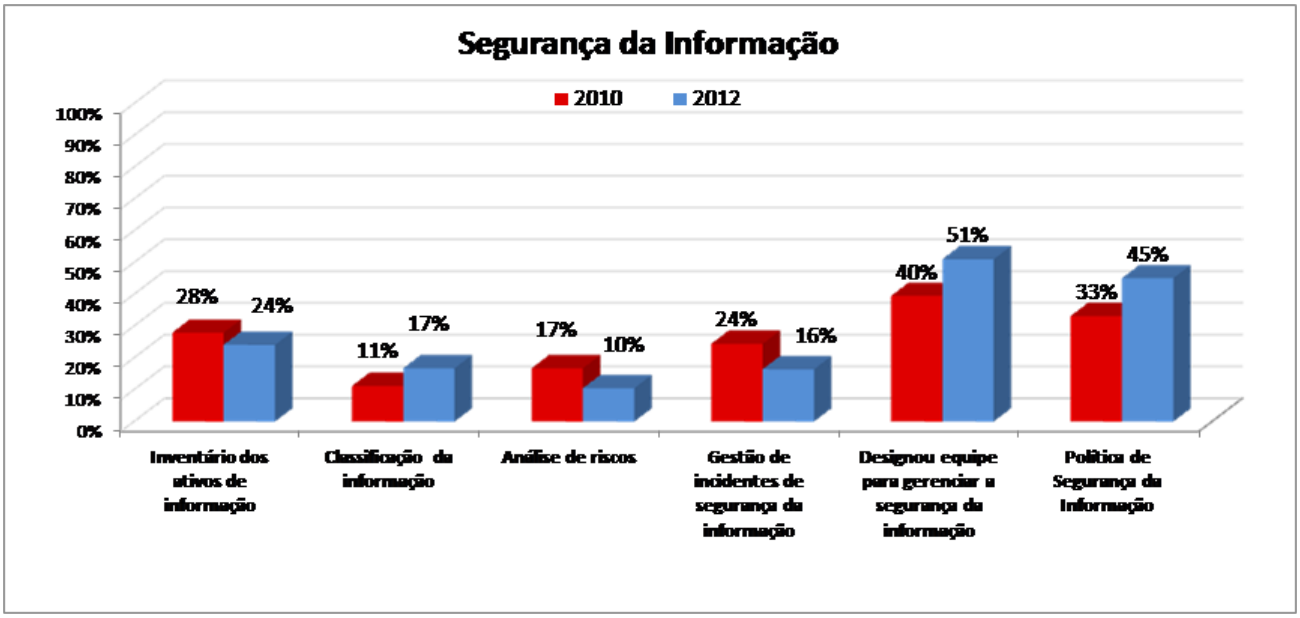

Figura 2.3: Ações relacionadas à segurança da informação na Administração Pública Federal. (BRASIL, 2012a)

2.4 SISTEMA SOCIOTÉCNICO DA GESTÃO DE RISCOS

2.4.1 Responsabilidade

Um sistema sociotécnico é, segundo Somerville (2007), um ou mais sistemas técnicos que incluem pessoas como partes inerentes do sistema e inclui também conhecimento de como o sistema deve ser usado. É dito ainda que seu comportamento está ligado diretamente com o fator humano, onde a maneira que as pessoas interpretam os objetivos organizacionais a serem alcançados influencia no apoio a estes objetivos. Sua finalidade é o auxílio na conquista de determinada meta organizacional.

O sistema sociotécnico da gestão de riscos no Brasil é estabelecido pela Associação Brasileira de Normas Técnicas (ABNT), organismo responsável pela elaboração e oficialização de normas e diretrizes. A ABNT é o fórum nacional de normalização reconhecido pelo Estado Brasileiro.

Uma norma é um documento elaborado por um organismo reconhecido que contém as principais diretrizes, regras, sistematizações e orientações de determinadas atividades. O objetivo de ter uma norma traçada para determinado setor é possibilitar um maior grau de organização dentro do mesmo, visando obter uma melhora de resultados. Uma NBR, Norma Brasileira, é uma norma elaborada pela ABNT que tem o poder de validá-la em todo o território nacional. A ABNT tem também o poder de cancelar uma NBR sempre que esta for substituída, considerada obsoleta ou outras razões apontadas. O processo de cancelamento, no entanto, é submetido à consulta pública para avaliar se há aceitação ou não da ação.

O processo de elaboração de uma norma é iniciado quando, a partir da identificação de demanda de algum setor ou organismo regulamentador, a ABNT direciona a um comitê técnico do determinado setor a responsabilidade de trabalhar a ideia de um projeto de norma. Este comitê irá inserir em seu plano de normalização setorial (PNS) da comissão de estudos responsável o pedido da nova norma. Se uma comissão de estudos especifica para o assunto não existir, é criada uma comissão de estudo especial (ABNT/CEE) encarregada do caso.

A partir daí os membros da comissão, formada por representantes dos setores envolvidos, desenvolvem o texto inicial da norma e encaminham para consulta pública em forma de projeto de norma. A consulta pública fica disponível no sítio da ABNT e qualquer pessoa ou entidade pode enviar sugestões ou comentários relacionados ao projeto apresentado. Após este período, a ABNT irá avaliar a pertinência das opiniões coletadas e as acatará ou não.

A seguir da consulta pública e reformulação do texto inicial, o projeto de norma vira NBR e é colocada em acervo na ABNT, entrando em vigor depois de 30 dias de sua aprovação.

Sabe-se que anualmente a ABNT divulga publicamente em sua página na internet um plano nacional de normalização contendo os títulos que serão desenvolvidos durante o ano. É uma maneira de mostrar à sociedade o que será trabalhado e despertar interesse de participação nas elaborações.

2.4.2 As normas da gestão de riscos

Considerando a importância da segurança da informação para as organizações, a ISO/IEC publicou a família de normas 27000 com o objetivo de criar um código de boas práticas de segurança da informação no qual as organizações pudessem se basear. O escopo deste trabalho inclui três normas desta família: ABNT NBR ISO/IEC 27001:2006, ABNT NBR ISO/IEC 27002:2005 e a ABNT NBR ISO/IEC 27005:2011. A norma ABNT NBR ISO/IEC 27005:2011 trata especificamente da gestão de riscos de segurança da informação, principal objeto de estudo deste trabalho. Sobre o processo de gestão de riscos, será utilizado o vocabulário ABNT ISO GUIA 73:2009.

A ABNT NBR ISO/IEC 27001:2006 - Sistemas de gestão de segurança da informação - Requisitos - especifica os requisitos para o estabelecimento de um SGSI em uma organização. Um SGSI é definido como *"a parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação."*(ABNT, 2006)

Compreende-se então que o SGSI é um processo contínuo que passa por constantes melhorias para ajustá-lo aos requisitos de segurança e expectativas das partes interessadas. Para estruturar este processo, a norma adota o modelo PDCA (Plan-Do-Check-Act).

A ABNT NBR ISO/IEC 27002:2005 descreve um código de prática para a gestão de segurança da informação em uma organização baseada nas melhores práticas de segurança da informação.

Esta norma estabelece diretrizes gerais para uma gestão de segurança da informação: não diz como fazer, mas sim o quê deve ser feito. (ABNT, 2005)

As duas normas mencionadas acima compõem a base sociotécnica da Instrução Normativa GSI/PR n^o 01 e suas Normas Complementares no que diz respeito à segurança da informação.

Da necessidade de normatizar o processo de gerenciamento de riscos surgiu a ABNT NBR ISO 31000: 2009 - Gestão de Riscos - Princípios e diretrizes. Esta norma é um guia para princípios, diretrizes e implementação de gestão de riscos e tem como função agir como um ponto em comum para as diferentes implementações de gerência de riscos nos mais diversos tipos de organização (ABNT, 2009b). Seu vocabulário básico é o ABNT ISO GUIA 73:2009. O Guia 73 - Gestão de riscos - Vocabulário contém os conceitos básicos de gestão de riscos a serem empregados nas diversas normas que abordam o assunto.

Por fim, a ABNT NBR ISO/IEC 27005:2011 - Gestão de Riscos de Segurança da Informação define as melhores práticas em GRSI e fornece diretrizes para o processo de gestão de riscos de segurança da informação em uma organização, atendendo aos requisitos de um SGSI. Seu objetivo é facilitar a implementação da segurança da informação tendo como base a GR. A norma, que está em sua segunda edição, emprega conceitos, modelos e processos globais especificados na norma ABNT NBR ISO/IEC 27001:2006 e está alinhada com a ABNT NBR ISO 31000:2009.

3 LEGISLAÇÃO E NORMAS SOCIOTÉCNICAS VIGENTES

As normas sociotécnicas e as regulamentações governamentais possuem grande complexidade e são os objetos de estudo dessa pesquisa. Este capítulo tem por função a descrição e o detalhamento de cada uma destas normas e regulamentações.

3.1 ESCOPO DE REGULAMENTAÇÕES E NORMAS SOCIOTÉCNICAS VIGENTES

Foram selecionadas para análise neste trabalho normas vigentes do sistema sociotécnico e regulamentações governamentais para a APF relacionadas à gestão de risco de segurança da informação. A Tabela 3.1 ilustra o assunto geral de cada norma e regulamentação e a área de aplicação de cada uma. São elas: ABNT ISO GUIA 73:2009, ABNT NBR ISO/IEC 27005:2011, Instrução Normativa GSI/PR n^o 01, Norma Complementar 02/IN01/DSIC/GSIPR e Norma Complementar 04/IN01/DSIC/GSIPR. Foram consideradas as publicações feitas até o dia 11 de junho de 2013. A norma ABNT NBR ISO/IEC 31000:2009 não foi considerada um objeto de estudo uma vez que a ABNT 27005 já adota seu processo de gestão de riscos, adequando-o ao contexto de segurança da informação.

Todos os conceitos apresentados neste capítulo constam no Anexo III deste trabalho.

3.1.1 Regulamentações

A Instrução Normativa GSI/PR n^o 01 trata das orientações gerais para gestão de segurança da informação e comunicações a serem empregadas nos órgãos e entidades da Administração Pública Federal, direta e indireta. A IN01 fornece inicialmente conceitos e definições para o melhor entendimento da segurança da informação e comunicações e define também as funções, competências e âmbitos de atuação do comitê gestor de segurança da informação e do Gabinete de Segurança Institucional da Presidência da República.

i) Definições:

- Política de segurança da informação e comunicações;
- Segurança da informação e comunicações;
- Disponibilidade;

- Integridade;
- Confidencialidade;
- Autenticidade;
- Gestão de segurança da informação e comunicações;
- Quebra de segurança; e
- Tratamento da informação (BRASIL, 2008a).

Tabela 3.1: Normas e regulamentações analisadas

Título	**Norma ou Regulamentação**	**Assunto Geral**	**Gestão de Riscos**	**Segurança da Informação**
ABNT NBR ISO/IEC 27005:2011	Norma	Tecnologia da informação - Técnicas de segurança - GRSI	X	X
ABNT ISO GUIA 73:2009	Norma	Gestão de Riscos - Vocabulário	X	
IN GSIPR No 1	Regulamentação	Disciplina a GSIC na APF, direta e indireta, e dá outras providências		X
NC 02/DSIC/GSIPR	Regulamentação	Metodologia de GSIC		X
NC 04/DSIC/GSIPR	Regulamentação	Diretrizes para o processo de GRSIC nos órgãos e entidades da APF	X	X

ii) Atribuições:

Estão explicitadas nesta Instrução Normativa as atribuições para cada um dos seguintes elementos: Gabinete de Segurança Institucional da Presidência da República através do DSIC, comitê gestor de segurança da informação, comitê de segurança da informação e comunicações e gestor de segurança da informação e comunicações.

As orientações mais específicas e detalhadas dos variados itens que compõem a GSIC são feitas em Normas Complementares, que funcionam como adendos à IN 01. Existem dezoito Normas Complementares relacionadas à IN 01, das quais duas serão analisadas nesta pesquisa:

Norma Complementar 02: Metodologia de Gestão de Segurança da Informação e Comunicações

i) Sobre a metodologia da gestão de segurança da informação e comunicações:

A Norma Complementar 02 apresenta uma metodologia de gestão de segurança da informação e comunicações composta de 4 passos: planejar, fazer, checar e agir. A esta metodologia é dado o nome de PDCA, um processo de melhoria contínua referenciado pela norma ABNT NBR ISO/IEC 27001:2006. A regulamentação define as ações que devem ser feitas em cada uma das etapas:

Planejar - Definição de escopo e limites, definição de objetivos, definição de abordagem de Gestão de Riscos, identificação dos riscos, análise dos riscos, identificação de opções de tratamento de riscos, seleção de ações de SIC necessárias para o tratamento de riscos e obtenção da aprovação de autoridade decisória do órgão ou entidade; (BRASIL, 2008b)

Fazer - Formulação de plano de metas, obtenção da autorização para implementar plano de metas, implantação do plano de metas, definição de medida de eficácia das ações de SIC, implantação de programas de conscientização e treinamento, gerenciamento das ações de Segurança da Informação e Comunicações, gerenciamento de recursos e implementação de procedimentos de detecção e resposta a incidentes; (BRASIL, 2008b)

Checar - Execução de procedimentos de avaliação e análise crítica, realização de análises críticas regulares, verificação de requisitos e diretrizes, atualização da avaliação e análise de riscos, condução de auditoria interna das ações de SIC, atualização dos planos de SIC, registro e comunicação de possíveis impactos na eficácia da missão da entidade ou órgão; (BRASIL, 2008b)

Agir - Proposta de melhorias, execução de ações preventivas ou corretivas, comunicação das melhorias e verificação dos objetivos. (BRASIL, 2008b)

Norma Complementar 04: Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)

i) Definições:

- Ameaça;
- Análise de riscos;
- Análise/Avaliação de riscos;
- Ativos de informação;
- Avaliação de riscos;
- Comunicação do risco;
- Estimativa de riscos;
- Evitar risco;
- GRSIC;
- Identificação de riscos;
- Reduzir risco;
- Reter risco;

- Riscos de SIC;
- Transferir risco;
- Tratamento dos riscos; e
- Vulnerabilidade (BRASIL, 2013).

ii) Sobre os Procedimentos do Processo de GRSIC:

Define-se um processo sistemático de GRSIC, composto por etapas, visando manter os riscos em um limiar aceitável. São 8 as etapas estabelecidas e detalhadas: definições preliminares; análise/avaliação dos riscos; plano de tratamento dos riscos; aceitação dos riscos; implementação do plano de tratamento dos riscos; monitoração e análise crítica; melhoria do processo de GRSIC; e comunicação do risco (BRASIL, 2013).

3.1.2 Normas Sociotécnicas Vigentes

O ABNT ISO GUIA 73:2009 apresenta-se no sistema sociotécnico como o vocabulário regente de gestão de riscos. Mais especificamente voltada para a gestão de riscos de segurança da informação, existe a Norma ABNT NBR ISO/IEC 27005:2011. Serão justamente estes dois documentos os analisados do ponto de vista normativo nesta pesquisa.

ABNT ISO GUIA 73:2009 : Gestão de Riscos - Vocabulário

i) Definições:

O fornecimento de todo o vocabulário básico para entendimento comum de conceitos da gestão de riscos é de responsabilidade desta norma. Nela são definidos desde termos simples como "risco"até definições mais complexas como "auditoria de gestão de riscos".

ii) Estrutura da Norma:

A apresentação dos termos é feita em 3 tópicos: termos relativos ao risco; termos relativos à gestão de riscos; e termos relativos ao processo de gestão de riscos (ABNT, 2009a). Os conceitos do ABNT Guia 73 podem ser encontrados no Anexo III desta pesquisa.

ABNT NBR ISO/IEC 27005:2011: Tecnologia da informação - Técnicas de segurança - Gestão de Riscos de Segurança da Informação (GRSI)

i) Definições:

- Consequência;
- Controle;
- Evento;
- Contexto externo;
- Contexto interno;
- Nível de risco;
- Probabilidade (Likelihood);

- Riscos residual;
- Risco;
- Análise de riscos;
- Processo de avaliação de riscos;
- Comunicação e consulta;
- Critérios de risco;
- Avaliação de riscos;
- Identificação de riscos;
- Gestão de riscos;
- Tratamento de riscos; e
- Parte interessada (ABNT, 2011).

É importante frisar que os conceitos presentes na ABNT 27005 foram retirados do Guia 73.

ii) Estrutura:

O processo de GRSI é definido e detalhado em seis etapas nesta norma: definição do contexto; processo de avaliação de riscos; tratamento do risco; aceitação do risco; comunicação e consulta do risco; e monitoramento e análise crítica de riscos (ABNT, 2011). As fases bem como as diretrizes de cada um dos 6 tópicos definidos são descritas mais especificamente no decorrer da norma.

iii) Anexos:

Para auxiliar no cumprimento do processo de GRSI descrito na norma, os sete anexos nela presentes tem caráter informativo sobre as etapas e detalhes que podem gerar dúvidas ou ambiguidades em suas implementações. São eles:

- Anexo A: Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação;
- Anexo B: Identificação e valoração dos ativos e avaliação do impacto;
- Anexo C: Exemplos de ameaças comuns;
- Anexo D: Vulnerabilidades e métodos de avaliação de vulnerabilidades;
- Anexo E: Abordagens para o processo de avaliação de riscos de segurança da informação;
- Anexo F: Restrições para a modificação do risco;
- Anexo G: Diferenças nas definições entre a ABNT NBR ISO/IEC 27005:2008 e a ABNT NBR ISO/IEC 27005:2011.

4 ANÁLISE COMPARATIVA

Este capítulo discorre sobre a comparação entre normas e regulamentações referentes à gestão de riscos de segurança da informação. A análise é feita em dois níveis: terminológico e de processos. A partir dos resultados aqui obtidos, pode-se compreender melhor as diferenças entre conjunto de regulamentações governamentais e o sistema sociotécnico.

4.1 ANÁLISE TERMINOLÓGICA

Considerando os conceitos apresentados nos objetos de pesquisa detalhados no Capítulo 3, concluiu-se que há uma disparidade terminológica entre as normas e as regulamentações. Segundo a ABNT, "as diferenças entre sistemas de conceitos paralelos, por um lado, e as pseudo-semelhanças dos termos, por outro, prejudicam a comunicação internacional"(1997). Desta forma é indicado que em casos de sistemas de conceitos da mesma área de interesse, os glossários sejam alinhados. A harmonização dos conceitos - termos e definições - é vista como a "atividade de redução ou eliminação de pequenas diferenças entre dois ou mais conceitos muito similares"(ABNT, 1997).

A análise terminológica desenvolvida neste capítulo, trata dos conceitos apresentados nas normas e regulamentações. Observando os termos e definições aqui relembrados, verificou-se a existência de três grupos:

- Conceitos presentes nas normas e regulamentações.
- Conceitos presentes somente nas normas; e
- Conceitos presentes somente nas regulamentações;

As tabelas 4.1, 4.2 e 4.3 e ilustram a divisão dos termos que compõem estes conceitos. Os termos constantes na Tab. 4.1 foram considerados presentes em ambas por apresentarem possível equivalência.

Tabela 4.1: Relação de termos presentes nas normas e nas regulamentações

ABNT Guia 73	**NC 04**
Risco	Risco de Segurança da Informação e Comunicações
Comunicação e Consulta	Comunicação do Risco
Gestão de Riscos	Gestão de Riscos de Segurança da Informação e Comunicações
Vulnerabilidade	Vulnerabilidade
Avaliação de Riscos	Avaliação de Riscos
Compartilhamento de Riscos	Transferir Risco
Tratamento de Riscos	Tratamento de Riscos
Ação de Evitar o Risco	Evitar Risco
Retenção de Riscos	Reter Risco
Análise de Riscos	Análise de Riscos
Identificação de Riscos	Identificação de Riscos

Tabela 4.2: Relação de termos presentes somente nas regulamentações

IN 01	Segurança da Informação e Comunicações Disponibilidade Integridade Confidencialidade Autenticidade Gestão de SIC Quebra de Segurança Tratamento de Informação
NC 04	Ameaça Análise/Avaliação de riscos Ativos de Informação Estimativa de riscos Reduzir Riscos

A tabela 4.1 foi utilizada como base para a elaboração do questionário previsto na metodologia (Capítulo 1). Ele serve um duplo propósito: verificar o grau de equivalência dos conceitos dúbios e sua adequação ao contexto de GRSI. O conteúdo do questionário aplicado pode ser encontrado no Anexo I desta pesquisa e as respostas dos entrevistados no Anexo II.

Tabela 4.3: Relação de termos presentes somente nas normas da ABNT

27005	Parte Interessada Contexto Externo Contexto Interno Critérios de Riscos Evento Probabilidade (likelihood) Nível de Risco Consequência Risco Residual
Guia 73	Percepção do Risco Estabelecimento do Contexto Descrição dos Riscos Fonte de Riscos Probabilidade Exposição Frequência Matriz de Risco Atitude Perante o Risco Apetite pelo Risco Tolerância ao Risco Aversão ao Risco Agregação de Risco Aceitação do Risco Financiamento de Riscos Resiliência Monitoramento Análise Crítica Reporte de Riscos Registro de Riscos Perfil de Risco Auditoria de Gestão de Riscos

4.1.1 Resultados do questionário

O questionário foi submetido a 14 (quatorze) especialistas da área de segurança da informação, que classificaram o grau de equivalência entre os 11 pares de conceitos apresentados na

Tab. 4.1 e escolheram dentre estes os mais adequados ao contexto de GRSI. O grupo de entrevistados contou com membros de diversos setores: sete deles trabalham na área de segurança da informação da esfera governamental (4 no Tribunal de Contas da União e 3 no Senado Federal), outros dois trabalham na iniciativa privada, em uma empresa provedora de soluções integradas de Tecnologia da Informação e Comunicação (NEC Corporation) e os cinco especialistas restantes fazem parte da esfera acadêmica (1 professor e 4 alunos de mestrado, todos da Universidade de Brasília).

No âmbito do grau de conformidade entre os conceitos listados, a maioria destes (64% ou 7 ao total) foram considerados parcialmente equivalentes. 36% dos termos e definições usados no questionário foram apontados como equivalentes e não houve nenhum par que tenha sido classificado como não equivalente. Como esperado, ocorreram casos de polissemia - com termos que possuem mais de um significado e por isso foram considerados parcialmente equivalentes ou não equivalentes. Houve também casos de sinonímia - quando os termos eram considerados equivalentes. Estes resultados estão ilustrados no gráfico da Figura 4.1:

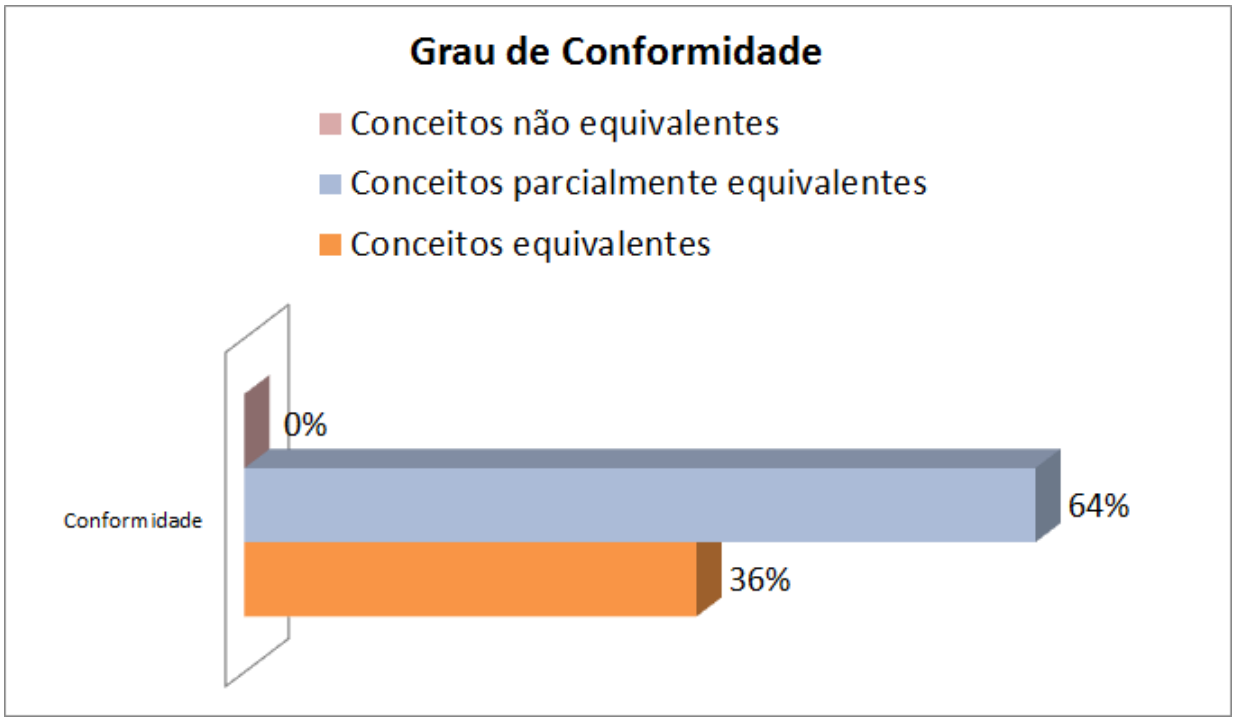

Figura 4.1: Grau de equivalência entre os conceitos abordados no questionário

Com relação à adequação ao contexto de gestão de riscos de segurança da informação, o resultado indica o nível elevado de contextualização no sistema sociotécnico: das onze comparações sugeridas, em 73% delas (8 ao total) o conceito da norma foi preferível ao da regulamentação. A Fig. 4.2 detalha os resultados obtidos:

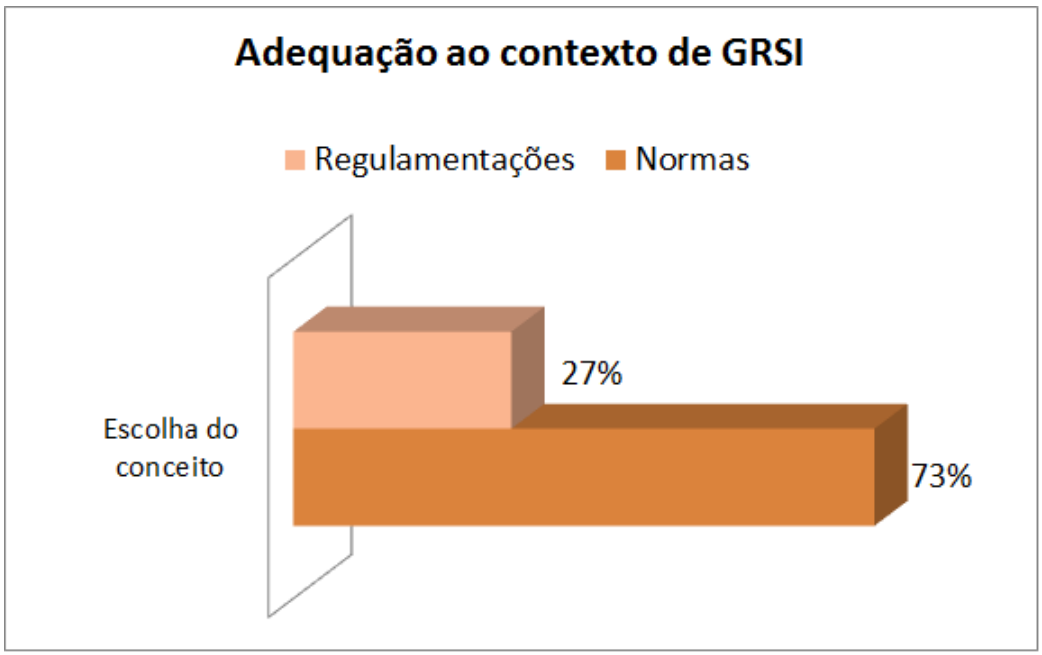

Figura 4.2: Adequação dos conceitos apresentados no questionário ao contexto de GRSI

Retomando cada um dos 11 pares de conceitos norma/regulamentação temos na Tab. 4.4 o nível de harmonização dos conceitos e a escolha dos entrevistados.

Os resultados aqui expostos confirmam a hipótese inicial desta pesquisa de que os conceitos propostos pelas normas e regulamentações referentes à GRSI são diferentes entre si e que é necessário o alinhamento terminológico. Isso fica evidenciado de duas formas: pela existência de conceitos que só existem nas normas ou nas regulamentações e pelo nível de equivalência entre os que são vistos como similares em uma análise inicial. Um aspecto positivo revelado pelos dados coletados é que dentre os pares de conceitos nenhum se apresentou como não equivalente. As regulamentações governamentais e o sistema sociotécnico não estão completamente afastados: a maioria dos conceitos foram considerados parcialmente equivalentes. Entretanto, o resultado mostra que a situação ainda não é ideal e que é possível buscar a harmonização dos conceitos.

No contexto de gestão de riscos de segurança da informação, houve uma predileção pelas normas da ABNT por parte dos especialistas de segurança da informação, embora em alguns conceitos a opção tenha sido pelas regulamentações governamentais. Busca-se neste trabalho um equilíbrio entre o que é proposto pelo governo e pelo sistema sociotécnico, de forma que os conceitos presentes nestes estejam adequados da melhor forma à GRSI.

As sugestões para a uniformização dos termos e definições aqui analisados é um dos temas abordados no Capítulo 5.

Tabela 4.4: Resultados do questionário para os pares de conceito norma/regulamentação

ABNT Guia 73	**NC 04**	**Grau de conformidade**	**Conceito escolhido pelos entrevistados no questionário**
Risco	Risco de Segurança da Informação e Comunicações	Parcialmente equivalentes	Regulamentação
Comunicação e Consulta	Comunicação do Risco	Parcialmente equivalentes	Norma
Gestão de Riscos	Gestão de Riscos de Segurança da Informação e Comunicações	Parcialmente equivalentes	Regulamentação
Vulnerabilidade	Vulnerabilidade	Equivalentes	Norma
Avaliação de Riscos	Avaliação de Riscos	Parcialmente equivalentes	Norma
Compartilhamento de Riscos	Transferir Risco	Parcialmente equivalentes	Norma
Tratamento de Riscos	Tratamento de Riscos	Parcialmente equivalentes	Norma
Ação de Evitar o Risco	Evitar Risco	Equivalentes	Regulamentação
Retenção de Riscos	Reter Risco	Parcialmente equivalentes	Norma
Análise de Riscos	Análise de Riscos	Equivalentes	Norma
Identificação de Riscos	Identificação de Riscos	Equivalentes	Norma

4.2 ANÁLISE DOS PROCESSOS

Como visto no capítulo anterior, as normas da ABNT e as regulamentações do governo propõem um processo de GRSI cada. Os processos apresentados são convergentes em alguns pontos, mas possuem diferenças significativas em outros que impactam diretamente em sua implantação. A convergência deve-se em grande parte ao fato dos dois processos utilizarem como metodologia base o ciclo PDCA. Este ciclo, descrito inicialmente na ABNT NBR ISO/IEC 27001:2006 - Sistemas de gestão de segurança da informação - Requisitos e ilustrado na Fig. 4.3 foi adaptado ao processo de gestão de riscos de segurança da informação nas respectivas normas e regulamentações.

No entanto, por mais que a metodologia de implantação derive de uma mesma base de gerenciamento dos processos, os sub-processos descritos em cada uma das etapas (planejar, executar, checar e agir) apresentam divergências e muitas vezes se confundem. A maioria destas divergências ocorre porque o processo de GRSI da NC 04 firma todos os seus sub-processos em alguma etapa do PDCA, mantendo o formato deste fixo. Já na ABNT 27005 o PDCA foi utilizado como base para integrar todo o processo.

A figura 4.4 ilustra os processos de GRSI da NC 04 e da norma ABNT 27005 com intuito de auxiliar na comparação dos mesmos. Este é o principal objetivo desta seção.

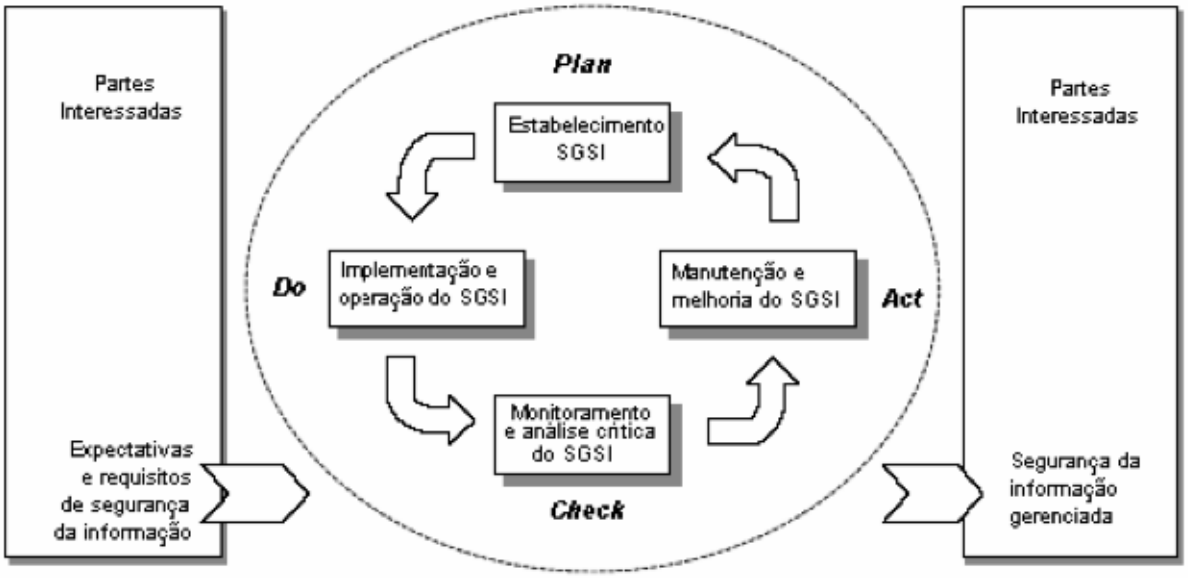

Figura 4.3: Modelo PDCA para um Sistema de Gestão de Segurança da Informação (SGSI) (ABNT, 2006)

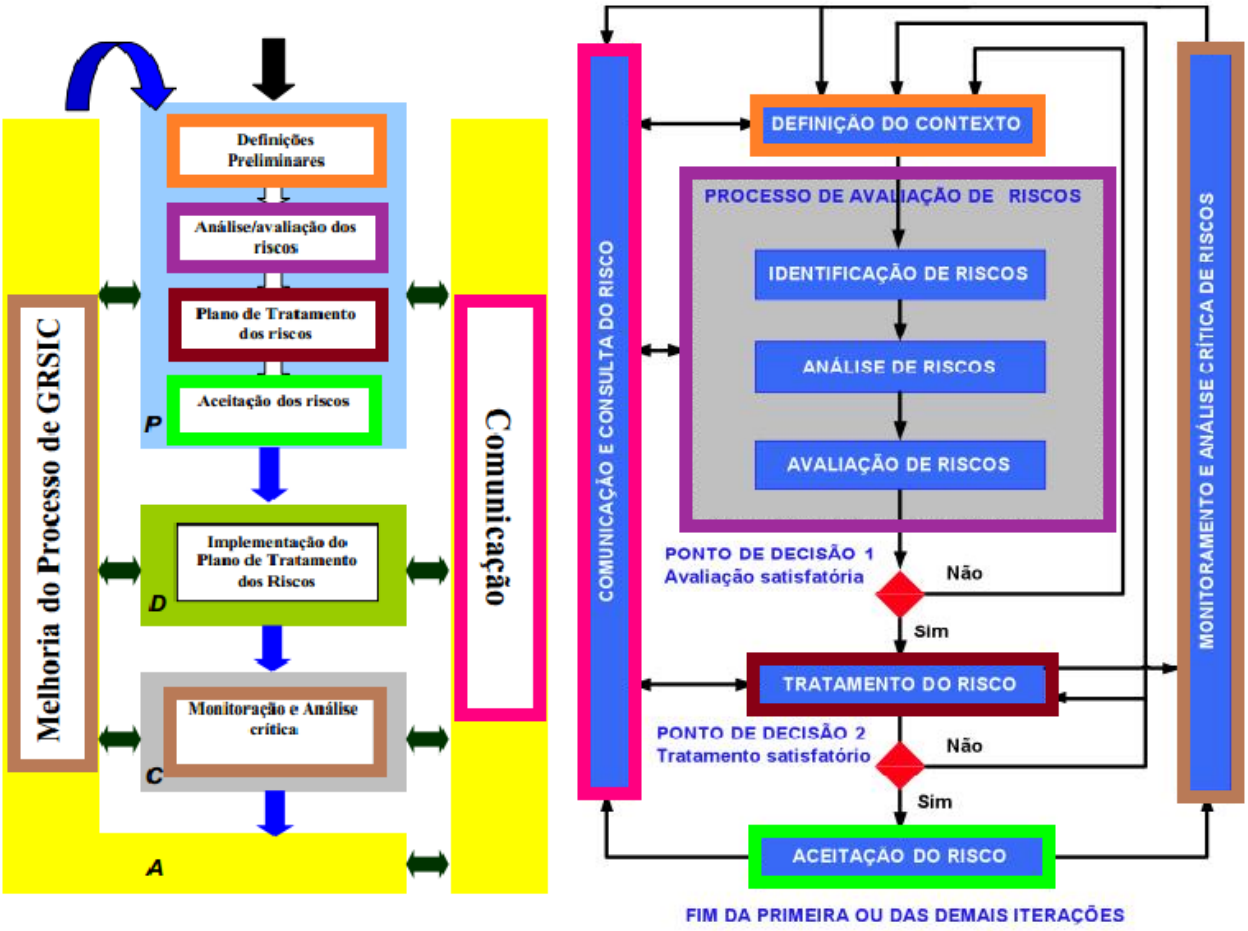

Figura 4.4: Processos de gestão de riscos - Norma Complementar 04 e ABNT NBR ISO/IEC 27005

Na figura 4.4, o processo a esquerda representa a regulamentação NC 04 e o da direita a norma ABNT 27005. Etapas destacadas com a mesma cor são consideradas equivalentes. Etapas que não foram destacadas não possuem equivalência no outro modelo. Desta forma, temos as seguintes associações:

a) Laranja - Definições preliminares e definição do contexto;
b) Roxo - Análise/avaliação de riscos e processo de avaliação de risco (identificação, análise e avaliação de riscos);
c) Vinho - Plano de tratamento dos riscos e tratamento do risco;
d) Verde - Aceitação dos riscos e aceitação do risco;
e) Marrom - Monitoração e análise crítica, melhoria do processo de GRSIC e monitoramento e análise cítica;
f) Rosa - Comunicação e comunicação e consulta.

A etapa de implementação do plano de tratamento de riscos não possui equivalente na ABNT 27005 e os pontos de decisão desta não constam na NC 04.

4.2.1 Detalhamento dos processos da NC 04 e da ABNT 27005

A seguir são mostradas as diferenças entre cada uma das etapas mencionadas anteriormente. A análise é dividida em três partes: descrição do conteúdo da Norma Complementar 04, descrição do conteúdo da ABNT NBR ISO/IEC 27005 e comparação.Para ilustrar com mais riqueza as etapas descritas foram desenhados fluxogramas. Os fluxogramas não são o objetivo desta seção e servem apenas para facilitar a visualização das diferenças encontradas.

a) Definições preliminares / Definição do contexto

NC 04 - Esta regulamentação sugere uma análise da organização, onde inicialmente deve ser definido o escopo de atuação do processo de GRSI. A partir dele, deve-se adotar uma metodologia que também seja compatível com os objetivos e as diretrizes gerais. A metodologia em questão precisa contemplar, no mínimo, os critérios de avaliação e aceitação do risco. A Fig. 4.5 ilustra o fluxograma desta etapa:

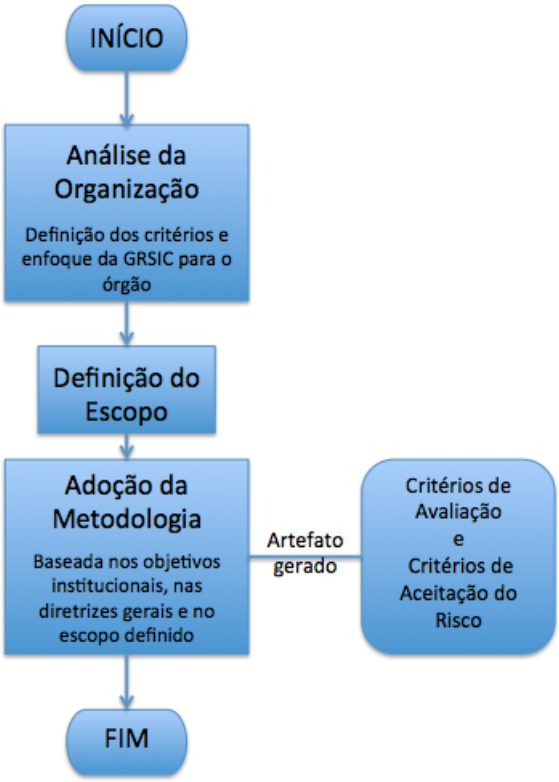

Figura 4.5: Fluxograma das definições preliminares na NC 04

ABNT 27005 - A norma determina a importância de se determinar o propósito da GRSI para que seu escopo e seus objetivos possam ser bem definidos. Uma vez especificados, eles servem de base para a definição de contexto em si. Esta definição deverá se firmar sobre critérios de avaliação de riscos, critérios de impacto e critérios de aceitação de risco. O desenvolvimento de cada um destes é orientado em detalhes pela norma e, além disso, seu Anexo A contem maiores

informações sobre a definição do escopo e limites do processo de GRSI. Por fim, a norma ainda trata da organização e responsabilidades para o processo. A Fig. 4.6 detalha esta etapa:

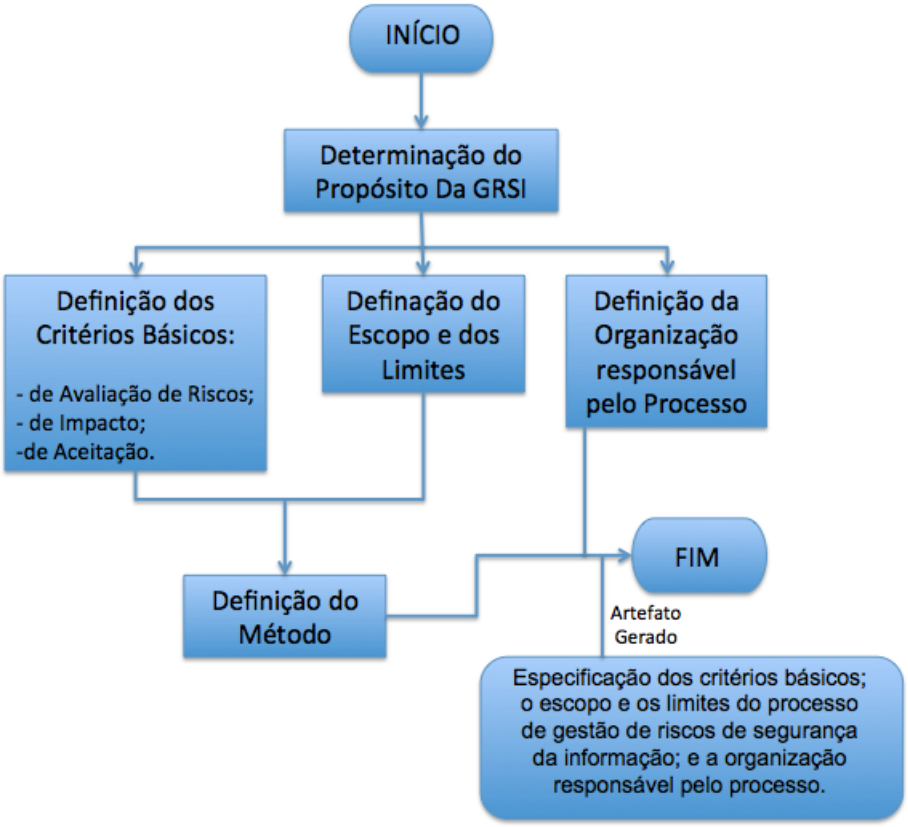

Figura 4.6: Fluxograma da definição do contexto na ABNT 27005

Comparação - Embora a norma e a regulamentação partam do mesmo princípio de análise da organização e desenvolvimento de uma metodologia, a ABNT NBR ISO/IEC 27005 vai mais além, com maior riqueza em detalhes que auxiliam na definição do contexto. Na regulamentação os passos necessários para a definição do contexto são apenas citados, sem jamais explicitar a forma com a qual devem ser conduzidos. A falta de uma orientação sobre a elaboração dos critérios de avaliação e aceitação do risco na NC 04 talvez seja a maior lacuna nesta primeira etapa.

b) Análise/avaliação de riscos / Processo de avaliação de risco (identificação, análise e avaliação de riscos)

NC 04 - A etapa de análise/avaliação de riscos é apresentada em três passos: identificação dos riscos, estimativa dos riscos levantados e avaliação de riscos. A identificação dos riscos é em relação ao escopo definido e possui duas partes: identificação dos ativos e seus responsáveis, detalhada na Norma Complementar n^o 10, e identificação de riscos. A estimativa dos riscos deve considerar níveis para a probabilidade e para a consequência do risco associados aos atributos de SI, sendo uma das entradas do passo avaliação de riscos. Neste passo, a estimativa é comparada

com os critérios estabelecidos nas definições preliminares, definindo se os riscos são aceitos ou requerem tratamento. A saída dessa etapa é uma relação dos riscos que requerem tratamento, priorizados de acordo com os critérios estabelecidos pelo órgão ou entidade. A Fig. 4.7 ilustra o fluxograma desta etapa:

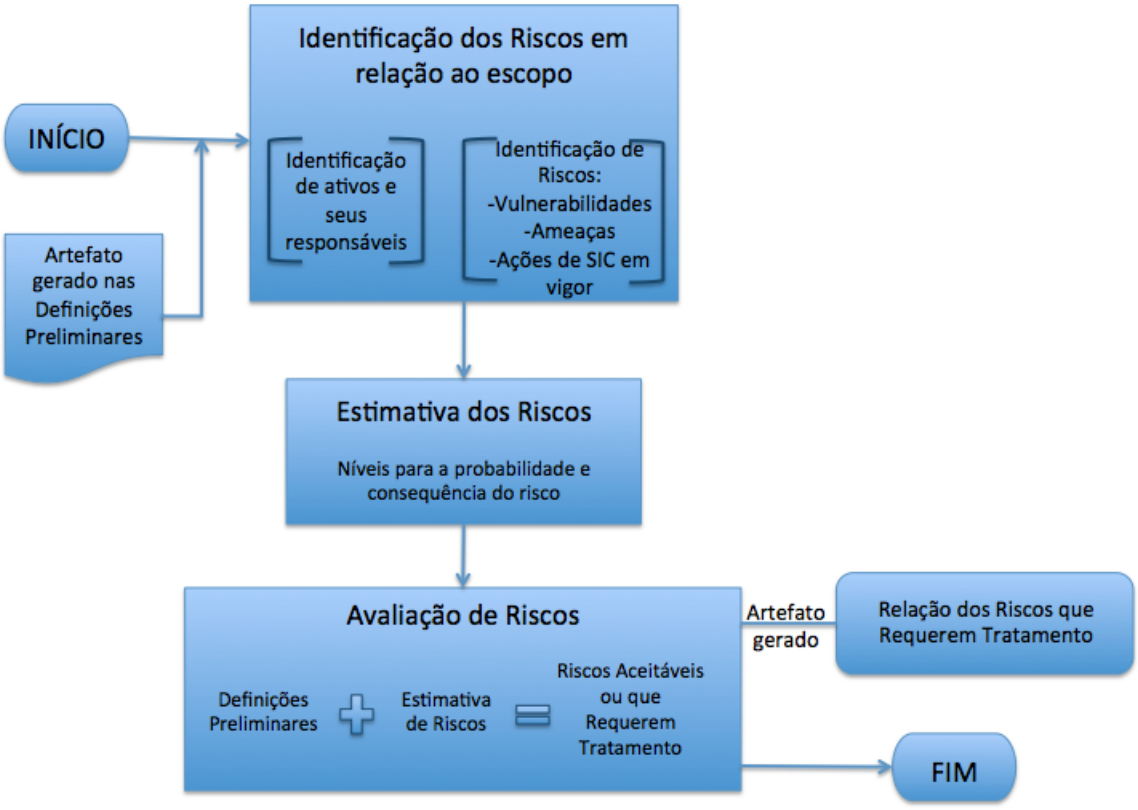

Figura 4.7: Fluxograma da Análise/Avaliação de Riscos na NC 04

ABNT 27005 - Na norma, a avaliação de risco é considerada um processo composto pelas etapas de identificação, análise e avaliação de riscos. A primeira etapa ainda se subdivide em outras cinco: identificação de ativos, das ameaças, dos controles existentes, das vulnerabilidades e das consequências. Com relação à análise de riscos, são descritas metodologias distintas (análise qualitativa e quantitativa) e dadas diretrizes para a implementação da avaliação das consequências, da avaliação da probabilidade dos incidentes e da análise de nível de risco. Finalmente, na última etapa o nível dos riscos obtido na análise de riscos é comparado com os critérios de avaliação e aceitação do risco, resultando em uma lista de riscos avaliados, ordenados por prioridade de acordo com os critérios de avaliação de risco. Além da descrição de cada uma dessas etapas, a norma contém os anexos que auxiliam na implementação de suas recomendações: o anexo B discute sobre a identificação e valoração dos ativos e a avaliação do impacto, o anexo C dá exemplos de ameaças típicas, o anexo D trata de vulnerabilidades e métodos para análise de vulnerabilidades e o anexo E apresenta exemplos de abordagens para o processo de avaliação de

riscos de segurança da informação. A Fig. 4.8 detalha esta etapa:

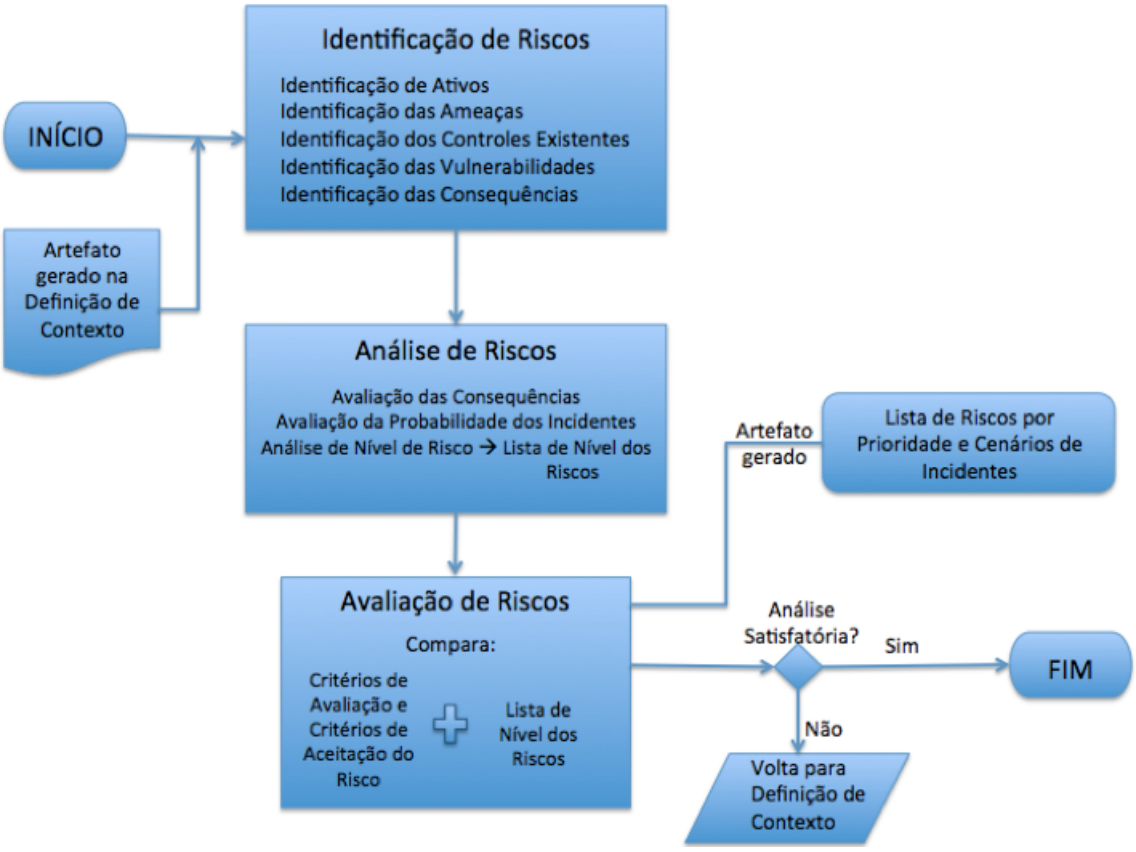

Figura 4.8: Fluxograma do processo de avaliação de riscos na ABNT 27005

Comparação - A primeira grande diferença é que enquanto a norma ABNT NBR ISO/IEC 27005 trata do processo de avaliação de riscos, considerando suas componentes como etapas distintas do processo de GRSI, a NC 04 considera a análise/avaliação de riscos uma única etapa, em que as componentes se tornam apenas passos. Ademais, a regulamentação mais uma vez se mostra incompleta, utilizando termos como "probabilidade"e "consequência do risco"sem tê-los definidos, referenciando os critérios previamente estabelecidos sem sequer orientar sua elaboração na etapa anterior. Novamente, os passos são apresentados superficialmente, sem orientação para sua implementação, orientação que é abundante na norma. Por fim, os anexos na ABNT 27005 são outro fator destoante, tornando-a mais completa e fácil de implementar.

c) Plano de tratamento dos riscos / tratamento do risco

NC 04 - A terceira etapa do processo de GRSIC aborda as formas de tratamento dos riscos. As opções são: reduzir, evitar, transferir ou reter o risco. Convém que a adoção das opções observe aspectos como a eficácia das ações de SIC já existentes, restrições organizacionais, técnicas e estruturais, requisitos legais e análise custo/benefício. A saída desta etapa é um plano de tratamento de riscos contendo as ações de SIC, os responsáveis, prioridades e prazos de execução. A Fig. 4.9 ilustra o fluxograma desta etapa:

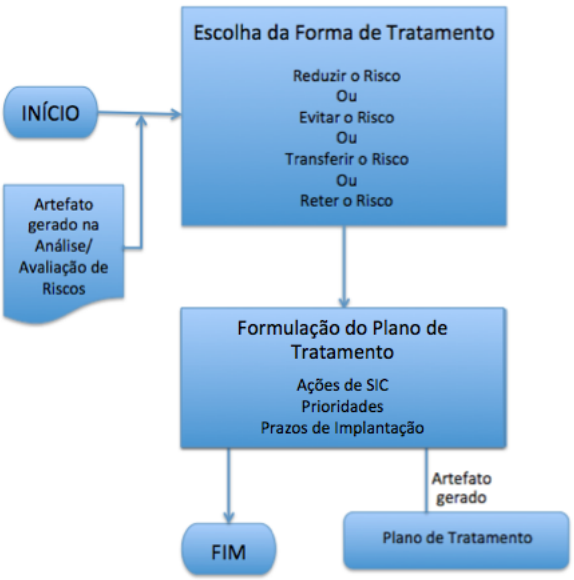

Figura 4.9: Fluxograma do plano de tratamento dos riscos na NC 04

ABNT 27005 - O tratamento do risco pode ser feito de diferentes maneiras. Pode-se modificar, reter, evitar e/ou compartilhar o risco. A seleção deve se basear no resultado do processo de avaliação de riscos, na relação custo/benefício, na percepção dos riscos pelas partes afetadas e nos diferentes tipos de restrições, que são detalhados no Anexo F da norma. A saída desta etapa é o plano de tratamento do risco e os riscos residuais, que devem ser submetidos à decisão de aceitação por parte dos gestores da organização. A Fig. 4.10 detalha esta etapa:

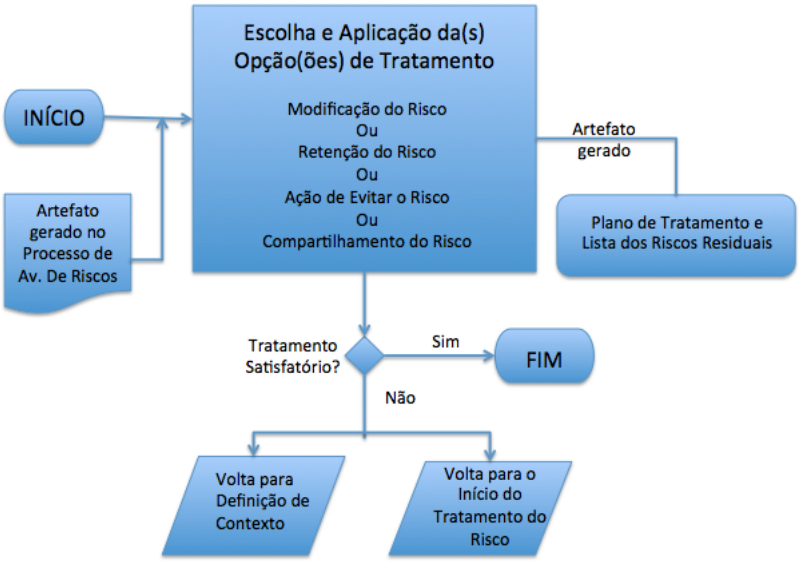

Figura 4.10: Fluxograma do tratamento do risco na ABNT 27005

Comparação - Os objetivos das etapas de tratamento de riscos são semelhantes. No entanto,

as opções de tratamento apresentadas na regulamentação e na norma são distintas. A redução do risco, proposta na NC 04 não possui equivalente na ABNT 27005, bem como a modificação do risco na norma não possui contrapartida na regulamentação. Os pares compartilhamento de riscos/transferir riscos e retenção de riscos/reter riscos foram apontados como parcialmente equivalentes pelos especialistas de segurança da informação e as opções apresentadas pelas normas foram consideradas as mais adequadas à gestão de riscos de segurança da informação. Já o par "ação de evitar risco"/evitar risco foi analisado como equivalente e se deu preferência pela opção descrita pela NC 04. Outro aspecto a ser ressaltado é a questão do risco residual, que não é tratada pela NC 04.

d) Aceitação dos riscos / aceitação do risco

NC 04 - Na aceitação dos riscos, deve-se verificar os resultados obtidos do processo executado, considerando o plano de tratamento. Os riscos podem ser aceitos ou submetidos à nova avaliação. A Fig. 4.11 ilustra o fluxograma desta etapa:

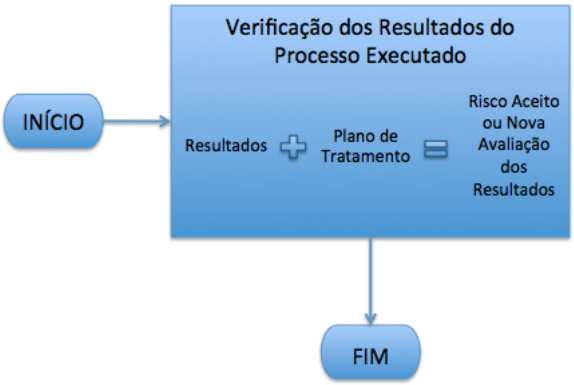

Figura 4.11: Fluxograma da aceitação dos riscos na NC 04

ABNT 27005 - A aceitação do risco tem como entrada o plano de tratamento de riscos e o processo de avaliação do risco residual. A decisão de aceitar os riscos deve levar em conta os critérios de aceitação estabelecidos na definição do contexto e prever a aceitação de riscos baseada em argumentos válidos, mesmo que o nível do risco residual não satisfaça os critérios. A saída dessa etapa é uma lista de riscos aceitos, com justificativa para aqueles que não satisfazem os critérios normais de aceitação do risco. A Fig. 4.12 detalha esta etapa:

Comparação - É notável a ausência de detalhes sobre o conteúdo desta etapa na regulamentação. Nem a determinação do artefato de entrada nem a especificação dos resultados a serem analisados pelo plano de tratamento são especificados. A falta do conceito "risco residual"também é percebida aqui, onde sua aceitação seria possível se justificada. A decisão entre "risco aceito"ou "nova avaliação dos resultados"é feita com atraso, pois a mesma está presente subjetivamente no ponto de decisão ao final da etapa "processo de avaliação de riscos"da ABNT 27005.

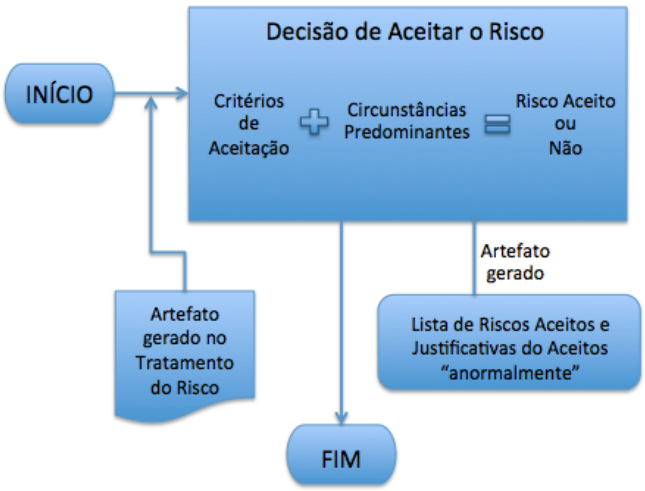

Figura 4.12: Fluxograma da aceitação do risco na ABNT 27005

e) Monitoração e análise crítica, melhoria do processo de GRSIC / monitoramento e análise crítica

NC 04 - Aqui, a monitoração e análise crítica e a melhoria do processo de GRSIC são consideradas etapas distintas. A monitoração e análise são feitas em dois níveis: risco e processo. Já as possíveis melhorias identificadas nesta etapa devem ser propostas à autoridade decisória durante a melhoria do processo de GRSIC e se aprovadas, são executadas. Deve-se verificar se os objetivos das melhorias foram atingidos. A Fig. 4.13 ilustra o fluxograma desta etapa:

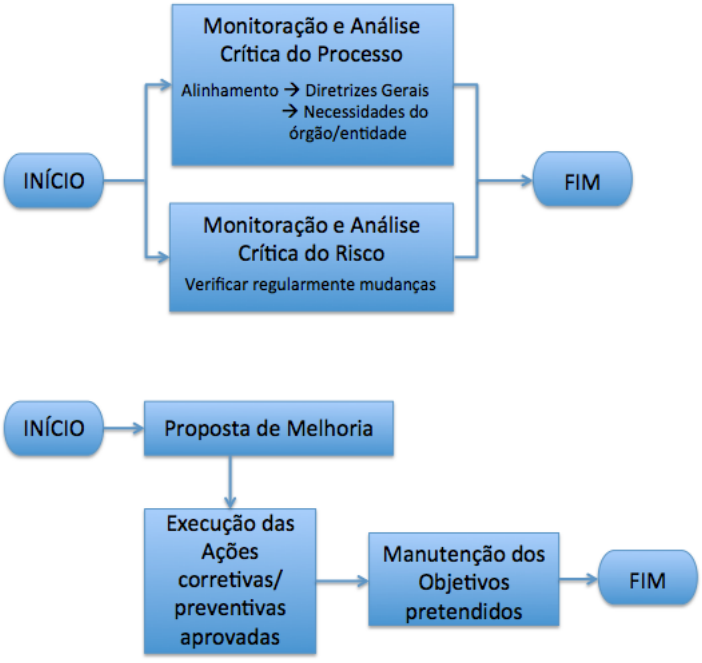

Figura 4.13: Fluxogramas da monitoração e análise crítica e da melhoria do processo de GRSIC na NC 04

ABNT 27005 - Na etapa de monitoramento e análise crítica, os riscos e o processo são revistos, verificados, monitorados e analisados e caso seja detectada a necessidade de melhorias, estas são implementadas. O objetivo desta etapa é a garantia do alinhamento e da relevância do processo de SIC em relação aos objetivos da organização e aos critérios para a aceitação do risco. A Fig. 4.14 detalha esta etapa:

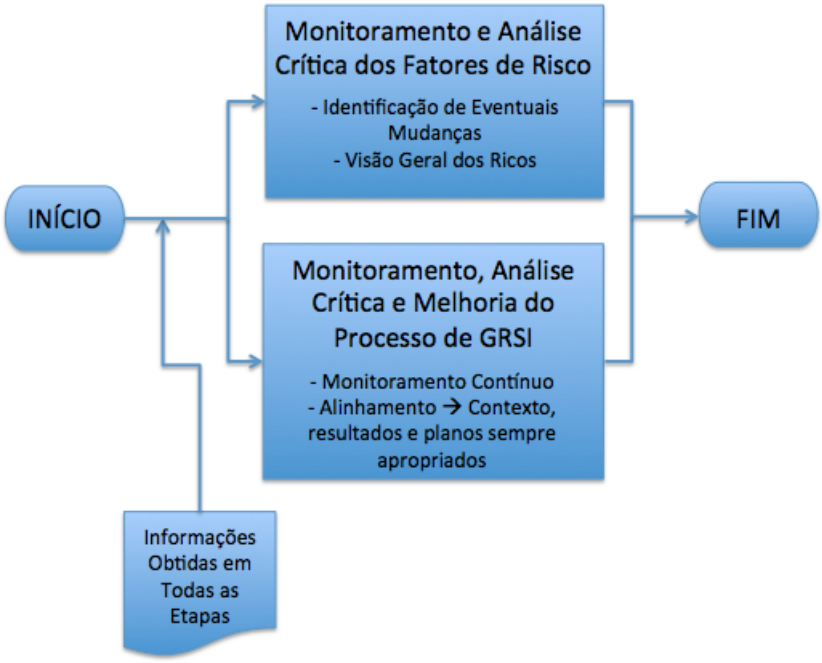

Figura 4.14: Fluxograma do monitoramento e análise crítica na ABNT 27005

Comparação - A finalidade das etapas descritas anteriormente é semelhante. Destaca-se como principal ponto de divergência a separação feita pela NC 04 entre monitoramento e análise crítica e melhoria do processo de GRSIC. A norma aborda estas etapas como uma só e com um maior grau de detalhamento.

f) Comunicação / Comunicação e consulta do risco

NC 04 - A etapa de comunicação do risco objetiva manter as instâncias superiores informadas sobre todas as etapas da gestão de risco e compartilhar as informações entre o tomador da decisão e as partes envolvidas e interessadas. A Fig. 4.15 ilustra o fluxograma desta etapa.

ABNT 27005 - Pretende-se com a comunicação e consulta obter um consenso sobre o gerenciamento dos riscos, a partir da troca e/ou partilha das informações sobre o risco entre os tomadores de decisão e outras partes interessadas. A Fig. 4.16 detalha esta etapa.

Comparação - Os dois processos são quase equivalentes. A única diferença ressaltada é o compartilhamento de informação ocorrer também entre tomador de decisão e partes envolvidas, e não somente com as partes interessadas, na ABNT 27005. Mais uma vez, a norma apresenta maior detalhamento, mas a ausência deste na NC 04 não dificulta sua implementação.

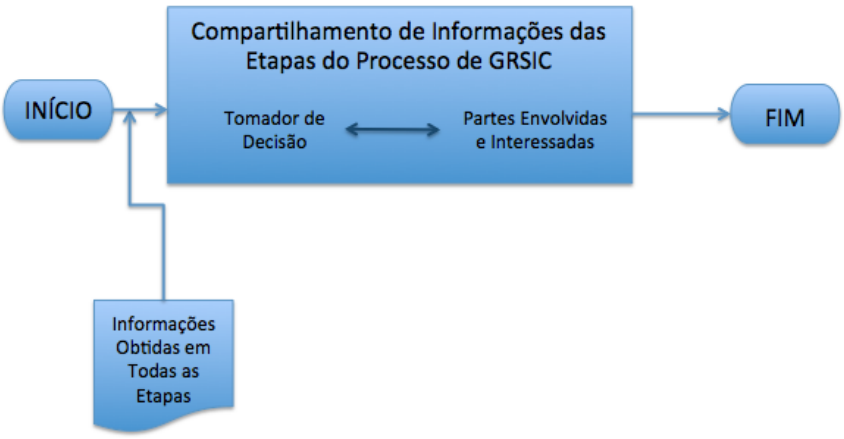

Figura 4.15: Fluxogramas da comunicação do risco na NC 04

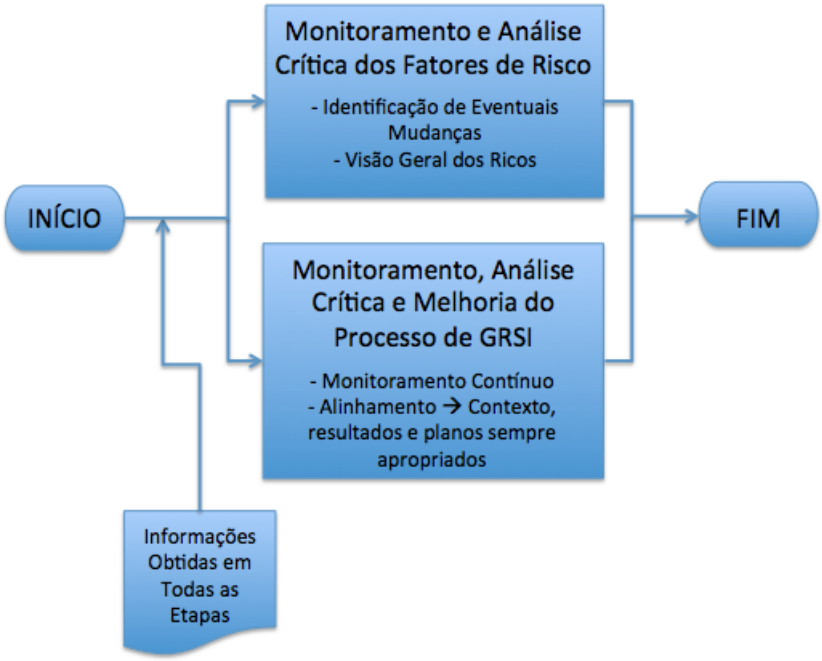

Figura 4.16: Fluxograma da comunicação e consulta do risco na ABNT 27005

Finalizada a diferenciação entre as etapas equivalentes, resta analisar os aspectos que não possuem correspondência. O primeiro deles é a etapa "implementação do plano de tratamento de riscos", visto na NC 04. Essa etapa trata da execução do plano de tratamento de riscos criado em etapas anteriores, e não consta na ABNT 27005. A colocação dessa etapa causa certa estranheza, pois o plano de tratamento pode ser implementado apenas parcialmente ou nem chegar a ser executado. A implementação de riscos no processo de GRSI acontece de maneira subentendida no decorrer das etapas.

É necessário também observar os dois pontos de decisão presentes no processo da norma ABNT 27005, um ao final do processo de avaliação de riscos e outro ao final do tratamento do

risco. Em ambos será feita uma decisão a respeito do nível de satisfação dos produtos destas etapas, definindo a continuidade do processo de GRSI. Estes pontos de decisão não são encontrados na NC 04, nela existe apenas um momento em que se discute uma possível decisão. Na aceitação de riscos diz-se que uma decisão deve ser tomada em relação *"aos resultados do processo executado"* (BRASIL, 2013), no entanto não fica claro a quais resultados e a qual processo ela se refere.

Comparados os processos de GRSI, fica evidenciada a falta de alinhamento entre regulamentação e norma, tanto no âmbito terminológico quanto no dos processos. O capítulo 5 a seguir apresenta propostas de recomendações que visam diminuir ou resolver as diferenças aqui encontradas.

5 SUGESTÕES PARA ALINHAMENTO

Este capítulo dispõe sobre as sugestões elaboradas com base nos problemas de uniformização encontrados no capítulo anterior.

5.1 SUGESTÕES TERMINOLÓGICAS

Com base na análise comparativa terminológica desenvolvida no Capítulo 4 é possível propor um conjunto de sugestões que visam reduzir o abismo existente entre a estrutura terminológica do sistema sociotécnico e das regulamentações do governo. A diferenciação entre os termos e definições empregados nos dois processos de GRSI são essencialmente causadas por dois fatores: conceitos que existem em apenas um dos processos e conceitos que estão presentes em ambos, mas que geram dúvida quanto ao seu emprego.

Levando em conta os conceitos que estão presentes em apenas um dos processos, é preciso lembrar que o Guia 73, vocabulário de gestão de riscos da ABNT, contém uma gama de termos e definições gerais para gestão de riscos que não necessariamente se enquadram quando aplicados ao contexto de segurança da informação. Consequentemente, muitos destes termos sequer são usados na ABNT 27005. Uma vez que nosso interesse é no alinhamento da gestão de riscos de segurança da informação, podemos nos focar nos termos presentes na ABNT 27005, retirados da Guia 73, que não são definidos nas regulamentações governamentais. Para uma melhor visualização a Tab. 5.1 retoma estes termos:

Tabela 5.1: Relação de termos presentes somente na ABNT 27005

ABNT 27005	Parte Interessada
	Contexto Externo
	Contexto Interno
	Critérios de Riscos
	Evento
	Probabilidade (likelihood)
	Nível de Risco
	Consequência
	Risco Residual

Os termos mostrados anteriormente são usados ao longo da ABNT 27005 e, portanto, integram o processo de GRSI. Alguns deles inclusive são vistos nas regulamentações para a APF.

Deste modo, sugere-se a inclusão dos conceitos referentes aos termos destacados na Tab. 5.1 na esfera governamental.

A Tabela 5.2 recorda os termos que estão presentes somente nas regulamentações. Os conceitos exclusivamente pertencentes à IN 01 e suas normas complementares não são, em sua maioria, parte da GRSI. Com exceção de análise/avaliação de riscos, estimativa de riscos e reduzir riscos, os termos definidos nas regulamentações são mais apropriados ao contexto de segurança da informação. Sua presença se justifica nas regulamentações porque a IN01 e suas normas complementares tratam da segurança da informação como um todo. No sistema sociotécnico, a família de normas 27000 aborda a SI e suas várias componentes e estes conceitos permeiam suas normas, sendo desnecessária a inclusão destes conceitos nas normas da ABNT.

Com referência aos três termos relativos à GRSI, o primeiro deles é definido apenas como o processo de análise/avaliação de riscos, que é equivalente ao processo de avaliação de riscos visto na ABNT 27005. Os termos restantes, estimativa de riscos e reduzir riscos são particulares da NC 04. O conceito de estimativa de riscos não está presente nas normas, sendo recomendada sua possível admissão no sistema sociotécnico. Por fim, redução de riscos, assim como modificação do risco (ABNT 27005) são opções de tratamento de riscos propostas pelas regulamentações e normas, respectivamente. Sugere-se que a adoção destas, bem como dos conceitos que as explicam, sejam consideradas por ambas as partes.

Tabela 5.2: Relação de termos presentes somente nas regulamentações

IN 01	Segurança da Informação e Comunicações Disponibilidade Integridade Confidencialidade Autenticidade Gestão de SIC Quebra de Segurança Tratamento de Informação
NC 04	Ameaça Análise/Avaliação de riscos Ativos de Informação Estimativa de riscos Reduzir Riscos

Finalmente, as sugestões para os conceitos dúbios previamente submetidos ao questionário compõem a última etapa de recomendações terminológicas. Como foi visto no Capítulo 4, o resultado dos questionários demonstra a propensão dos especialistas de segurança da informação a

optar pelos conceitos das normas ABNT quando se trata de gestão de riscos de segurança da informação. Com base nos resultados obtidos e em busca da harmonização dos conceitos, aconselha-se a utilização dos listados a seguir. Para os conceitos retirados da Guia 73, vide Anexo III para as notas sobre cada um:

Riscos de segurança da informação e comunicações:

> Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização; (BRASIL, 2013)

Comunicação e consulta:

> Processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas (3.18) e outros, com relação a gerenciar riscos... (ABNT, 2009a)

Gestão de Riscos de Segurança da Informação e Comunicações:

> Conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos; (BRASIL, 2013)

Vulnerabilidade:

"Propriedades intrínsecas de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência."(ABNT, 2009a)

Avaliação de riscos:

"Processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável."(ABNT, 2009a)

Compartilhamento de riscos:

"Forma de tratamento de riscos que envolve a distribuição acordada de riscos com outras partes."(ABNT, 2011)

Tratamento de riscos:

"Processo para modificar o risco."(ABNT, 2009a)

Evitar risco:

"Uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco."(BRASIL, 2013)

Retenção de riscos:

"Aceitação do benefício potencial de ganho, ou do ônus da perda, a partir de um risco específico."(ABNT, 2009a)

Análise de riscos:

"Processo de compreender a natureza do risco e determinar o nível de risco."(ABNT, 2009a)

Identificação de riscos:

"Processo de busca, reconhecimento e descrição de riscos."(ABNT, 2009a)

Embora a maioria dos conceitos escolhidos seja proveniente das normas, uma crítica pode ser feita a ABNT 27005: como a norma simplesmente reproduz os conceitos do Guia 73, estes se enquadram perfeitamente na gestão de riscos, mas deixam a desejar quando contextualizados na gestão de riscos de *segurança da informação*. Uma forma de solucionar esse problema é a complementação do vocabulário na norma sobre GRSI conforme previsto pelo próprio Guia 73 em sua introdução.

5.2 SUGESTÕES REFERENTES AOS PROCESSOS

Com base na análise de processos no Capítulo 4, pôde-se observar com mais clareza a existência das diferenças entre os processos das regulamentações e os das normas. A exposição dos fluxogramas descritivos auxiliou na identificação visual destas diferenças.

Identificou-se então as possíveis recomendações que podem vir a solucionar ou minimizar a discrepância entre os objetos estudados:

a) Definições preliminares / definição do contexto

O principal aspecto identificado na NC 04 nesta etapa foi a falta de maiores detalhes sobre orientações nas fases. Observa-se que a definição de critérios e a definição de escopo não possuem especificações na regulamentação e seus estabelecimentos ficam a critério dos responsáveis pelo processo de GRSI. A recomendação aqui seria de criar diretrizes para auxiliar estas definições.

Outro fato apontado foi o condensamento das fases na NC 04. Isto causa dúvidas acerca do foco de cada uma delas. Temos como exemplo a "definição de critérios", que é extremamente importante para definir o contexto, inserida na fase "análise da organização"cujo objetivo principal é dar o enfoque da GRSI dentro do órgão. O desmembramento desta fase em duas separadas seria de grande proveito.

Uma última sugestão é o estabelecimento da ocorrência simultânea de fases para aumentar a praticidade das definições preliminares na NC 04.

b) Análise/Avaliação de Riscos / Processo de Avaliação de Riscos

A sugestão da existência de níveis de estimativa dos riscos na NC 04 é um ponto positivo que aproxima a regulamentação do sistema sociotécnico na etapa em questão. No entanto os detalhamentos e orientações de criação destes ficam em aberto. Isto é um exemplo da superficialidade da regulamentação a ser corrigida para melhor emprego do processo de GRSI nos órgãos e entidades da APF. Nota-se ainda que durante a aplicação da NC 04 corre-se o risco de confundir a fase "avaliação de riscos"com a fase "aceitação de riscos", pois a seleção de riscos aceitáveis pode ser misturada com a seleção de riscos aceitos. Confusão que não deveria ocorrer, pois causará problemas mais adiante no processo geral da NC 04.

A NC 04 apresenta superficialidade nas diversas fases descritas nesta etapa e se baseia em um modelo "análise/avaliação de riscos"antigo, já reformulado e em vigor na ABNT 31000 e na ABNT 27005 como "processo de avaliação de riscos". Atualizar a regulamentação ao modelo mais recente é altamente indicado para reduzir o afastamento da APF em relação à iniciativa privada que já o adota.

Tendo conhecimento de que o "processo de avaliação de riscos"é o momento mais importante do processo geral de GRSI na ABNT 27005, seria ideal que ele fosse mais detalhado, cuidadosamente repensado e renovado na NC 04.

c) Plano de Tratamento de Riscos/ Tratamento do Risco

Nesta etapa a NC 04 e a ABNT 27005 são bastante semelhantes em suas abordagens. Dentre as quatro opções de tratamento oferecidas em ambas, três possuem equivalência parcial ou total. A ABNT 27005 apenas se destaca aqui pela riqueza na explicação de cada opção e pelo estabelecimento de um ponto de decisão ao final que acrescenta iteratividade ao processo geral de GRSI.

Recomenda-se que esta etapa da NC 04 seja revisada e aprofundada à luz da ABNT 27005 pois aqui surge um conceito muito importante não abordado na regulamentação: riscos residuais. Os riscos residuais são aqueles que permanecem mesmo após o tratamento do risco. Uma lista contendo todos eles é gerada nesta etapa da ABNT 27005 e é importante para etapas futuras do processo. Uma outra sugestão é que a adoção das opções de tratamento de riscos denominadas redução do risco (NC 04) e modificação do risco (ABNT 27005) seja considerada por ambas as partes.

d) Aceitação dos Riscos/ Aceitação do Risco

O texto original da regulamentação sobre esta etapa possui apenas uma frase em duas linhas para defini-la. Nota-se, somente desta informação, que o tratamento dado a "aceitação dos riscos"é demasiadamente vago. O ideal neste ponto seria o abandono do modelo de aceitação da NC 04 e a adoção do modelo da ABNT 27005.

e) Monitoração e Análise Crítica, Melhoria do Processo de GRSIC/ Monitoramento e Análise Crítica

Enquanto a regulamentação aborda a "monitoração e análise crítica"e a "melhoria do processo de GRSIC"como duas etapas separadas, a norma inclui a melhoria como parte da etapa "monitoramento e análise crítica". Os objetivos de ambas, no entanto, são bastante correlacionados.

Apesar da ideia de separar as etapas ser boa para melhorar a especialização de cada uma delas, a ABNT 27005 se apresenta mais completa no relato das fases de sua única etapa. O ideal seria mesclar as duas formas de abordagem para melhor e mais clara execução dos objetivos.

f) Comunicação do Risco / Comunicação e Consulta do Risco

Esta etapa apresenta altíssimo grau de equivalência entre regulamentação e norma, tanto em seu artefato de entrada quanto em sua fase. Porém a norma demonstra maior abrangência ao considerar as partes envolvidas como integrantes do compartilhamento. Ela ainda vai além e define e orienta as peculiaridades da etapa como um todo. A NC 04 deve portanto ser revista, com base na ABNT 27005, para complementar seu conteúdo e aumentar seu alcance.

Existe ainda a etapa "implementação do plano de tratamento de riscos"presente apenas na NC 04. Esta etapa surge como tentativa da regulamentação de se adequar de forma literal ao PDCA. No entanto a implementação do plano de tratamento de riscos não pode ser considerada uma etapa isolada por estar implícita em todo o processo de GRSI. Aconselha-se então a remoção desta da metodologia da NC 04.

5.3 SUGESTÕES GERAIS

Em resumo, as recomendações feitas neste capítulo demonstram a necessidade de:

- Incluir nas regulamentações os conceitos referentes aos seguintes termos, encontrados apenas na ABNT 27005: *parte interessada*, *contexto externo*, *contexto interno*, *critérios de riscos*, *evento*, *probabilidade (likelihood)*, *nível de risco*, *consequência* e *risco residual*;
- Incluir na ABNT 27005 o conceito de *estimativa de riscos*, encontrado somente nas regulamentações;
- Adotar nas normas da ABNT os conceitos vistos nas regulamentações referentes aos seguintes termos: *riscos de segurança da informação e comunicações*, *gestão de riscos de segurança da informação e comunicações* e *evitar risco*;
- Adotar nas regulamentações do governo os conceitos vistos nas normas ABNT referentes aos seguintes termos: *comunicação e consulta*, *vulnerabilidade*, *avaliação de riscos*, *compartilhamento de riscos*, *tratamento de riscos*, *retenção de riscos*, *análise de riscos* e *identificação de riscos*
- Adotar em ambas as partes as opções de tratamento de riscos denominadas *redução do risco* (NC 04) e *modificação do risco* (ABNT 27005), bem como suas definições; e
- Reformular o processo de GRSI da NC 04, principalmente no que diz respeito à funda-

mentação de cada etapa dele;

A vantagem da regulamentação aparece nos termos e definições empregados, pois os conceitos estão inseridos no cenário de GRSI. No entanto o detalhamento dos processos é bastante superficial. A ABNT 27005 fica bem a frente em relação aos processos pela sua minuciosidade na descrição de cada etapa e fase. Já na questão terminológica, a norma poderia revisar alguns termos e definições para que se adequem ao contexto específico de GRSI. Esses pontos são destacados na Tabela 5.3

Tabela 5.3: Resumo do estudo comparativo

Aspectos a serem destacados	**Normas**	**Regulamentações**
Pontos Positivos	Fundamentação nas diretrizes do processo	Conceitos adequados ao contexto de GRSI
Pontos Negativos	Conceitos genéricos	Superficialidade na descrição do processo

Sabe-se que por serem regulamentações de caráter normativo, a IN 01 e suas as Normas Complementares devem ter um aspecto resumido e objetivo. Sendo assim, uma sugestão maior seria a elaboração de um guia acompanhante delas, a exemplo da publicação do Guia Prático para Contratação de Soluções de Tecnologia da Informação pela Secretaria de Logística e Tecnologia de Informação (SLTI) que orienta e complementa a IN SLTI/MP n^{o}04/2010 e seu emprego.

6 CONCLUSÕES

Após percebermos a disfunção existente nos órgãos e entidades da Administração Pública Federal em relação à gestão de riscos de segurança da informação, buscamos as regulamentações que tratavam do estabelecimento do processo de gestão de riscos de segurança da informação neste ambiente. Descobrimos então que estas regulamentações estavam em desacordo com o proposto pelo sistema sociotécnico vigente, a ABNT. A escolha pela comparação entre essas duas abordagens se deu pelo fato de que a ABNT representa uma metodologia internacionalmente aceita e amplamente adotada pela iniciativa privada. Definimos que a comparação seria feita em duas frentes: terminológica e de processos.

A partir daí efetuamos a análise de cada uma das normas e regulamentações referentes ao processo de GRSI. Dentre este universo de recomendações, destacaram-se como objetos de estudo: ABNT ISO GUIA 73:2009, ABNT NBR ISO/IEC 27005:2011, Instrução Normativa GSI/PR n^o 01, Norma Complementar 02/IN01/DSIC/GSIPR e Norma Complementar 04/IN01/DSIC/GSIPR, detalhados no Capítulo 3.

A análise comparativa das normas e regulamentações se deu no desenvolvimento do Capítulo 4. Para a análise em nível terminológico, a solução encontrada foi a separação de conceitos presentes apenas nas normas (9 na ABNT 27005 e 22 no Guia 73) ou nas regulamentações (8 na IN 01 e 5 na NC 04) dos conceitos comuns entre ambas. Estes últimos, 22 no total, foram submetidos a um questionário aplicado aos especialistas da área de segurança da informação. Eles foram questionados quanto ao grau de conformidade entre os conceitos e a adequação ao contexto de GRSI. Os resultados mostram que 64% dos conceitos são parcialmente equivalentes e 36% são equivalentes, não existindo a não equivalência. Já em relação ao contexto de GRSI, o sistema sociotécnico foi considerado o mais adequado em 73% das comparações feitas. No entanto, alguns conceitos das normas da ABNT foram considerados muito gerais, pois tratavam da gestão de riscos sem a especificidade da segurança da informação.

Pelo lado da análise de processos, observou-se que as 8 etapas das regulamentações possuem conteúdo muito superficial, dando margem a diferentes interpretações e critérios de aplicação. Já as 6 etapas contempladas pela ABNT 27005 se destacam por seu maior alcance, detalhando os passos a serem seguidos de forma clara e objetiva. Foram desenvolvidos 13 fluxogramas com o objetivo de melhor ilustrar as principais etapas, suas fases e diferenças.

No Capítulo 5, foram elaboradas as seguintes sugestões gerais para alinhamento dos processos e harmonização dos conceitos:

- Inclusão nas regulamentações dos conceitos referentes aos seguintes termos, encontrados apenas na ABNT 27005: *parte interessada*, *contexto externo*, *contexto interno*, *critérios de*

riscos, *evento*, *probabilidade (likelihood)*, *nível de risco*, *consequência* e *risco residual*;
- Inclusão na ABNT 27005 do conceito de *estimativa de riscos*, encontrado somente nas regulamentações;
- Adoção pelas normas da ABNT dos conceitos vistos nas regulamentações referentes aos seguintes termos: *riscos de segurança da informação e comunicações*, *gestão de riscos de segurança da informação e comunicações* e *evitar risco*;
- Adoção pelas regulamentações dos conceitos vistos nas normas ABNT referentes aos seguintes termos: *comunicação e consulta*, *vulnerabilidade*, *avaliação de riscos*, *compartilhamento de riscos*, *tratamento de riscos*, *retenção de riscos*, *análise de riscos* e *identificação de riscos*
- Adoção por ambas as partes das opções de tratamento de riscos denominadas *redução do risco* (NC 04) e *modificação do risco* (ABNT 27005), bem como de suas definições;
- Revisão do vocabulário presente na ABNT 27005 considerando especificamente o contexto de gestão de riscos de segurança da informação no sistema sociotécnico; e
- Reformulação do processo de GRSI na Norma Complementar 04 atentando para a fundamentação de cada uma de suas etapas.

Conforme demonstrado, todos os objetivos propostos inicialmente - análise conceitual e de processos descritos pelas regulamentações e pela ABNT, identificação das diferenças entre os dois sistemas e propostas de medidas de alinhamento conceitual e de processos - foram atingidos neste projeto.

Dada a natureza resumida de regulamentações de caráter normativo, sugere-se para trabalhos futuros a elaboração e implementação de um guia que acompanhe a IN 01 e suas Normas Complementares. Este guia contemplaria as principais diretrizes, orientações, termos e definições, com maior detalhamento, para aplicação do processo de gestão de riscos de segurança da informação na Administração Pública Federal.

Outra sugestão para trabalhos posteriores é um estudo mais fundamentado acerca da estrutura dos fluxogramas das etapas dos processos. Como nem as regulamentações nem o sistema sociotécnico possuem diagramas de processo definidos para a gestão de riscos de segurança da informação, um estudo para a formulação e estruturação de fluxogramas que auxiliem na elaboração destes diagramas seria de grande utilidade e pertinência.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANDERSON, J. Why we need a new definition of information security. *Computers Security*, v. 22, n. 4, p. 308–313, 2003.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 13790*: Terminologia - Princípios e métodos - Harmonização de conceitos e termos. [S.l.], 1997. 6 p.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27002*: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão de segurança da informação. [S.l.], 2005. 120 p.

[4] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001*: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos. [S.l.], 2006. 34 p.

[5] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ISO Guia 73*: Gestão de riscos - Vocabulário. [S.l.], 2009a. 12 p.

[6] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO 31000*: Gestão de riscos - Princípios e diretrizes. [S.l.], 2009b. 24 p.

[7] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27005*: Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação. [S.l.], 2011. 87 p.

[8] BEAL, A. *Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações*. São Paulo: Atlas, 2004.

[9] BRASIL. Decreto nº 7411, de 29 de dezembro de 2010. Dispõe sobre remanejamento de cargos em comissão do grupo-direção e assessoramento superiores - DAS, aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão e das gratificações de exercício em cargo de confiança do Gabinete de Segurança Institucional da Presidência da República; altera o Anexo II do Decreto nº 7.063, de 13 de janeiro de 2010, e dá outras providências. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 30 de dez. 2010. N. 250, Seção 1, p. 44-6.

[10] BRASIL. Gabinete de Segurança Institucional da Presidência da República. Instrução Normativa GSI nº 01, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 18 jun. 2008a. N. 115, Seção 1, p. 6.

[11] BRASIL. Gabinete de Segurança Institucional da Presidência da República. Norma Complementar n^o 02/IN01/DSIC/GSIPR - Metodologia de Gestão de Segurança da Informação e Comunicações, de 13 de outubro de 2008. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 14 out. 2008b. N. 199, Seção 1, p. 1-2.

[12] BRASIL. Gabinete de Segurança Institucional da Presidência da República. Norma complementar n^o 04 /IN01/DSIC/GSIPR, e seu anexo, (Revisão 01) - Diretrizes para o processo de gestão de riscos de segurança da informação e comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal, de 15 de fevereiro de 2013. *Diário Oficial da União*, Poder Executivo, Brasília, DF, 25 fev. 2013. N. 37, Seção 1, p. 1-3.

[13] BRASIL. Tribunal de Contas da União. *Acórdão 2585/2012*: Relatório de levantamento. Avaliação da governança de tecnologia da informação na administração pública federal. Oportunidades de melhoria. Recomendações. [S.l.], 2012a.

[14] BRASIL. Tribunal Regional Federal. Região, 2. Apelação cível 2002.51.10.003849-4. Apelante: União Federal/Fazenda Nacional. Apelado: Cia Sulamericana de Tabacos s/a. Relator: Juiz Federal Convocado Luiz Norton Baptista de Mattos. Acórdão, 06 março de 2012. *Lex* — Diário Eletrônico da Justiça Federal da 2a Região, p. 109, mar. 2012b. Disponível em: <https://dje.trf2.jus.br/DJE/Paginas/VisualizarCadernoPDF.aspx?ID=6450>. Acesso em: 06 dez. 2012.

[15] DE MORAES, A. *Direito Constitucional*. 10. ed. São Paulo: Atlas, 2001.

[16] OLIVEIRA, W. J. de. *Segurança da Informação - Técnicas e Soluções*. Florianópolis: Editora Visual Books, 2001.

[17] LORENS, E. M. *Aspectos normativos da segurança da informação: um modelo de cadeia de regulamentação*. Dissertação (Mestrado em Ciência da Informação) — Departamento de Ciência da Informação, Universidade de Brasília, Brasília, 2007.

[18] MORENO, C. Polissemia e homonímia. mai. 2009. Disponível em: <wp.clicrbs.com.br/sualingua/2009/05/13/polissemia-e-homonimia/>. Acesso em: 08 mai. 2013.

[19] SÊMOLA, M. *Gestão de Segurança da Informação*: uma visão executiva. 12. ed. Rio de Janeiro: Elsevier, 2003.

[20] SOMMERVILLE, I. *Engenharia de Software*. São Paulo: Pearson Prentice Hall, 2007.

[21] VIANA, H. de S. *Governança de TI e suas Metodologias Dentro do Mundo Corporativo*: um enfoque de alto nível baseado na ISO:IEC 27005. Monografia (Especialização em Engenharia de Produção) — Universidade Cândido Mendes, Rio de Janeiro, 2010.

[22] ZAPATER, M.; SUZUKI, R. *Segurança da Informação*: Um diferencial na competitividade das corporações. Rio de Janeiro: Promon Business & Technology Review, 2005.

ANEXOS

I. QUESTIONÁRIO

Tentando esclarecer dubiedades em relação a questões de gestão de riscos de SI, o questionário a seguir trará conceitos que deverão ser comparados para obter o melhor vocabulário do tema. Este questionário foi organizado da seguinte maneira: são apresentados conceitos presentes nas normas e regulamentações, mantendo suas fontes ocultas para não influenciar na escolha do entrevistado. Para cada par de conceitos, é perguntado o grau de conformidade, que pode ser: equivalente, parcialmente equivalente ou não equivalente. Em seguida, é pedido que o entrevistado analise a adequação de cada um deles ao contexto de gestão de riscos de segurança da informação e que escolha o que considera mais apropriado.

Os conceitos foram retirados das seguintes fontes:

- ABNT. Associação Brasileira de Normas Técnicas. ISO Guia 73 - Gestão de Riscos - Vocabulário, 2009

- Norma Complementar n^o 04: Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Brasília: 2013

1) Verifique as duas definições e julgue:

1 - **Risco** - efeito da incerteza nos objetivos

NOTA 1 Um efeito é um desvio em relação ao esperado - positivo e/ou negativo.

NOTA 2 Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar-se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo).

NOTA 3 O risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências, ou uma combinação destes.

NOTA 4 O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade (likelihood) de ocorrência associada.

NOTA 5 A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade;

2 - **Riscos de Segurança da Informação e Comunicações** - potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado contexto de GRSI?

( ) 1

( ) 2

2) Verifique as duas definições e julgue:

1 - **Comunicação e consulta** - processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos

NOTA 1 As informações podem referir-se à existência, natureza, forma, probabilidade (likelihood), severidade, avaliação, aceitabilidade, tratamento ou outros aspectos da gestão de riscos.

NOTA 2 A consulta é um processo bidirecional de comunicação sistematizada entre uma organização e suas partes interessadas ou outros, antes de tomar uma decisão ou direcionar uma questão específica. A consulta é: um processo que impacta uma decisão através da influência ao invés do poder; e uma entrada para o processo de tomada de decisão, e não uma tomada de decisão em conjunto.

2 -**Comunicação do risco** - troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

3) Verifique as duas definições e julgue:

1 - **Gestão de riscos**- atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

2 - **Gestão de Riscos de Segurança da Informação e Comunicações** - conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

4) Verifique as duas definições e julgue:

1 - **Vulnerabilidade** - propriedades intrínsecas de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência.

2 - **Vulnerabilidade** - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

5) Verifique as duas definições e julgue:

1 - **Avaliação de riscos** - processo de comparar os resultados da análise de riscos com os

critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.

2 - **Avaliação de riscos** - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

6) Verifique as duas definições e julgue:

1 - **Compartilhamento de riscos** - forma de tratamento de riscos que envolve a distribuição acordada de riscos com outras partes.

NOTA 1 Requisitos legais ou regulatórios podem limitar, proibir ou ordenar o compartilhamento de risco.

NOTA 2 O compartilhamento de risco pode ser realizado através de seguros ou outras formas de contrato.

NOTA 3 A extensão em que o risco é distribuído pode depender da confiabilidade e clareza dos acordos de compartilhamento.

NOTA 4 A transferência de risco é uma forma de compartilhamento de risco.

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

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

7) Verifique as duas definições e julgue:

1 - **Tratamento de riscos** - processo para modificar o risco.

NOTA 1 O tratamento de risco pode envolver:

- a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco;

- assumir ou aumentar o risco, a fim de buscar uma oportunidade;

- a remoção da fonte de risco;

- a alteração da probabilidade (likelihood);

- a alteração das consequências;

- o compartilhamento do risco com outra parte ou partes [incluindo contratos e financiamento do risco];

- a retenção do risco por uma escolha consciente.

NOTA 2 Os tratamentos de riscos relativos a consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos"e "redução de riscos".

NOTA 3 O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

2 - **Tratamento dos riscos** - processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

8) Verifique as duas definições e julgue:

1 - **Ação de evitar o risco** - decisão informada de não se envolver, ou retirar-se de uma

atividade, a fim de não ser exposto a um risco específico.

NOTA A ação de evitar o risco pode ser baseada nos resultados da avaliação de riscos e/ou em obrigações legais e regulatórios.

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

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

9) Verifique as duas definições e julgue:

1 - **Retenção de riscos** - aceitação do benefício potencial de ganho, ou do ônus da perda, a partir de um risco específico.

NOTA 1 A retenção de riscos inclui a aceitação de riscos residuais.

NOTA 2 O nível de risco retido pode depender dos critérios de risco.

2 - **Reter risco** - uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

10) Verifique as duas definições e julgue:

1 -**Análise de riscos** - processo de compreender a natureza do risco e determinar o nível de

risco.

NOTA 1 A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos.

NOTA 2 A análise de riscos inclui a estimativa de riscos.

2 - **Análise de riscos** - uso sistemático de informações para identificar fontes e estimar o risco;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

11) Verifique as duas definições e julgue:

1 - **Identificação de riscos** - processo de busca, reconhecimento e descrição de riscos.

NOTA 1 A identificação de riscos envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais.

NOTA 2 A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

2 - **Identificação de riscos** - processo para localizar, listar e caracterizar elementos do risco;

( ) Os conceitos acima podem ser considerados equivalentes;

( ) Os conceitos acima podem ser considerados parcialmente equivalentes;

( ) Os conceitos acima não são equivalentes.

Dentre os conceitos apresentados, qual você considera mais adequado ao contexto de GRSI?

( ) 1

( ) 2

II. RESULTADOS DO QUESTIONÁRIO

Este anexo mostra as tabelas que resumem os resultados do questionário visto no Anexo I, elaboradas com a ferramenta Microsoft Office Excel 2010. A Tabela II.1 traz as respostas dos 14 entrevistados quanto ao grau de conformidade. A opção 1 representa conceitos equivalentes, a 2 conceitos parcialmente equivalentes enquanto a 3 trata dos conceitos não equivalentes.

A Tabela II.2 ilustra a conclusão dos entrevistados em relação a adequação dos conceitos ao contexto de GRSI. Neste caso, a opção 1 indica a preferência pelo conceito da ABNT enquanto a opção 2 mostra a escolha dos conceitos das regulamentações.

QUESTÕES E RESPOSTAS	Questão 1	Questão 2	Questão 3	Questão 4	Questão 5	Questão 6	Questão 7	Questão 8	Questão 9	Questão 10	Questão 11
Entrevistado 1	2	2	2	3	1	2	2	2	2	3	1
Entrevistado 2	2	3	1	1	2	1	2	1	2	1	1
Entrevistado 3	3	2	2	3	2	2	2	1	3	3	1
Entrevistado 4	2	2	2	2	2	1	2	1	3	1	2
Entrevistado 5	2	3	2	1	1	1	1	1	1	2	1
Entrevistado 6	2	2	1	2	2	2	2	1	2	2	2
Entrevistado7	2	1	2	1	1	1	2	1	2	1	1
Entrevistado 8	2	1	2	2	1	2	1	1	2	1	1
Entrevistado 9	2	1	1	1	1	2	1	2	3	1	1
Entrevistado 10	2	2	2	1	1	2	2	1	3	2	1
Entrevistado 11	2	2	2	1	2	2	2	1	2	2	1
Entrevistado 12	3	1	2	3	2	3	2	1	2	3	2
Entrevistado 13	3	1	2	3	2	1	2	2	3	3	2
Entrevistado 14	3	3	1	3	3	1	3	2	3	1	1
Grau de Conformidade	2	2	2	1	2	2	2	1	2	1	1

Legenda:
1 - conceitos equivalentes
2 - conceitos parcialmente equivalentes
3 - conceitos não equivalentes

Tabela II.1: Respostas dos entrevistados quanto ao grau de conformidade entre os conceitos.

QUESTÕES E RESPOSTAS	Questão 1	Questão 2	Questão 3	Questão 4	Questão 5	Questão 6	Questão 7	Questão 8	Questão 9	Questão 10	Questão 11
Entrevistado 1	2	1	1	1	1	1	1	1	1	1	1
Entrevistado 2	2	2	2	2	2	1	2	2	2	2	2
Entrevistado 3	2	1	2	1	1	1	1	2	1	1	1
Entrevistado 4	2	1	2	2	1	2	1	2	1	1	1
Entrevistado 5	1	2	2	1	1	1	1	2	1	1	1
Entrevistado 6	1	1	2	1	2	1	1	2	1	1	1
Entrevistado 7	2	1	2	2	1	2	2	2	2	1	2
Entrevistado 8	2	2	2	2	1	2	1	2	1	1	1
Entrevistado 9	2	2	2	1	1	1	2	2	2	2	2
Entrevistado 10	2	1	2	1	1	1	1	2	1	1	1
Entrevistado 11	2	1	2	1	1	1	1	2	1	1	1
Entrevistado 12	1	1	2	1	1	1	1	1	1	1	1
Entrevistado 13	1	1	1	1	1	1	1	1	1	1	1
Entrevistado 14	2	2	2	2	2	1	2	1	2	2	2
Opção Escolhida	2	1	2	1	1	1	1	2	1	1	1

Legenda:
1 - Conceito da ABNT
2 - Conceito da regulamentação

Tabela II.2: Respostas dos entrevistados sobre a adequação dos conceitos ao contexto de GRSI.

III. GLOSSÁRIO

Este glossário apresenta a compilação dos conceitos usados nos objetos de pesquisa desta monografia. Primeiramente, são mostrados os termos e definições da ABNT ISO GUIA 73 e, em seguida, os da Instrução Normativa GSI N^o 1 e da Norma Complementar n^o 04/IN01/DSIC/GSIPR.

ABNT ISO GUIA 73:2009 (ABNT,2009a)

risco

efeito da incerteza nos objetivos

NOTA 1 Um efeito é um desvio em relação ao esperado - positivo e/ou negativo.

NOTA 2 Os objetivos podem ter diferentes aspectos (tais como metas financeiras, de saúde e segurança e ambientais) e podem aplicar-se em diferentes níveis (tais como estratégico, em toda a organização, de projeto, de produto e de processo).

NOTA 3 O risco é muitas vezes caracterizado pela referência aos eventos potenciais e às consequências, ou uma combinação destes.

NOTA 4 O risco é muitas vezes expresso em termos de uma combinação de consequências de um evento (incluindo mudanças nas circunstâncias) e a probabilidade (likelihood) de ocorrência associada.

NOTA 5 A incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

gestão de riscos

atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

estrutura da gestão de riscos

conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização

NOTA 1 Os fundamentos incluem a política, objetivos, mandatos e comprometimento para gerenciar riscos.

NOTA 2 Os arranjos organizacionais incluem planos, relacionamentos, responsabilidades, recursos, processos e atividades.

NOTA 3 A estrutura da gestão de riscos está incorporada no âmbito das políticas e práticas estratégicas e operacionais de toda a organização.

política de gestão de riscos

declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos

plano de gestão de riscos

esquema dentro da estrutura de gestão de riscos, que especifica a abordagem, os componentes de gestão e os recursos a serem aplicados para gerenciar riscos

NOTA 1 Os componentes de gestão tipicamente incluem procedimentos, práticas, atribuição de responsabilidades, sequência e a cronologia das atividades.

NOTA 2 O plano de gestão de riscos pode ser aplicado a um determinado produto, processo e projeto, em parte ou em toda a organização.

processo de gestão de riscos

aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos

comunicação e consulta

processos contínuos e iterativos que uma organização conduz para fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas e outros, com relação a gerenciar riscos

NOTA 1 As informações podem referir-se à existência, natureza, forma, probabilidade (likelihood), severidade, avaliação, aceitabilidade, tratamento ou outros aspectos da gestão de riscos.

NOTA 2 A consulta é um processo bidirecional de comunicação sistematizada entre uma organização e suas partes interessadas ou outros, antes de tomar uma decisão ou direcionar uma questão específica. A consulta é:

- um processo que impacta uma decisão através da influência ao invés do poder; e
- uma entrada para o processo de tomada de decisão, e não uma tomada de decisão em conjunto.

parte interessada

pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade

NOTA Um tomador de decisão pode ser uma parte interessada.

percepção do risco

visão de risco da parte interessada

NOTA A percepção de risco reflete as necessidades, questões, conhecimento, crença e valores da parte interessada.

estabelecimento do contexto

definição dos parâmetros externos e internos a serem levados em consideração ao gerenciar riscos, e estabelecimento do escopo e dos critérios de risco para a política de gestão de riscos

contexto externo

ambiente externo no qual a organização busca atingir seus objetivos

NOTA O contexto externo pode incluir:

- o ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja internacional, nacional, regional ou local;
- os fatores-chave e as tendências que tenham impacto sobre os objetivos da organização; e
- as relações com partes interessadas externas e suas percepções e valores.

contexto interno

ambiente interno no qual a organização busca atingir seus objetivos

NOTA O contexto interno pode incluir:

- governança, estrutura organizacional, funções e responsabilidades;
- políticas, objetivos e estratégias implementadas para atingi-los;
- capacidades compreendidas em termos de recursos e conhecimento (por exemplo, capital, tempo, pessoas, processos, sistemas e tecnologias);
- sistemas de informação, fluxos de informação e processos de tomada de decisão (tanto formais como informais);
- relações com partes interessadas internas, e suas percepções e valores;
- cultura da organização;
- normas, diretrizes e modelos adotados pela organização; e
- forma e extensão das relações contratuais.

critérios de risco

termos de referência contra os quais a significância de um risco é avaliada

NOTA 1 Os critérios de risco são baseados nos objetivos organizacionais e no contexto externo e contexto interno.

NOTA 2 Os critérios de risco podem ser derivados de normas, leis, políticas e outros requisitos.

processo de avaliação de riscos

processo global de identificação de riscos, análise de riscos e avaliação de riscos

identificação de riscos

processo de busca, reconhecimento e descrição de riscos

NOTA 1 A identificação de riscos envolve a identificação das fontes de risco, eventos, suas causas e suas consequências potenciais.

NOTA 2 A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e especialistas, e as necessidades das partes interessadas.

descrição dos riscos

declaração estruturada de riscos, contendo normalmente quatro elementos: fontes, eventos, causas e consequências

fonte de risco

elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco
NOTA Uma fonte de risco pode ser tangível ou intangível.

evento

ocorrência ou mudança em um conjunto específico de circunstâncias
NOTA 1 Um evento pode consistir em uma ou mais ocorrências e pode ter várias causas.
NOTA 2 Um evento pode consistir em alguma coisa não acontecer.
NOTA 3 Um evento pode algumas vezes ser referido como um "incidente"ou um "acidente".
NOTA 4 Um evento sem consequências também pode ser referido como um "quase acidente", ou um "incidente"ou "por um triz".

perigo

fonte de potencial dano
NOTA O perigo pode ser uma fonte de risco).

proprietário do risco

pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco

análise de riscos

processo de compreender a natureza do risco) e determinar o nível de risco
NOTA 1 A análise de riscos fornece a base para a avaliação de riscos e para as decisões sobre o tratamento de riscos.
NOTA 2 A análise de riscos inclui a estimativa de riscos.

probabilidade (likelihood)

chance de algo acontecer
NOTA 1 Na terminologia de gestão de riscos, a palavra "probabilidade"é utilizada para referir-se à chance de algo acontecer, não importando se de forma definida, medida ou determinada ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos

gerais ou matemáticos (tal como probabilidade ou frequência durante um determinado período de tempo).
NOTA 2 O termo em Inglês "likelihood"não têm um equivalente direto em algumas línguas; em vez disso, o equivalente do termo "probability"é frequentemente utilizado. Entretanto, em Inglês, "probability"é muitas vezes interpretado estritamente como uma expressão matemática. Portanto, na terminologia de gestão de riscos, "likelihood"é utilizado com a mesma ampla interpretação de que o termo "probability"tem em muitos outros idiomas além do Inglês.

exposição
grau em que uma organização e/ou parte interessada está sujeita a um evento

consequência
resultado de um evento que afeta os objetivos
NOTA 1 Um evento pode levar a uma série de consequências.
NOTA 2 Uma consequência pode ser certa ou incerta e pode ter efeitos positivos ou negativos sobre os objetivos.
NOTA 3 As consequências podem ser expressas qualitativa ou quantitativamente.
NOTA 4 As consequências iniciais podem desencadear reações em cadeia

probabilidade
medida da chance de ocorrência expressa como um número entre 0 e 1, onde 0 é a impossibilidade e 1 é a certeza absoluta
NOTA Ver definição de probabilidade(likelihood), Nota 2.

frequência
número de eventos ou resultados por unidade de tempo definida
NOTA Frequência pode ser aplicada a eventos passados ou a potenciais eventos futuros, onde eles podem ser usados como uma medida de probabilidade (likelihood))/probabilidade

vulnerabilidade
propriedades intrínsecas de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma consequência

matriz de risco
ferramenta para classificar e apresentar riscos definindo faixas para consequência e probabilidade (likelihood)

nível de risco

magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades (likelihood)

avaliação de riscos

processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável

NOTA A avaliação de riscos auxilia na decisão sobre o tratamento de riscos.

atitude perante o risco

abordagem da organização para avaliar e eventualmente buscar, reter, assumir ou afastar-se do risco

apetite pelo risco

quantidade e tipo de riscos que uma organização está preparada para buscar, reter ou assumir

tolerância ao risco

disposição da organização ou parte interessada em suportar o risco após o tratamento do risco, a fim de atingir seus objetivos

NOTA A tolerância ao risco pode ser influenciada por requisitos legais ou regulatórios.

aversão ao risco

atitude de afastar-se de riscos

agregação de risco

combinação de um número de riscos dentro de um único risco para desenvolver o mais completo entendimento do risco global

aceitação do risco

decisão consciente de assumir um risco específico

NOTA 1 A aceitação do risco pode ocorrer sem o tratamento do risco ou durante o processo de tratamento de riscos.

NOTA 2 Riscos aceitos estão sujeitos a monitoramento e análise crítica.

tratamento de riscos

processo para modificar o risco

NOTA 1 O tratamento de risco pode envolver

- a ação de evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao

risco;
- assumir ou aumentar o risco, a fim de buscar uma oportunidade;
- a remoção da fonte de risco;
- a alteração da probabilidade (likelihood);
- a alteração das consequências;
- o compartilhamento do risco com outra parte ou partes (incluindo contratos e financiamento do risco); e
- a retenção do risco por uma escolha consciente.
NOTA 2 Os tratamentos de riscos relativos a consequências negativas são muitas vezes referidos como "mitigação de riscos", "eliminação de riscos", "prevenção de riscos"e "redução de riscos".
NOTA 3 O tratamento de riscos pode criar novos riscos ou modificar riscos existentes.

controle

medida que está modificando o risco
NOTA 1 Os controles incluem qualquer processo, política, dispositivo, prática ou outras ações que modificam o risco.
NOTA 2 Os controles nem sempre conseguem exercer o efeito de modificação pretendido ou presumido.

ação de evitar o risco

decisão informada de não se envolver, ou retirar-se de uma atividade, a fim de não ser exposto a um risco específico
NOTA A ação de evitar o risco pode ser baseada nos resultados da avaliação de riscos e/ou em obrigações legais e regulatórios.

compartilhamento de riscos

forma de tratamento de riscos que envolve a distribuição acordada de riscos com outras partes
NOTA 1 Requisitos legais ou regulatórios podem limitar, proibir ou ordenar o compartilhamento de risco.
NOTA 2 O compartilhamento de risco pode ser realizado através de seguros ou outras formas de contrato.
NOTA 3 A extensão em que o risco é distribuído pode depender da confiabilidade e clareza dos acordos de compartilhamento.
NOTA 4 A transferência de risco é uma forma de compartilhamento de risco.

financiamento de riscos

forma de tratamento de riscos que envolve arranjos contingentes para a provisão de fundos, a fim de atender ou modificar eventuais consequências financeiras, caso ocorram

retenção de riscos

aceitação do benefício potencial de ganho, ou do ônus da perda, a partir de um risco específico
NOTA 1 A retenção de riscos inclui a aceitação de riscos residuais.
NOTA 2 O nível de risco retido pode depender dos critérios de risco.

risco residual

risco remanescente após o tratamento do risco
NOTA 1 O risco residual pode conter riscos não identificados.
NOTA 2 O risco residual também pode ser conhecido como "risco retido".

resiliência

capacidade adaptativa de uma organização em um ambiente complexo e de mudanças

monitoramento

verificação, supervisão, observação crítica ou identificação da situação, executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado
NOTA O monitoramento pode ser aplicado à estrutura da gestão de riscos, ao processo de gestão de riscos, ao risco ou aos controles.

análise crítica

atividade realizada para determinar a adequação, suficiência e eficácia do assunto em questão para atingir os objetivos estabelecidos
NOTA A análise crítica pode ser aplicada à estrutura da gestão de riscos, ao processo de gestão de riscos, ao risco ou aos controles.

reporte de riscos

forma de comunicação destinada a informar partes interessadas específicas, internas ou externas, fornecendo informações relativas ao estado atual do risco) e a sua gestão

registro de riscos

registro de informações sobre riscos identificados
NOTA O termo "risk log"é algumas vezes utilizado no lugar de "registro de risco".

perfil de risco

descrição de um conjunto qualquer de riscos
NOTA O conjunto de riscos pode conter riscos que dizem respeito a toda a organização, parte da

organização, ou referente ao qual tiver sido definido.

auditoria de gestão de riscos
processo sistemático, independente e documentado para obter evidências e avaliá-las de maneira objetiva, a fim de determinar a extensão na qual a estrutura da gestão de riscos, ou qualquer parte sua selecionada, é adequada e efetiva

Instrução Normativa GSI N^o 1 (BRASIL, 2008a)

Política de Segurança da Informação e Comunicações
documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

Segurança da Informação e Comunicações
ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

disponibilidade
propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

integridade
propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

confidencialidade
propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

autenticidade
propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Gestão de Segurança da Informação e Comunicações
ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento,

segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

quebra de segurança
ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

tratamento da informação
recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Norma Complementar n^o 04/IN01/DSIC/GSIPR (BRASIL, 2013)

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

Análise de riscos
uso sistemático de informações para identificar fontes e estimar o risco;

Análise/avaliação de riscos

processo completo de análise e avaliação de riscos;

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

Avaliação de riscos
processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco;

Comunicação do risco
troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;

Estimativa de riscos

processo utilizado para atribuir valores à probabilidade e consequências de um risco;

Evitar risco
uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco;

Gestão de Riscos de Segurança da Informação e Comunicações
conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

Identificação de riscos
processo para localizar, listar e caracterizar elementos do risco;

Reduzir risco
uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco;

Reter risco
uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

Riscos de Segurança da Informação e Comunicações
potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

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

Tratamento dos riscos
processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

Vulnerabilidade

conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.