UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
ESPECIALIZAÇÃO EM INFORMÁTICA: ÁREA DE CONCENTRAÇÃO: GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

Henrique Alcântara Veloso Mota

METODOLOGIA PARA GESTÃO DE RISCOS NOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO NA FUNDAÇÃO NACIONAL DE SAÚDE

Brasília
2020

HENRIQUE ALCÂNTARA VELOSO MOTA

METODOLOGIA PARA GESTÃO DE RISCOS NOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO NA FUNDAÇÃO NACIONAL DE SAÚDE

Monografia apresentada ao Curso de Especialização em Informática - Área de Concentração: Gestão de Tecnologia da Informação, ofertado pela Escola Nacional de Administração Pública, ENAP, em parceria com a Universidade Federal de Minas Gerais, UFMG, como parte dos requisitos necessários à obtenção do título de Especialista.

Orientador: Prof. Dr. Jeroen van de Graaf

Brasília
2020

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa
CRB 6ª Região nº 1510

Mota, Henrique Alcântara Veloso

M917m Metodologia para gestão de riscos nos ativos de tecnologia da informação na fundação nacional de saúde. / Henrique Alcântara Veloso Mota – Brasília,2020.
x, 63 f., il.

Monografia (especialização) – Universidade Federal de Minas Gerais. Departamento de Ciência da Computação.

Orientador: Jeroen van de Graaf

1.Computação. 2. Segurança da informação 3. Gestão da informação. 4. Lei de proteção de dados. I. Orientador. II. Título

CDU 519.6*

UNIVERSIDADE FEDERAL DE MINAS GERAIS

INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
ESPECIALIZAÇÃO EM INFORMÁTICA: ÁREA DE CONCENTRAÇÃO GESTÃO EM TECNOLOGIA DA INFORMAÇÃO

Metodologia para Gestão de Riscos nos Ativos de Tecnologia da Informação na Fundação Nacional de Saúde

HENRIQUE ALCANTARA VELOSO

Monografia apresentada aos Senhores:

Prof. Jeroen Antonius Maria van de Graaf
Orientador
DCC - ICEx – UFMG

Prof. José Nagib Cotrim Árabe
DCC - ICEx - UFMG

Prof. José Marcos Silva Nogueira
DCC - ICEx - UFMG

Belo Horizonte, 09 de junho de 2020

RESUMO

Este trabalho apresenta alternativas para minimizar a possibilidade da ocorrência de impactos sobre os ativos de TI com uma maneira simplificada de aplicação da metodologia a ser proposta pode ser utilizada em qualquer projeto de Gestão de Riscos de Segurança da Informação e Comunicações, sempre que se desejar uma avaliação dos riscos aos quais estão expostos os ativos envolvidos (pessoas, processos, tecnologia e ambientes), que exijam maior detalhamento dos levantamentos a serem realizados, independentemente do escopo, do mais simples ao mais complexo. A Metodologia para Gestão de Riscos nos Ativos de Tecnologia da Informação foi desdobrando-se por meio de um planejamento que envolve tratamento, monitoramento e controle de riscos, identificando e direcionando esses tratamentos de acordo com os tipos de riscos, entendendo ainda que algumas oportunidades podem surgir e com elas pode-se trabalhar para aprimoramentos, melhorias, ganhos, dentre outros impactos positivos.

Palavras-chave: Gestão de Riscos, Segurança da Informação e Comunicações, ativos de TI, Metodologia, avaliação dos riscos.

ABSTRACT

This work presents alternatives to minimize the possibility of impacts on IT assets with a simplified way of applying the methodology to be proposed. It can be used in any Information and Communications Security Risk Management project, whenever a assessment of the risks to which the assets involved (people, processes, technology and environments) are exposed, which require greater detail of the surveys to be carried out, regardless of the scope, from the simplest to the most complex. The Methodology for Risk Management in Information Technology Assets has been unfolded through planning that involves treatment, monitoring and control of risks, identifying and directing these treatments according to the types of risks, also understanding that some opportunities may arise and with them one can work for improvements, improvements, gains, among other positive impacts.

Keywords: Risk Management, Information and Communications Security, IT assets, Methodology, risk assessment.

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
CGMTI	Coordenação Geral de Modernização e Tecnologia da Informação
DEADM	Departamento de Administração
DSIC	Departamento de Segurança da Informação e Comunicações
ETIR	Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais
FUNASA	Fundação Nacional de Saúde
GRSI	Gestão de Riscos e Segurança da Informação
GSI	Gabinete de Segurança Institucional
ISO/IEC	*International Organization for Standardization / International Electrotechnical Commission*
NBR	Norma Técnica Brasileira
NIST	*National Institute of Standards and Technology*
PDCA	*Plan-Do-Check-Act*
PDTI	Plano Diretor de Tecnologia da Informação
PSR	Probabilidade, Severidade e Relevância
SGSI	Sistemas de Gestão de Segurança da Informação
TCU	Tribunal de Contas da União
TI	Tecnologias da Informação

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O crescente esforço dos órgãos de controle para o aumento da gestão de risco em ativos de Tecnologias da Informação (TI) na Administração Pública Federal (APF) tem apresentado cada vez mais abordagens de boas práticas para a gestão de TI por meio de leis, normas técnicas e modelos internacionais.

A falta de maturidade em gestão de riscos de TI contribui para a ocorrência de situações indesejadas, tais como:

> Priorização de investimentos em TI que não estejam alinhados às necessidades do negócio, riscos em ativos de TI que não são adequadamente identificados e tratados, ausência de políticas de continuidade de negócio aplicadas a TI, aquisições em desconformidade com a legislação aplicável, indisponibilidade de serviços públicos providos com uso de TI, falhas de segurança da informação, entre outros (Tribunal de Contas da União (TCU,) 2014).

Em regulamentações recentes do TC), existem inúmeras recomendações acerca das práticas de governança e segurança de TI no que se refere ao planejamento estratégico, a implantação de Comitê de TI e Comitê de Segurança da Informação, a gestão de pessoal de TI, a gestão de riscos de TI e a gestão orçamentária de TI (TCU, 2014).

Tais esforços surgem como estratégias na busca de um maior controle e direcionamento dos gastos de TI nos órgãos da APF. Além disso, a TI deve criar valor para a organização alinhando-se à sua missão institucional, pois a criação de valor é definida pela entrega de benefícios por meio do uso otimizado dos recursos disponíveis e pelo gerenciamento dos riscos existentes.

As normas de segurança da informação de TI na Funasa (Fundação Nacional de Saúde) seguem o roteiro estabelecido na Instrução Normativa GSI nº 1, de 13 de junho de 2008 e suas Normas Complementares, instruídos pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR) por intermédio do Departamento de Segurança da Informação e Comunicações (DSIC). As referidas normas complementares tratam das diretrizes e disciplina como a Metodologia de Gestão de Segurança da Informação, elaboração de Política de Segurança da Informação, criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR), Gestão de Continuidade de Negócios, entre outros.

A etapa de Análise de Riscos, na Funasa, segue o padrão disciplinado pela

Norma Complementar nº 04/IN01/DSIC/GSIPR. A identificação dos riscos é feita de maneira abrangente, sem a especificação de critérios objetivos e controles internos. Acerca dos riscos de TI na Funasa, atualmente, somente o principal sistema é gerenciado por meio de políticas de segurança da informação.

Não há uma previsão de ampliação do escopo de análise, construção de uma base de conhecimentos ou criação de controles sobre as possíveis ameaças e vulnerabilidades de sistemas não analisados.

O desenvolvimento de técnicas e metodologias em gestão de riscos de TI na Funasa pode se tornar um exemplo a ser adotado por outros órgãos da APF, que utilizem dos mesmos procedimentos para as gestões de riscos de TI. A principal contribuição do presente trabalho é a possibilidade de aumento da maturidade da gestão de riscos de TI na Funasa e, como consulta aos demais órgãos da APF, pois a identificação de riscos é procedimento crítico para uma boa prestação de serviço de TI e garantia na continuidade destes serviços.

Os serviços de TI na Funasa são vitais institucionalmente, pois compõem os objetivos estratégicos definidos pelo Órgão. Um planejamento alinhado com uma adequada identificação de riscos poderá reduzir ameaças e otimizar a prestação dos serviços.

A governança de TI tem uma relação conceitual muito forte com a gestão de riscos, por isso, o foco da governança na Funasa é garantir a conformidade com a legislação e diretrizes estratégicas de TI definidas pelo Governo Federal.

O acompanhamento constante dos riscos de TI na Funasa é estratégico, a utilização da metodologia a ser proposta apoiará o gerenciamento de ameaças e vulnerabilidades, oferecendo maior controle dos riscos identificados com o suporte de um material de referência direcionado aos profissionais que atuam na gestão de TI da referida Fundação.

Este trabalho apresenta alternativas para minimizar a possibilidade da ocorrência de impactos sobre os ativos de TI com uma maneira simplificada de aplicação para não comprometer mais esforço de recurso humano dedicado, devido a dificuldade atual na Funasa.

2 DEFINIÇÕES PARA SEGURANÇA RELACIONADA À INFORMAÇÃO

A Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) apresenta-se como referencial teórico para composição da base para o Estudo de Caso aqui proposto. O objetivo deste capítulo é reunir conceitos e definições pertinentes a temática da Segurança da Informação, classificação da informação e os aspectos inerentes a Segurança da Informação, construindo um quadro que apresenta sua importância. Outras questões serão tratadas para contextualizar os desdobramentos acerca do significado e papel da Segurança da Informação.

2.1 VISÃO GERAL

A classificação que Boran (1996) faz a respeito de informações é dividida em níveis baseados em prioridades e considerando-se a necessidade inerente a cada organização ou empresa, acreditando que a classe de informações importa para manutenção das atividades que envolvem os processos que ocorrem nas empresas. Abaixo estão descritas cada classe de informações que os autores definem:

- **Pública**: aquelas informações que podem apresentar-se publicamente sem oferecer grandes consequências à organização;
- **Interna**: informação cujo acesso deve ser limitado, ou o acesso livre deve ser evitado. Possíveis consequências derivadas do uso não autorizado não se apresentam sérias, porém, a integridade desse tipo de informação importa, mesmo não sendo vital para a empresa;
- **Confidencial**: informações confidenciais de porte restrito aos limites da organização. A divulgação pode provocar perdas ou desequilíbrio das operações ou perdas financeiras, podendo também prejudicar a confiança dos clientes;
- **Secreta**: informação que possui criticidade para as operações e atividades da empresa. Sua integridade necessita ser preservada e seu acesso é bastante restrito, apresentando limite de algumas pessoas na empresa. Neste sentido, trata-se de informação vital à organização.

Segurança da Informação trata-se da área que possui conhecimento direcionado à proteção dos ativos relacionados a informação, protegendo as informações de acessos indesejados ou não autorizados, além de proteger contra alterações ou mudanças indevidas ou mesmo da sua indisponibilidade. Ativos podem

ser pessoas, recursos, serviços, produtos e/ou bens que uma organização ou empresa utiliza para gerar receitas (SÊMOLA, 2003).

Os ativos necessitam de grande segurança, no entanto, a segurança muitas vezes é tratada como questão superficial por parte de muitas organizações. A importância, nestes casos, não é devidamente dada as estratégias para segurança, utilizando-se técnicas de maneira parcial ou de capacidade incompleta, aumentando a vulnerabilidade (NAKAMURA; GEUS, 2007).

O aumento do uso e interesse na tecnologia de computadores abre espaço nos ambientes de escritórios, chegando a qualquer lugar do mundo por meio da usabilidade de dispositivos, especialmente daqueles considerados móveis ou portáteis, utilizando ainda rede mundialmente conectada: a internet (SÊMOLA, 2003).

Internet e Segurança da Informação evoluíram, deixando de pertencer apenas a área de TI, em que a preocupação permeava a necessidade de um sistema de antivírus ou um *firewall* cheio de configurações, assim, necessitando de desenvolvimento de equipes mais preparadas, uma gestão mais específica e investir em processos mais avançados. Segurança da Informação é uma temática amplamente discutida por vários especialistas. Possivelmente, pode-se afirmar que nada está em total segurança (GABBAY, 2003).

2.2 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios básicos para Segurança da Informação, como descrevem Albuquerque (2002) e Krause (1999), são definidos em três principais, sendo:

- **Confidencialidade**: o acesso à informação é dado a pessoas com explicitude para autorização, esta é a proteção dada de sistemas de informação com intuito de impedir acesso de pessoas não autorizadas;
- **Disponibilidade**: a disponibilidade diz respeito a informação estar exposta quando necessário;
- **Integridade**: a recuperação da informação deve ser realizada de forma íntegra, quando ocorrer seu armazenamento. Assim, Figura-se a proteção de dados e das informações contra ações que possam modificá-las de maneira intencional ou acidental, sendo não autorizadas.

Considera-se vulnerabilidade, defeitos ou fraquezas em aspectos ou componentes ligados a informação ou ao sistema de informação, considerando

procedimentos e controle de segurança relacionadas ao sistema, podendo ser intencional ou acidental, explorando e influenciando em aspectos de confidencialidade, de integridade ou no aspecto de disponibilidade (WEILL e ROSS, 2006).

Portanto, questões que envolvem vulnerabilidade precisam ser investigadas e tratadas como questões prioritárias podendo acarretar prejuízos, caso sejam manipuladas por pessoas de intenções duvidosas ou más.

2.3 AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

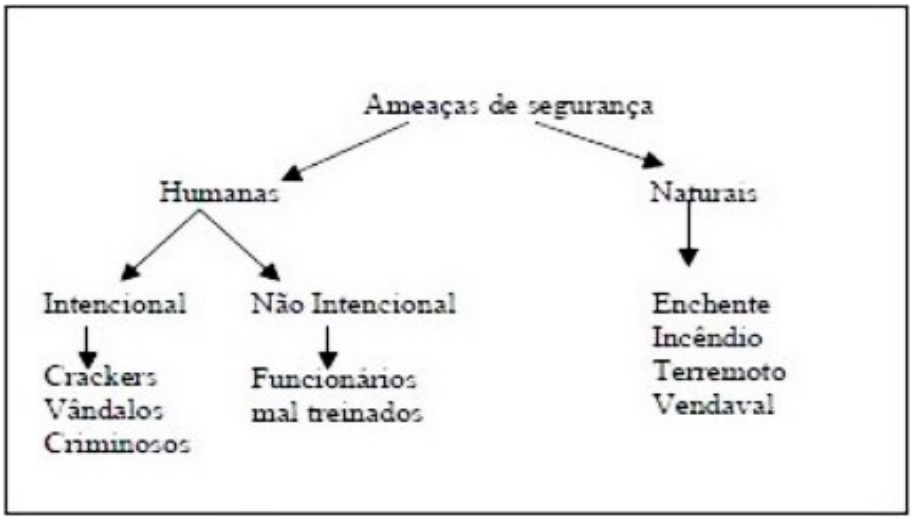
Sêmola (2003) define ameaças como condições ou agentes que podem causar situações ou incidentes comprometedores a informações e também a seus ativos, explorando vulnerabilidades, redução da confiabilidade e prejuízos aos outros principais aspectos inerentes à Segurança da Informação, como integridade e a disponibilidade, permitindo impactos aos negócios da empresa ou da organização.

Deste panorama, reflete-se sobre as questões importantes que figuram a composição e ameaças à Segurança da Informação, como destacar quais condições são de fato nocivas e quais são oportunidades ou precursoras dessas. Ainda refletindo sobre ameaças na composição dos riscos que as informações correm, pode-se destacar que as más intenções de pessoas são grandes ocasionadoras de danos e prejuízos aos aspectos supracitados.

2.4 TIPOS DE AMEAÇAS

Para compor um quadro mais claro dos tipos de ameaças contribuindo com os direcionamentos e decisões, as ameaças são divididas em humanas e naturais, como ilustra a Figura 1. A natureza humana das ameaças deriva-se de atitudes intencionais, sendo estas provocadas propositalmente. As ameaças humanas também podem ser não intencionais, podendo surgir do mau treinamento ou falhas, por exemplo.

Figura 1: tipos de ameaças



Fonte: (SÊMOLA, 2003)

A Figura 1 traz alguns tipos de ameaças mais recorrentes. Importa salientar que a imagem apresenta como principais ameaças humanas alguns perigos comuns que rondam as empresas e organizações, como criminosos virtuais. Não é simples controlar as intenções de variadas pessoas, pois cada indivíduo possui suas motivações e convicções, no entanto, reconhecer essas ameaças, principalmente em caráter preventivo, pode significar neutralização de efeitos negativos dessas ameaças à empresa.

Ainda sobre a exposição na Figura 1, os funcionários mal treinados podem apresentar ameaças à medida em que não atendem as necessidades da organização, não compreendem as nuances e as atividades que possibilitam a funcionalidade da empresa. Assim, pode ocorrer, mesmo que não intencionalmente, exposição de informações confidenciais, disponibilização errônea, confiabilidade reduzida, integridade diminuída, dentre outros prejuízos. As ameaças provocadas por desastres naturais podem apresentar prejuízos de larga escala não somente a uma determinada organização, mas a várias simultaneamente e a longo prazo.

2.5 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Objetivamente, a Política de Segurança da Informação desempenha a função de fornecimento de orientações e apoio para Gestão de Segurança da Informação e ainda sobre os requisitos relacionados aos negócios e as regulamentações legislativas pertinentes. A política dada pela gerência deve ser clara e concisa, acordando com os objetivos propostos pelo negócio, demonstrando apoio e

compromisso com a segurança da informação observando a manutenção das políticas de segurança de forma que atinja a todos da organização (NBR ISO/IEC 27002, 2005).

Atribuídos à Política de Segurança da Informação têm-se os direitos e responsabilidades das pessoas que desempenham funções e lidam com os recursos de TI da empresa ou organização, sendo as tratativas quanto as informações de uma instituição importantes para sua sobrevivência e permanência no mercado, pois nelas encontram-se armazenadas. A boa Política de Segurança da Informação oferece a prevenção por meio de ações na rede da instituição, considerando o que poderá ou não ser inaceitável. Sobretudo, o que estiver fora da política pode ser considerado incidente de segurança. Além disso, na política encontram-se as penalidades a serem direcionadas aos que a descumprirem (NBR ISO/IEC 27002, 2005).

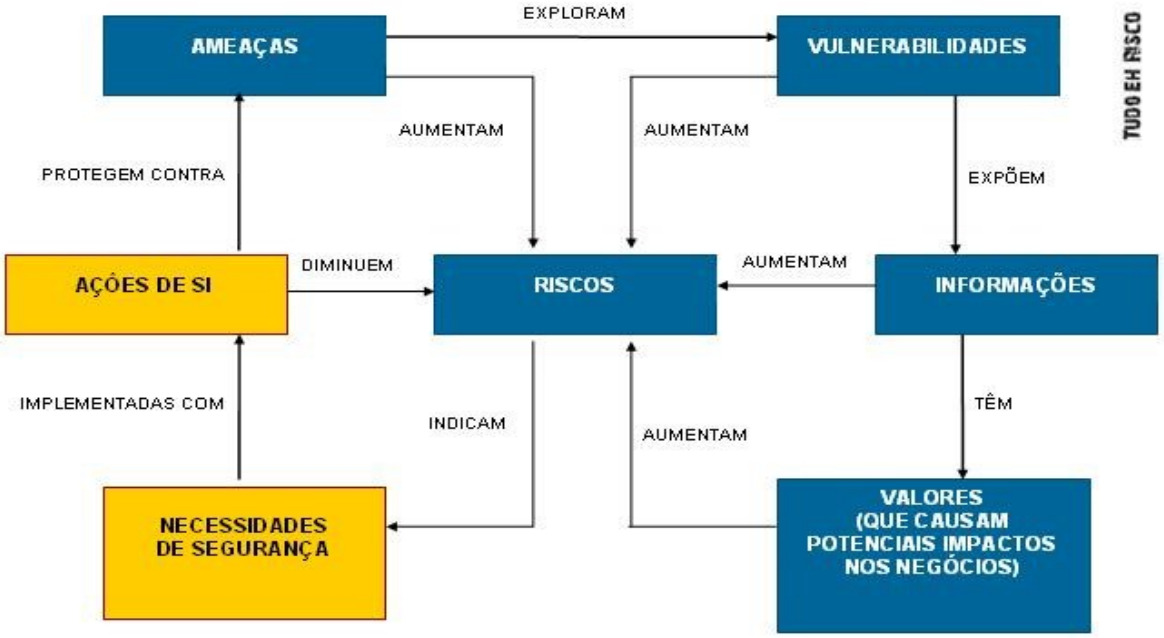
Obviamente a Segurança da Informação encontra-se intimamente ligada à boa gestão dessa segurança. Neste sentido, as leis que permeiam essa área auxiliam na promoção das ações a serem tomadas e direcionadas, clarificando aos gestores quais caminhos são viáveis, bem como, orientam na formulação de políticas. Ora, seriam as políticas aquelas que determinam e delimitam até onde as ações podem chegar no tocante aos negócios da organização, empresa ou instituição, respeitando requisitos de recursos, mercado, dentre outros tantos, sempre observando a segurança das informações que possuem, especialmente no que remete ao atendimento íntegro e de qualidade.

Portanto, a Política de Segurança de cada instituição parte das leis vigentes, construindo um quadro do qual todos os colaboradores devem inteirar-se, compreendendo como avaliar as situações e determinar o que é ameaça ou oportunidade, aumentando as chances de sucesso e de acertos.

2.6 AVALIAÇÃO DE RISCOS

Risco pode ser definido como a probabilidade de ameaças à medida em que explora as vulnerabilidades, causa perdas de requisitos como confidencialidade, integridade e disponibilidade, prejudicando e provocando prejuízos e impactos na instituição. Medidas relacionadas à segurança podem reduzir impactos negativos, proteger os negócios, pois é nas informações, alvo dos requisitos supracitados, que se encontra a base para funcionamento da organização (SÊMOLA, 2003). A Figura 2 apresenta a composição dos riscos:

Figura 2: composição do risco



Ciclo da Segurança da Informação - ISO/IEC 13335-1:1998

Fonte: (ISO/IEC 27002, 2005)

Como apresentado na Figura 2, os riscos podem figurar-se de várias maneiras. Em algumas situações, os riscos podem sujeitar a instituição a oportunidades que devem ser estudadas e tratadas da melhor maneira para que o impacto possa gerar benefícios. Importa destacar que as ameaças podem significar prejuízos, mas as oportunidades podem significar diferenciais para a instituição destacar-se no mercado e aumentar sua qualidade de atendimento e oferta de produtos e serviços. Neste viés, a Segurança da Informação com suas políticas atua fortemente nas análises deste tipo, identificando riscos e avaliando-os.

2.7 A SEGURANÇA FÍSICA

Manter a segurança física significa proteger o ambiente físico de interferências indevidas. De acordo com a norma NBR ISO/IEC 27002:2005 as boas práticas para manter essa segurança auxiliam para impedir o acesso indevido e não autorizado ao ambiente físico e aos serviços nele ocorrentes, valendo-se de meios como barreiras, controles de entrada, dentre outros. Sobre a segurança física a norma clarifica quanto aos aspectos que constroem o conceito de segurança física e de ambiente,

destacando que se trata de um objetivo a impedir acessos físicos não autorizados. Ainda considera danos interferências nas instalações ou informações da instituição.

Neste contexto, medidas e cuidados para segurança devem permear o conceito dado pela norma e soma-se as particularidades e necessidades de cada ambiente. As providências dadas pelas normativas associam-se, portanto, ao bom senso dos gestores quanto aos serviços e processamentos da organização, criando barreiras adequadas e entradas com controle correto. Essas medidas ainda devem ter possibilidades de se dinamizar e adequar de acordo com os riscos identificados. Assim, evita-se perdas, protege-se maquinários, dispositivos e aparelhos, conferindo proteção contra ameaças.

Para que os processos que envolvem os serviços de uma organização sejam realizados de maneira segura é necessário que o ambiente físico proporcione, dentro de seus limites, condições para execução desses processos compreendendo e condicionando meios pelos quais se possa recorrer, caso haja algum incidente, assim como meios para prever incidentes e realizar contenções. Como manter informações seguras se não há seleção de pessoas e ferramentas para adentrar no ambiente físico da instituição? Existem ameaças que utilizam brechas nos recursos automatizados, mas partindo da reflexão que as piores ameaças derivam das más intenções humanas, o acesso por meio do ambiente físico pode ser perigoso e significar grandes riscos que apresentem impactos negativos e prejuízos.

2.8 GESTÃO DE RISCOS

A identificação de riscos torna-se necessária à medida em que é preciso especificar ameaças e vulnerabilidades, afetando a segurança dos sistemas de informação incluindo todo seu ciclo de vida (HAMPSHIRE e TOMIMURA, 2004).

Implementar metodologias de avaliações dos riscos exige identificação de ativos, de ameaças, de vulnerabilidades e também de riscos, objetivando avaliar e selecionar medidas de segurança para reduzir riscos e implementação de medidas de segurança (VELLANI, 2006).

2.9 SEGURANÇA DA INFORMAÇÃO E SUA IMPORTÂNCIA DENTRO DA AMBIENTE COORPORATIVO

Em todo o mundo as questões que envolvem os incidentes de segurança têm sofrido aumento, destacando-se os ataques de hackers, invadindo inúmeras áreas, exacerbando os ambientes empresariais. A Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nas empresas brasileiras - TIC Empresas 2017(NIC.BR / CETIC.BR, 2018) , destaca que fortalecer a confiança em serviços digitais é um ponto crítico para a adoção da banda larga e o compartilhamento de dados. A Indústria 4.0 também cria riscos que podem corroer os benefícios percebidos nas tecnologias digitais. Apesar de serem difíceis de mensurar, os incidentes de segurança digital parecem estar aumentando quanto à sua sofisticação, frequência e influência. Esses incidentes afetam a reputação e a competitividade das empresas, bem como impõem custos significativos para a economia como um todo. A preocupação com a segurança digital e a privacidade restringe a adoção das TIC e as oportunidades de negócios. Especificamente, as pequenas e médias empresas precisam introduzir ou melhorar suas práticas de gestão de riscos e segurança digital.

As empresas tornaram-se dependentes da tecnologia e seus avanços, sobretudo, essa dependência tem aumentado ao longo do tempo. Uma das questões mais emergentes desse crescimento diz respeito ao aumento também da vulnerabilidade e disposição a fraudes. As organizações e empresas possuem processos inerentes à produtividade e oferta de serviços, contando com componentes e atores como clientes, colaboradores, acessibilidade a internet, informações e dados de classificação em vários níveis, configurando pontos críticos de interesse a indivíduos mal-intencionados.

3 NORMAS ABNT NBR ISO/IEC DA SÉRIE 27000 (ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005)

3.1 ABNT NBR ISO/IEC 27001

A ISO/IEC 27001 trata da norma destinada à substituição da norma BS7799-2, referente a certificação de sistema de Gestão de Segurança da Informação. A norma objetiva em suas providências um modelo para estabelecer melhorias em Sistemas de Gestão de Segurança da Informação (SGSI), além de monitoramento, implementação, operação, revisão e manutenção de um SGSI.

A decisão para adoção de um Sistema de Gestão de Segurança da Informação configura ação estratégica e sua implementação ocorre mediante influências de suas próprias necessidades e também objetivos, considerando ainda os aspectos exigidos para segurança, processos e estrutura da instituição (NBR ISO/IEC 27001, 2006).

Segundo a norma NBR ISO/IEC 27001, a aplicação de um sistema de processos dentro de uma organização junto com a identificação e interação destes processos e sua gestão, pode ser chamada de “abordagem de processo”. A abordagem de processo para a gestão da segurança da informação apresentada nesta norma encoraja que seus usuários enfatizem a importância de:

- Compreensão dos requisitos inerentes a segurança da informação, além da necessária política e também seus objetivos;
- Gerenciamento de riscos por meio de implementação e controle por operações de uma instituição, considerando riscos como um conceito relacionado à segurança da informação de maneira global dentro da organização;
- Monitoramento e realização de revisão dos aspectos que permeiam o desempenho e condições efetivas do SGSI;
- Continuidade de melhorias observando as medidas objetivas.

A NBR ISO/IEC 27001 possui processo de modelagem seguindo o *Plan-Do-Check-Act* (PDCA), sendo este modelo utilizado para construir a estrutura dos processos que fazem parte do Sistema de Gestão de Segurança da Informação.

Um Sistema de Gestão em Segurança da Informação acata os requisitos inerentes a Segurança da Informação, assim como as expectativas das partes interessadas. As ações relacionadas às considerações sobre requisitos necessários

aos processos de segurança desenvolvidos trazem resultados quanto ao atendimento desses requisitos e expectativas. Assim, o SGSI tem sua projeção fundamentada em assegurar as escolhas para controle de segurança de maneira adequada, protegendo ativos e dando confiança aos usuários quanto a segurança de informações (NBR ISO/IEC 27001, 2006).

A norma NBR ISO/IEC 27001 desempenha papel de auxiliar no processo de avaliação daquilo que se encontra em conformidade e também do que se encontra como sugestão para melhorias, focando objetivos para controles importantes dado o contexto empresarial.

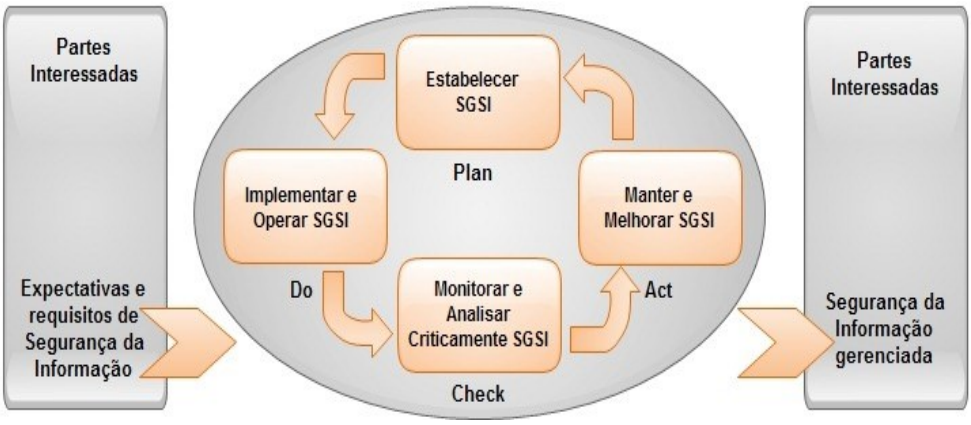
3.1.1 ABNT NBR ISO/IEC 27002

A norma antecessora a 27002, a BS7799, teve início no Governo Britânico e figurou como base para outras normas, como a ISO/IEC 17799, atualmente determinada como ISO/IEC 27002. A norma vigente oferta estrutura que possibilita avaliações de Sistema de Gestão de Segurança da Informação, condicionando as diretrizes e os princípios a serem adotadas por empresas, por governos e organizações empresariais de todo o mundo.

A norma 27002 é descrita e utilizada por vários autores para aplicação de pesquisas na área de TI, especialmente a delimitação de tema sobre segurança da informação, pois trata diretamente sobre providências e premissas para construção das políticas de segurança das instituições. Neste viés, importa destacar que este estudo salienta a norma à medida em que esta fornece condições de boas práticas, orientando pelo caminho correto e de menor risco.

O Planejamento possui um ciclo que a norma 27002 segue e utiliza e, ainda, os ciclos de Execução, Controle e de Ação, conhecidos como PDCA, já mencionados anteriormente. As ações e sequências que compõem o clico PDCA obedecem a ordem das letras da sigla, como ilustrado na Figura 3:

Figura 3: PDCA



Fonte: Associação Brasileira de Normas Técnicas (2006)

A sequência apresentada na Figura 3 trata de uma estrutura básica para composição do ciclo PDCA. Como pode-se observar, o ciclo apresenta 4 fases principais, as quais são definidas de acordo com o NBR ISO/IEC 27002. Sobre a divisão das etapas e fases tem-se:

- *Plan* (Planejar): estabelecer os objetivos e os processos necessários para fornecer resultados de acordo com os requisitos do cliente e políticas da organização. Esta etapa abrange a localização do problema, o estabelecimento de uma meta, a análise do fenômeno (utilizando diagramas estatísticos), a análise do processo (utilizando diagrama de causa e efeito) e a elaboração do plano de ação;
- *Do* (Fazer): implementar os processos, ou seja, execução das ações estabelecidas no plano de ação definidas na fase anterior, sendo realizadas no cronograma determinado, tendo todas as ações registradas e supervisionadas;
- *Check* (Checar): nesta fase deve-se executar a verificação da eficácia das ações executadas na fase anterior, utilizando a comparação dos resultados (planejados e executados), listagem dos efeitos secundários (oriundos das ações executadas), verificação da continuidade ou não do problema (eficácia das ações tomadas);
- *Act* (Agir): esta fase é responsável pela padronização dos procedimentos implantados na fase "*Do*", ou seja, sendo o resultado satisfatório deve-se padronizar essas ações, transformando-as em procedimentos padrão. Para realizar essa padronização é feita a elaboração

ou alteração do padrão, comunicação, treinamento e acompanhamento da utilização. A conclusão do projeto também ocorre nessa fase, sendo que poderão ser estipuladas novas metas futuras para que o processo de melhoria contínua possa ser desencadeado.

Inseridos dentro das 11 seções que fazem parte da estrutura da norma 27002, constituindo-se por categorias relacionadas a segurança da informação, encontra-se 133 controles em que cada uma das categorias tem o objetivo de definição e aplicação que se direciona aos objetivos dos próprios controles, das descrições desses controles, além das diretrizes para implementação e informações adicionais. São as seguintes a seções da norma:

1. Política de Segurança da Informação;
2. Organização da Segurança da Informação;
3. Gestão de Ativos;
4. Segurança em Recursos Humanos;
5. Segurança Física e do Ambiente;
6. Gestão das Operações e Comunicações;
7. Controle de Acesso;
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
9. Gestão de Incidentes de Segurança da Informação;
10. Gestão da Continuidade do Negócio;
11. Conformidade

Seguindo o exposto sobre a norma 27002, compreende-se, portanto, que suas diretrizes e seções auxiliam na elaboração da Política de Segurança da Informação de cada instituição, utilizando a norma para construção da principal estrutura dessas políticas, mas também considerando que cada organização possui necessidades específicas para alcançar objetivos e desenvolver suas funções e papeis com qualidade e sucesso.

3.1.2 ABNT NBR ISO/IEC 27005

A NBR ISO/IEC 27005 traz diretrizes de apoio para Gestão de Riscos e Segurança da Informação (GRSI) das organizações, condicionada ainda a NBR ISO/IEC 27001, porém, não configura uma metodologia específica para este tipo de gestão. A metodologia a ser aplicada pela GRSI é definida pela própria instituição,

considerando seu escopo de Sistema de Gestão de Segurança da Informação, o contexto adotado pelo Gerenciamento de Riscos pelo setor que trata das atividades econômicas. A norma NBR ISO/IEC 27005 exibe vários aspectos que podem ser adequados a diferentes metodologias. Trata-se de uma norma internacional com requisitos necessários para implementação de Sistemas de Gestão e Segurança da Informação.

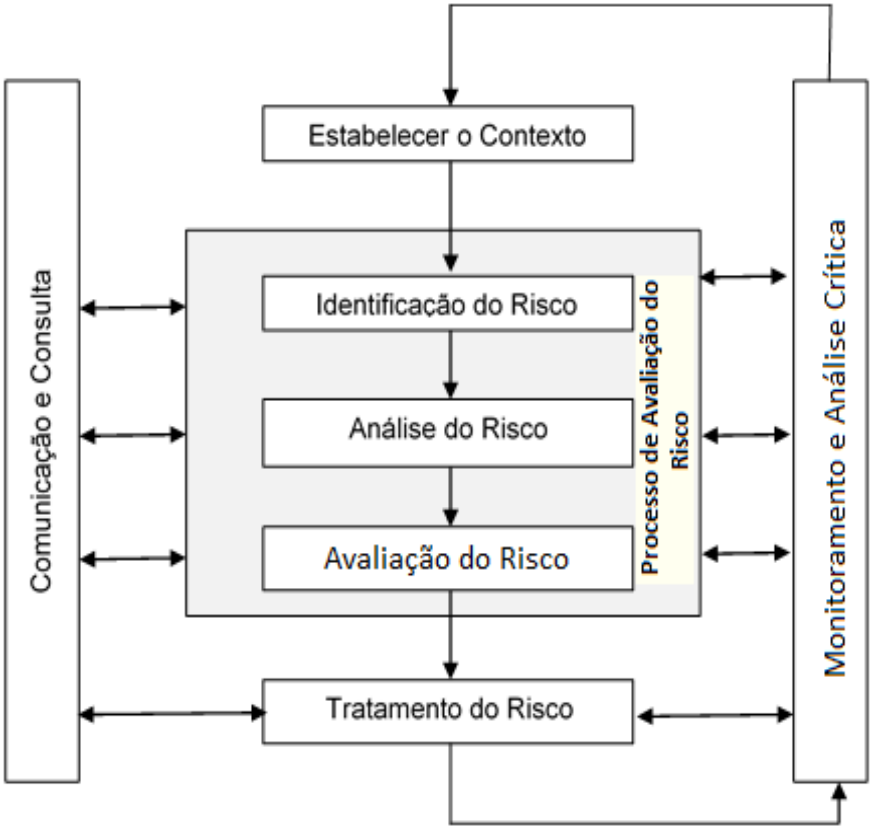
É necessário que a abordagem seja feita de maneira sistemática quanto a gestão de Riscos e Segurança da Informação, buscando a identificação das necessidades da instituição relacionados aos requisitos que a Segurança da Informação possui, criando assim, um sistema eficaz (NBR ISO/IEC 27005, 2008).

As contribuições previstas pela NBR ISO/IEC 27005 para Gestão de Riscos de Segurança da Informação são variadas e perpassam por muitos aspectos inerentes a qualidade dessa gestão. As contribuições previstas pela referida norma seguem abaixo:

1. Identificar os riscos;
2. Analisar e avaliar riscos para evitar-se consequências e suas probabilidades;
3. Comunicar riscos e probabilidades;
4. Priorizar riscos para possíveis tratamentos;
5. Priorizar ações a fim de reduzir riscos;
6. Partes interessadas envolvidas com o processo decisório pela Gestão de Riscos e suas informações;
7. Monitorar de forma eficaz os tratamentos de riscos;
8. Analisar e monitorar criticamente e regularmente os riscos e processos de gestão;
9. Coletar as informações para melhorias da abordagem sobre Gestão de Riscos.

Gestão de Riscos de Segurança da Informação trata de um processo aplicado pelas instituições de maneira global ou em áreas específicas, podendo ser uma localidade, um departamento inteiro ou um tipo de serviço, sistemas de informações, controles, planejamentos ou particularidades, como planos de continuidade (NBR ISO/IEC 27005, 2008).

Figura 4: processos GRSI



Fonte: (ISO/IEC 27002, 2005)

A Figura 4 apresenta o processo que decorre da Gestão de Riscos de Segurança da Informação por meio de atividades de análises, avaliações, tratamentos de riscos, podendo ainda ocorrer mais de uma vez. Existe a característica de interação entre esses processos para execução da análise e avaliações de riscos, tornando possível o aprofundamento em cada repetição. Assim, a interação pode minimizar tempo e esforço nas identificações dos controles, assegurando ainda a avaliação de riscos que podem gerar grandes impactos (ISO/IEC 27005, 2005).

Segundo o descrito acima, existe uma ordem para as atividades de GRSI considerando a execução de análises e avaliações como a primeira atividade. Assim, pode-se obter informações necessárias para determinação de ações para redução dos riscos de maneira aceitável, dessa forma, a tarefa estará completa e o tratamento pode ocorrer. Essa ordem no processo evita a insuficiência de informações, no entanto, se essa insuficiência ocorrer outra interação poderá ser executada, analisando e avaliando novamente, revisando o contexto.

3.2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Seguindo o que prevê a norma 27002, a Política de Segurança da Informação compreende as orientações necessárias para apoio da Gestão de Riscos e Segurança da Informação, assim como da alta direção, acordando com os requisitos de negócios, amparando-se nas leis e regulamentos das normativas pertinentes.

Para a segurança da informação alguns itens são importantes dentro das instituições, como uma boa e eficaz Política de Segurança da Informação e a gestão para suportes adequados, seguindo ainda o nível de medidas para conscientização dos colaboradores (ASCIUTTI, 2012).

A política de segurança demanda atribuições às partes pertinentes, como direitos e responsabilidades ao pessoal que deve lidar com recursos computadorizados da instituição e as informações neles guardadas. Essa política ainda define determinado conjunto de normas, além de procedimentos e métodos a serem utilizados na prática da manutenção da segurança da informação, formalizando e divulgando aos usuários a usabilidade dos ativos de informações (FERREIRA e ARAÚJO, 2008).

Assim, elaborar a Política de Segurança obedece a algumas importantes fases:

1. Levantar informações para abordagem e entendimento das necessidades, obtendo ainda informações do ambiente de negócios e de tecnologia;
2. Desenvolver o que constará na Política de Segurança;
3. Elaborar os procedimentos inerentes a Segurança da Informação, compreendendo as melhores práticas de mercado.

A Política de Segurança da Informação pode denotar benefícios alcançados por meio dos investimentos nessa política. Alguns dos principais benefícios são maior segurança em processos relacionados ao negócio e minimização de problemas e incidentes relativos a Segurança da Informação. Sumariamente, reflete-se sobre o papel da NBR ISO/IEC 27002 em que são dadas orientações para a criação de boas políticas, ressaltando a importância da consciência quanto ameaças e também como importa preocupar-se com segurança, sobretudo, de informações, mantendo-se devidamente equipados para fornecer apoio as próprias políticas da instituição na execução de suas atividades cotidianas.

Sob este enfoque, os colaboradores da organização devem apropriar-se de conhecimentos sobre a existência da Política de Segurança, ou seja, a política deve existir e alcançar a organização de forma global, pois a tecnologia destinada a proteção necessita da colaboração do elemento humano, especialmente para sua implementação.

3.3 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Complementarmente, a norma NC n° 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009, define gestão de risco de segurança da informação como processos reunidos para identificação e implementação de proteção por meio de medidas necessárias, buscando minimizar ou mesmo eliminar riscos que podem atingir os ativos de informação, objetivando equilibrá-los juntamente com os custos de operações e financeiros.

Torna-se possível com o processo de Gestão de Riscos identificar e realizar a avaliação correta de riscos relacionados a ativos de informações que mantêm o negócio da empresa. Com um processo sistemático de identificação, análise, avaliação, tratamento, comunicação e revisão dos riscos é possível traçar a evolução do nível de risco dos ativos, priorizando desta forma os investimentos e iniciativas para sua redução.

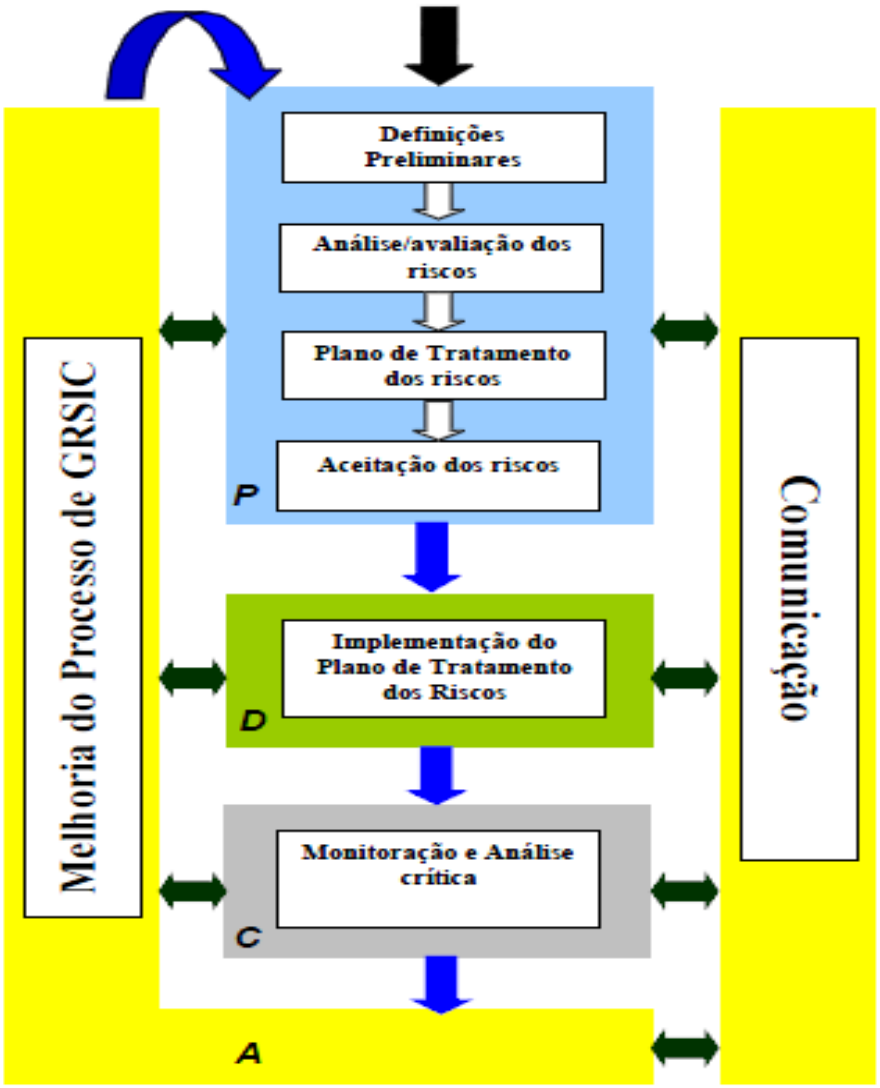
Para que os riscos sejam corretamente tratados, a primeira ação a ser tomada é o conhecimento de forma adequada dos riscos pertinentes às atividades finalísticas da Funasa e o método usado é o processo de Gestão de Riscos. A tabela a seguir, criada na Funasa, resume as atividades relevantes de gestão dos riscos atendendo ao ciclo PDCA do SGSI:

Tabela 1: Atividades de Gestão de Riscos - Funasa

PROCESSO SGSI	PROCESSO DE GRSIC
Plan–P: Planejar (estabelecer o SGSI)	Definir contextos; análise/avaliação, plano de tratamento e aceitação de riscos
DO–D: Fazer (implementar o SGSI)	Implementar plano de tratamento de riscos
Check–C: Checar (monitorar e analisar criticamente o SGSI)	Monitoramento e análise crítica
Act–A: Agir (manter e melhorar continuamente o SGSI)	Comunicação e melhoria do processo de GRSIC

Fonte: (FUNASA, 2017)

Figura 5: gestão de riscos



Fonte: (ISO/IEC 27002, 2005)

Para apoiar o processo de gestão da segurança da informação e comunicações, a Funasa poderá se utilizar de uma solução automatizada de gestão de riscos, baseada no ciclo PDCA, com o foco na melhoria contínua e capacidade para gerenciar o ciclo apresentado, suportando uma metodologia objetiva que auxiliará na efetiva realização de ações, bem como apoiar a tomada de decisão.

Importante ressaltar, que durante a escolha da documentação de apoio, o Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica do *National Institute of Standards and Technology* NIST (2019) não foi considerado por ter sua publicação posterior ao período de elaboração da metodologia. Este guia poderia facilitar o processo, porque seu framework demonstra de maneira simplificada e ilustrativa as fases que o compõem. De qualquer forma, ao selecionar os controles de

segurança foi considerada a *NATIONAL VULNERABILITY DATABASE* do NIST, utilizando controles de baixo, moderado e alto impacto.

3.4 A FUNASA

A Fundação Nacional de Saúde (Funasa), Órgão Executivo vinculado ao Ministério da Saúde, é uma das instituições do Governo Federal responsável pela promoção da inclusão social por meio de ações de saneamento para prevenção e controle de doenças, bem como formular e implementar ações de promoção e proteção à saúde relacionadas com ações estabelecidas pelo Subsistema Nacional de Vigilância em Saúde Ambiental.

a) Missão:

Promover a saúde pública e a inclusão social por meio de ações de saneamento e saúde ambiental.

b) Valores:

Ética;

Equidade;

Transparência;

Eficiência, Eficácia e Efetividade;

Compromisso socioambiental.

Para apoiar o cumprimento de sua missão institucional, a Funasa dispõe de uma infraestrutura tecnológica gerenciada pela Coordenação Geral de Modernização e Tecnologia da Informação (CGMTI), subordinada a um Departamento de Administração (DEADM).

As próximas seções apresentarão como foi a definição e implantação da metodologia de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) da Funasa. Foram usados como base os preceitos preconizados pela IN 04 do GSI, a fim de padronizar o processo de gestão de riscos de segurança da informação e produzir uma fonte de informação capaz de orientar as ações inerentes a esse processo.

4 A METODOLOGIA 1: PLANEJAR

A metodologia a ser proposta pode ser utilizada em qualquer projeto de Gestão de Riscos de Segurança da Informação e Comunicações, sempre que se desejar uma avaliação dos riscos aos quais estão expostos os ativos envolvidos (pessoas, processos, tecnologia e ambientes), que exijam maior detalhamento dos levantamentos a serem realizados, independentemente do escopo, do mais simples ao mais complexo.

Para melhorar o entendimento e a aplicabilidade da metodologia aqui apresentada, as atividades foram ordenadas segundo o ciclo PDCA, conforme preconiza a Norma Complementar NC 04/IN01/DSIC/GRSIC, podendo ser utilizada em sua totalidade ou em parte, conforme as necessidades definidas.

Tabela 2: PDCA

METODOLOGIA DE GESTÃO DE RISCOS E COMUNICAÇÕES			
Planejar	**Fazer**	**Checar**	**Agir**
- Definições preliminares - Análise e avaliação de riscos - Plano de tratamento de riscos - Aceitação dos riscos	Implementação do plano de tratamento de riscos	Monitoramento e análise critica	Comunicação e melhoria do processo de GRSIC

Fonte: (FUNASA, 2017)

4.1 DEFINIÇÕES PRELIMINARES

Nesta fase são levantadas as informações relevantes da organização, avaliados o contexto interno e o externo no qual a organização está inserida, são definidos o escopo e os limites da gestão de riscos, a estrutura, os recursos necessários, as responsabilidades e as autoridades para gerenciar riscos e as diretrizes para sua implementação. Também nesta etapa são definidos os critérios de avaliação, de impacto e de aceitação dos riscos, bem como os registros a serem mantidos. O atendimento a este conjunto de requisitos denomina-se “estabelecer contexto” e este poderá variar de acordo com as restrições impostas.

Em resumo, analisa-se a organização a fim de obter subsídios para o estabelecimento do contexto e estruturação do processo de gestão de riscos,

considerando-se as características e as restrições impostas. Para melhorar o entendimento, abaixo é apresentada a descrição sucinta de alguns dos requisitos mencionados:

- O contexto externo é o ambiente no qual a organização busca alcançar seus objetivos e é importante para assegurar que os objetivos e preocupações das partes interessadas externas sejam consideradas no desenvolvimento dos critérios de risco;
- O contexto interno é o ambiente no qual a organização busca alcançar seus objetivos e é importante que esteja alinhado com a cultura, processos, estrutura e estratégia da organização. Mais especificamente, é algo dentro da organização que poderá influenciar sua maneira de gerenciar riscos;
- O contexto do processo de gestão de risco é composto por objetivos, estratégias, escopo e parâmetros das atividades da organização ou daquelas partes da organização onde será aplicado o processo de gestão de riscos;
- O escopo da gestão de riscos compreende os ativos de informação e os processos de negócio da instituição, visando dar suporte a um SGSI, atender aos requisitos de conformidade legal e evidenciar a execução correta do procedimento;
- Os critérios de impacto devem ser desenvolvidos e especificados em função do montante de danos ou custos à organização causados por um evento relacionado com a segurança da informação, tais como violação da confidencialidade, integridade, disponibilidade e autenticidade, comprometimento da operação, danos a reputação, dentre outros;
- Os critérios para tratamento de riscos são utilizados para avaliar a significância do risco e devem refletir os valores, objetivos e recursos da organização, por isso devem ser compatíveis com a política de gestão de riscos e ser previamente definidos. Alguns destes critérios são requisitos legais ou regulatórios e devem ser atendidos pela organização.

A tabela 3 apresenta os níveis de riscos, as interpretações e quais ações devem ser tomadas:

Tabela 3: Critérios de Tratamento de Riscos

NÍVEL DE RISCO DO PSR	INTERPRETAÇÃO	AÇÃO
Muito alto	Riscos inaceitáveis e os gestores dos ativos devem ser orientados para que os eliminem imediatamente	Tratamento imediato
Alto	Riscos inaceitáveis e os gestores devem ao menos controlá-los	Tratamento necessário
Médio	Riscos que podem ser aceitáveis, no entanto, precisam de revisão e confirmação justificando a não implementação do controle, significando a aceitação do risco	Avaliação e confirmação dos gestores quanto ao tratamento
Baixo	Riscos que podem ser aceitáveis após revisão e confirmação da gestão	Previamente aceitos, mas precisam ainda da confirmação dos gestores e, caso aceitos, devem ser constantemente monitorados
Muito baixo	Riscos aceitáveis, mas devem ser informados à gestão	Aceitos automaticamente, mas com monitoramento constante

Fonte: (FUNASA, 2017)

Esta metodologia estabelece que os riscos classificados como MUITO ALTO e ALTO devem ser tratados até que atinjam os níveis de riscos considerados aceitáveis pela organização e só poderão ser aceitos, formalmente, pela alta direção. O risco, mesmo classificado como BAIXO ou MUITO BAIXO, deverá ser tratado sempre que este afete um ativo vital para o negócio da organização ou ameace algum dos pilares da segurança da informação (Confidencialidade, Integridade, Disponibilidade).

4.2 ANÁLISE/AVALIAÇÃO DE RISCOS

Análise e avaliação de riscos é um processo que consiste em desenvolver a compreensão e identificação dos riscos considerando as ameaças a que está exposto e as vulnerabilidades de um ativo, para estimar seu nível de risco objetivando avaliá-lo e priorizá-lo.

4.2.1 Identificação de Riscos

É um processo usado para localizar, relacionar e caracterizar elementos de risco com o propósito de determinar eventos que possam causar uma perda potencial, identificando onde e porque esta pode ocorrer.

4.2.2 Identificação dos Ativos

Ativos são elementos que possuem valor para a organização e necessitam de proteção, considerando-se o escopo definido. A tabela 4 define as categorias de ativos para a presente metodologia:

Tabela 4: Tipos de ativos

Tipo de ativo	Exemplos de ativos
Processo	Processos referentes a aplicações, gestão, jurídico e normativo
Tecnologia	Equipamentos computacionais e de comunicação, aplicativos, sistema operacional, banco de dados e redes
Pessoa	Servidores públicos, terceiros, diretor, gestor de TI, técnico de TI e usuário final
Ambiente	Ambientes administrativos - escritórios e ambiente de TI

Fonte: (FUNASA, 2017)

O levantamento dos ativos é importante, pois a partir deles é que são consideradas as vulnerabilidades ou ausência de controles em função das ameaças. Nessa etapa, devem ser cadastrados os ativos atribuindo a sua relevância (grau de importância do ativo para o negócio da organização) considerando os sistemas e serviços que ele suporta.

4.2.3 Cálculo de Risco

O nível de risco pode ser calculado de acordo com o índice dado por Probabilidade, Severidade e Relevância (PSR). O índice PSR estabelece definição de risco para cada controle que conste ausência na análise, considerando não somente aspectos de operações que direcionam ao risco, mas também aos impactos que estes riscos podem causar nos negócios da instituição, sendo este aspecto traduzido pela variável relevância.

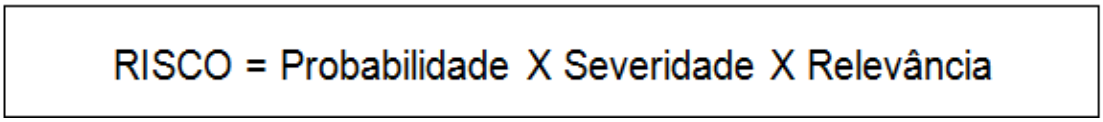
Tabela 5: Componentes do Risco

Variável	Descrição
Probabilidade	Possibilidade da vulnerabilidade ser explorada pela ameaça
Severidade	Consequência da vulnerabilidade ser explorada pela ameaça
Relevância	Grau de importância do ativo para o negócio da empesa, considerando os componentes de negócio que ele apoia

Fonte: (FUNASA, 2017)

Para encontrarmos o valor do risco utilizamos a fórmula da multiplicação das variáveis: Probabilidade, Severidade e Relevância. Para isto, precisaremos nos basear nas tabelas 7, 8 e 9, onde estão estabelecidos os valores e os critérios utilizados.

Figura 6: fórmula de cálculo de risco



Fonte: (ISO/IEC 27002, 2005)

O PSR possui valor de risco que representa certo grau de associação à ausência de controle. Alguns fatores como de probabilidade e de severidade pontuam-se à medida em que as análises técnicas ocorrem, sendo esta relevância considerada a visão do negócio, em termos da importância do ativo para a organização, assim, o risco associado a cada controle ausente é calculado multiplicando-se os três fatores básicos e o resultado são um valores discretos demostrados na Tabela 6, entre 1 (um) e 125 (cento e vinte e cinco), com seu nível variando conforme o resultado desta multiplicação.

Tabela 6: Valor do risco

Nível de risco	**Valores possíveis do PSR**
Muito alto	60, 64, 75, 80, 100, 125
Alto	32, 36, 40, 45, 48, 50
Médio	18, 20, 24, 25, 27, 30
Baixo	8, 9, 10, 12, 15, 16
Muito baixo	1, 2, 3 ,4 ,5 ,6

Fonte: (FUNASA, 2017)

O índice de risco relacionado aos ativos é dado pelo resultado algébrico da soma do PSR dos controles ausentes em seus componentes. Apesar do risco técnico, que é a probabilidade e severidade dos controles não implementados, ser importante para os gestores e para a gestão dos riscos corporativos, o mais importante é sempre considerar o risco ao negócio como fator de priorização das ações de tratamento, pois considera o fator relevante do ativo.

As tabelas abaixo são referência para se estabelecer uma pontuação adequada para cada um dos fatores do PSR:

Tabela 7: Probabilidade

Grau da probabilidade		Probabilidade
5	A ocorrência da vulnerabilidade ser explorada pelas ameaças é quase certa	P > 95%
4	A ocorrência da vulnerabilidade ser explorada pelas ameaças é muito provável	65% < P < 95%
3	A ocorrência da vulnerabilidade ser explorada pelas ameaças é provável	35% < P < 65%
2	A ocorrência da vulnerabilidade ser explorada pelas ameaças é pouco provável	5% < P < 35%
1	A ocorrência da vulnerabilidade ser explorada pelas ameaças é improvável	P < 5%

Fonte: (FUNASA, 2017)

Tabela 8: Severidade

Severidade		Nível da severidade
5	A consequência da vulnerabilidade ser explorada pelas ameaças afetará extremamente a segurança do ativo	Muito alta
4	A consequência da vulnerabilidade ser explorada pelas ameaças afetará muito gravemente a segurança	Alta
3	A consequência da vulnerabilidade ser explorada pelas ameaças afetará gravemente a segurança	Média
2	A consequência da vulnerabilidade ser explorada pelas ameaças afetará pouco a segurança	Baixa
1	A consequência da vulnerabilidade ser explorada pelas ameaças quase não afetará a segurança	Muito baixa

Fonte: (FUNASA, 2017)

Tabela 9: Relevância

Nível qualitativo da relevância	Nível quantitativo da relevância	Relevância
Muito alta	5	Afeta extremamente o negócio da organização, pode abalar toda a Funasa e os prejuízos serão extremamente altos
Alta	4	Afeta muito gravemente a organização, pode afetar um ou mais ativos da Funasa e os prejuízos serão muito altos
Média	3	Afeta gravemente a organização, pode abalar uma parte do negócio da Funasa e os prejuízos serão razoáveis
Baixa	2	Afeta pouco a organização, pode abalar uma parte pequena e localizada do negócio da Funasa e os prejuízos serão baixos
Muito baixa	1	Quase não afeta a organização, pode afetar uma parte muito pequena e localizada do negócio da Funasa e os prejuízos serão desprezíveis

Fonte: (FUNASA, 2017)

4.2.4 Projeto de Análise

Nesta etapa é realizada a análise dos riscos considerando os componentes associados a cada ativo incluídos no escopo. Um componente é o elemento que compõe o ativo e que efetivamente é analisado. Para cada componente existe um questionário associado, uma base de conhecimento contendo um conjunto de controles baseados nas melhores práticas de segurança da informação. Cada controle analisado terá uma das situações descritas abaixo:

Tabela 10: Controles

Situação	Descrição
Implementado	O controle está totalmente implementado no ativo, ou seja, a boa prática é aplicada no ativo
Não Implementado	O controle está parcialmente implementado ou não implementado no ativo, ou seja, a boa prática não existe ou está sendo praticada de forma deficiente
Não aplicável	O controle não se aplica ao contexto da análise. Durante a resposta aos questionários é possível anexar arquivos e embasar a resposta sobre a situação do controle analisado

Fonte: (FUNASA, 2017)

4.2.5 Consolidação da Análise de Riscos Implementada (Relatórios)

A consolidação da análise de riscos se dará por meio de relatórios gerenciais e operacionais que apresentam os resultados dos projetos de análise em formatos de tabelas, gráficos e documentos. Esses resultados são os principais instrumentos a serem utilizados para se realizar a consolidação da etapa de avaliação dos riscos. As tabelas e documentos podem ser gerados do nível técnico até o gerencial, de acordo com a cultura da organização. Os resultados podem ser individuais, referentes a um componente do ativo, ou gerais, consolidando as análises de vários componentes e ativos.

A seguir, seguem os conteúdos dos principais relatórios referentes aos resultados dos projetos de análise de risco.

4.2.6 Relatório Gerencial de Análise de Riscos

Este relatório objetiva demonstrar o resultado final de um determinado projeto ou mesmo um grupo de projetos, podendo ser de análises em termos gerenciais, assim, consolidando-se os riscos identificados na execução do processo.

4.2.7 Relatório Operacional da Análise de Riscos

O Relatório Operacional da Análise de Riscos tem como objetivo orientar o gestor na priorização das recomendações que devem ser atendidas de acordo com o seu nível de risco (PSR). Este relatório deve ser utilizado também como instrumento para a implementação dos controles nos ativos analisados, por conter informações detalhadas sobre como deve ser a implementação dos controles não implementados identificados nas análises, funcionando como base para um plano de ação de tratamento dos riscos residuais.

4.3 TRATAMENTO DE RISCOS

O tratamento de riscos envolve a escolha de uma ou mais opções para mitigar o risco e a implementação dessas opções. Uma vez implementado, o tratamento resultará em novos controles.

Várias opções de tratamento de riscos podem ser consideradas e aplicadas individualmente ou combinadas, sendo que normalmente a utilização de uma combinação delas geram maior benefício. Abaixo, descrevemos as opções de tratamento de riscos:

1. Prevenir os riscos **–** apresenta-se como a forma que trata riscos de maneira que a gestão possa ter iniciativa decisória de não realizar a atividade, objetivando não se envolver ou retirar-se da situação que expõe aos riscos;

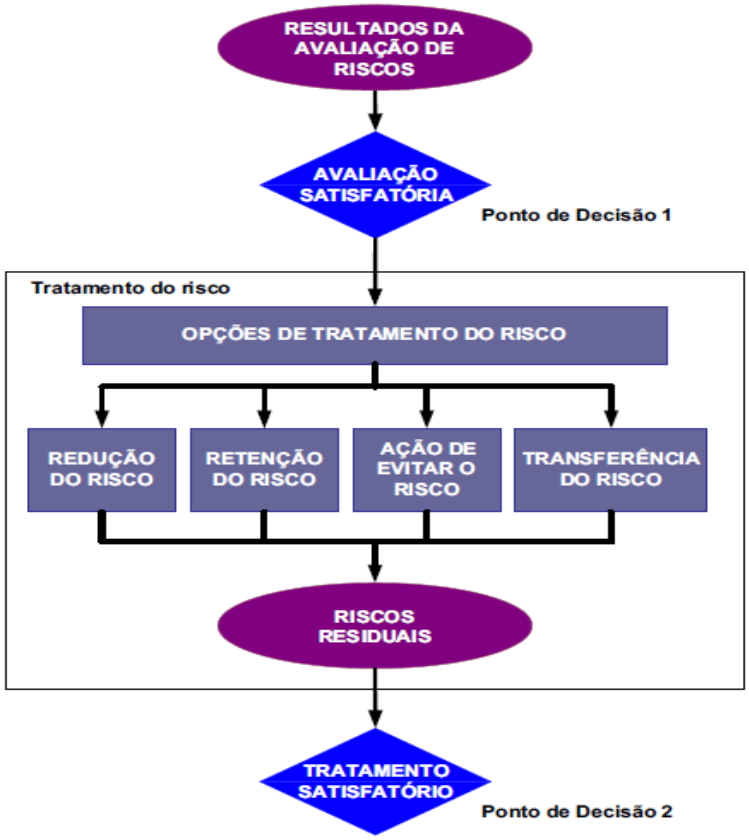
2. Minimização de riscos – apresenta-se como tratamento dos riscos de forma que a gestão tome decisões referentes a realização da atividade, reduzindo por meio de ações a probabilidade de acometimentos de riscos ou de consequências e impactos negativos derivados desses;

3. Aceitar os riscos – apresenta-se como o tratamento dos riscos que a gestão demonstra atitude decisória de realizar a atividade, sobretudo, assumindo responsabilidades caso ocorra o risco que foi identificado;

4. Compartilhamento dos riscos – apresenta-se como tratamento dos riscos que busca ações decisórias pela gestão direcionadas para realização da atividade, compartilhando o ônus relacionado aos riscos com outra entidade.

O tratamento de riscos implica na execução de algumas atividades, como ilustra o fluxograma da Figura 7, conforme estabelece a norma da ABNT NBR ISO/IEC 27005:2005:

Figura 7: atividade de tratamento dos riscos



Fonte: (ISO/IEC 27005, 2005)

Na etapa de tratamento dos riscos devem ser considerados os resultados da etapa de avaliação, a eficácia das ações de segurança da informação já existentes, as restrições organizacionais e técnicas, os requisitos legais e, principalmente, a relação custo/benefício e os recursos necessários para o tratamento (custos, pessoas e prazo).

Existe um planejamento de riscos que gera um plano que deve conter alguns itens e componentes, como registro de tratamentos executados, condicionando-se em atender os requisitos que a Norma Complementar preconizada pelo Gabinete da Presidência da República traz em suas providências, como mostra o modelo da tabela 11:

Tabela 11: requisitos para o plano de tratamento de riscos

Coluna	Descrição
Ativo ou agrupamento	Ativo ou conjunto de ativos
Controle	Descrição do controle a ser adotado para tratar o risco
Tipo de ativo	Ambiente, processo, tecnologia ou pessoa
P	Probabilidade (varia de 1 a 5)
S	Severidade (varia de 1 a 5)
R	Relevância do ativo (varia de 1 a 5)
PSR	Nível de risco (varia de 1 a 5)
Justificativa	Explicação do porquê da necessidade do controle
Recomendação	Forma de implementação do controle
Comentários	Observações incluídas quando da realização da análise (resposta ao questionário) ou justificativa da não implementação do controle (risco aceito)
Prazo	Data prevista de conclusão de implementação do controle
Responsável pelo ativo	Pessoa ou grupo responsável pela implementação dos controles
Situação	Situação do desenvolvimento da ação (não iniciada, em andamento, suspensa, cancelada ou concluída. Se concluída, informar data de conclusão). Nos casos em que não há ação a ser executada, informar a situação de risco aceito. A prioridade para a execução das ações está relacionada ao nível do risco (PSR) e deve estar de acordo com o planejamento definido em cada escopo ou projeto

Fonte: (FUNASA, 2017)

4.4 ACEITAÇÃO DOS RISCOS

Os critérios para a aceitação dos riscos podem apresentar um nível de complexidade maior do que a determinação se o risco residual está ou não abaixo de um limite bem definido.

Em alguns casos, o nível de risco residual pode não satisfazer os critérios de aceitação dos riscos, uma vez que os critérios aplicados não estão considerando as circunstâncias predominantes no momento. Por exemplo, pode ser legítimo

argumentar que é preciso que se aceite o risco porque os custos de sua redução são demasiadamente elevados. Esses casos indicam que os critérios para a aceitação dos riscos são inadequados e devem ser revistos se oportuno, pois nem sempre é possível rever os critérios para a aceitação dos riscos no tempo apropriado.

Nesses casos, os tomadores de decisão poderão aceitar riscos que não satisfaçam os critérios normais para o aceite. Caso isso ocorra o tomador de decisão deve formalmente comentar sobre os riscos e justificar a sua decisão de não acatar os critérios normais para a aceitação. Uma relação de riscos aceitos com uma justificativa para aqueles que não satisfaçam os critérios previamente estabelecidos para aceitação deve ser elaborada, conforme preconiza a norma ANBT NBR ISO/IEC 27005:2005.

5 A METODOLOGIA 2: FAZER, CHECAR E AGIR

5.1 FAZER

É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicação implementará as ações definidas na fase anterior.

5.1.1 Implementação do Plano de Tratamento dos Riscos

A implementação do Plano de Tratamento dos Riscos deve considerar, além das questões técnicas, fatores de negócio e decisões gerenciais. Se ocorrer que em alguma situação o controle não possa ser implementado, então os prazos não serão definidos e este risco será aceito. Os casos em que o controle não pode ser implementado são aqueles referentes à impossibilidade operacional, custo elevado ou falta de orçamento. Portanto, deve ser incluída a justificativa da não implementação do controle no campo “Comentários” e a expressão risco aceito no campo” Situação”.

Uma vez confirmados os controles a serem implementados, são atribuídos os prazos para finalização das implementações. Estes prazos deverão ser adequados ao tamanho e complexidade das ações, considerando-se inclusive os de outros projetos.

O plano de tratamento dos riscos deve ser controlado pelo gestor do escopo, de forma a garantir que o que foi planejado está sendo realizado até o seu encerramento, quando todas as ações forem implementadas ou de alguma forma encerradas. O campo “Situação” deve ser utilizado para incluir a situação da implementação do controle.

O plano deve conter o histórico de acompanhamento, que indica as ações tomadas pelo responsável pelo seu gerenciamento para cada uma das ações. Os riscos aceitos devem ser monitorados e revisados periodicamente.

5.1.2 Controle e Monitoramento das Atividades

Os controles não implementados que configurem riscos inaceitáveis para a organização, podem ser agrupados em tarefas de um Plano de Tratamento de Riscos. Estas tarefas podem ser classificadas como individuais, quando associadas a um único controle ou consolidadas, quando agrupam vários controles.

Para um efetivo controle da implantação do plano de tratamento dos riscos considerados, deverá haver um acompanhamento das atividades por meio de um *workflow* que possibilitará o controle e monitoramento sobre a execução das tarefas de tratamento de riscos.

5.2 CHECAR

É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicação avaliará as ações implementadas na fase anterior.

5.2.1 Monitorar e Analisar Criticamente

Esta fase objetiva a detecção das possíveis falhas de resultados, além de monitorar riscos, possibilitar ações de segurança a serem executadas e proporcionar eficácia do processo que envolve a Gestão de Riscos.

Dentre outros aspectos da fase, o acompanhamento da criticidade de análises relacionadas ao processo de Gestão de Riscos deve manter o alinhamento às diretrizes de natureza global na organização, verificando de maneira frequente as mudanças ocorridas quanto aos critérios associados a avaliação e aceitação dos riscos, assim como verificar mudanças no ambiente, nos ativos das informações, ações de seguranças relacionadas a informações e os fatores de riscos, sendo estes representados por ameaças, vulnerabilidade, probabilidade e impacto.

5.3 AGIR

É a fase do ciclo na qual o Gestor de Segurança da Informação e Comunicação aperfeiçoará as ações baseando-se no monitoramento realizado na fase anterior.

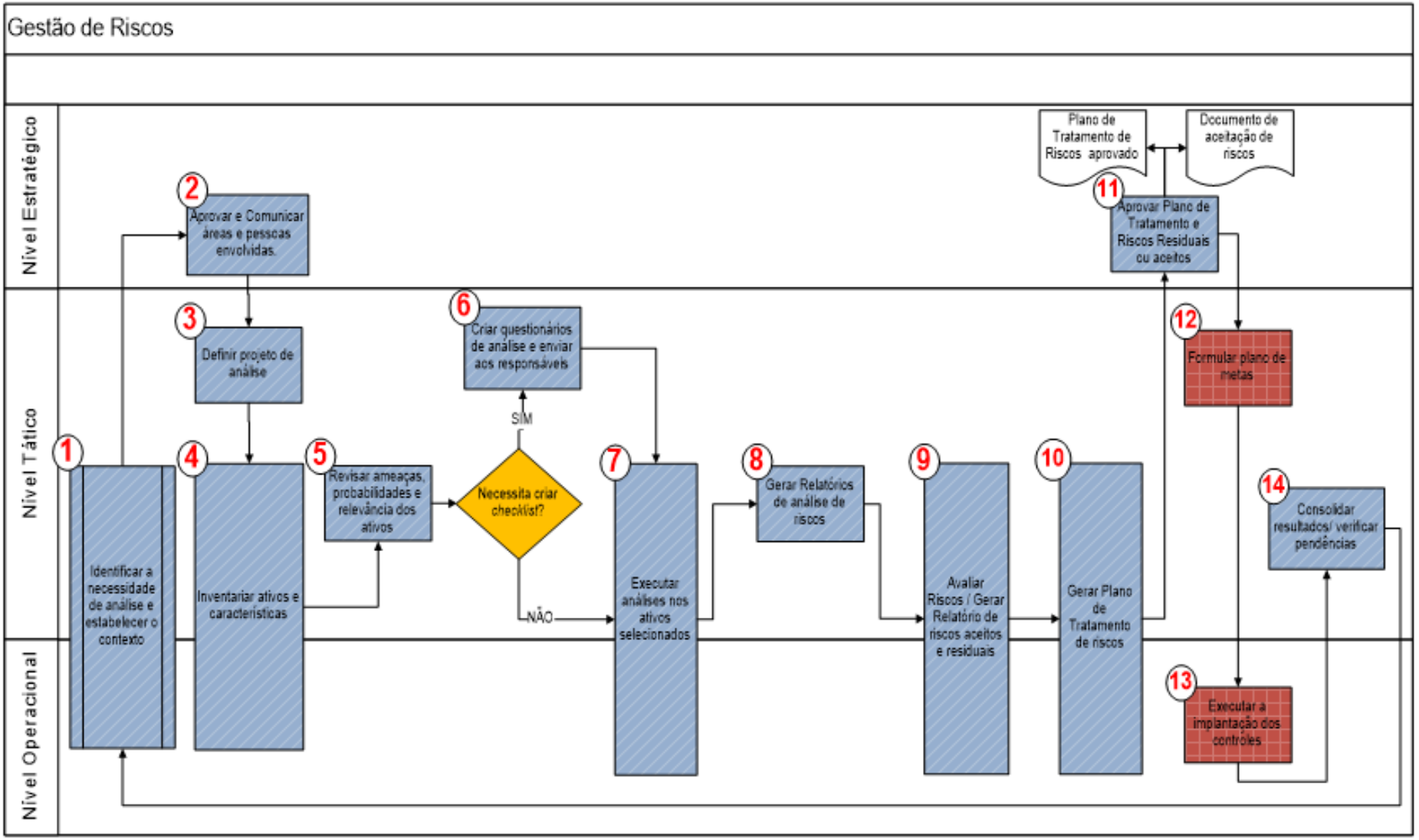
5.3.1 Melhoria Contínua do Processo de Gestão Riscos

A fim de realizar a melhoria contínua do processo é necessário sinalizar a alta direção da organização acerca da pertinência da implementação das melhorias identificadas, executar as ações preventivas e corretivas necessárias à conformidade, comunicar as melhorias efetuadas e obtidas e, principalmente, certificar-se de que as melhorias atinjam os resultados pretendidos.

6 FLUXO DA GESTÃO DE RISCOS

A Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) tem como objetivo identificar as necessidades da Funasa em relação aos requisitos de segurança da informação. Este processo deve ser contínuo e contemplar desde a definição do contexto, a análise e avaliação dos riscos, o tratamento e aceitação dos riscos identificados até sua divulgação às partes interessadas, conforme ilustrado no fluxograma da Figura 8:

Figura 8: fluxo da gestão de riscos



Fonte: (ISO/IEC 27002, 2005)

O fluxograma da Figura 8 representa de forma esquemática a proposta realizada nesta pesquisa, compondo um quadro possível de implementação futura, podendo ser associada à metodologia já utilizada pela Fundação Nacional de Saúde para Gestão de Riscos na Segurança da Informação e Comunicações. Assim, como aspecto importante para execução da proposta, deve-se considerar os níveis pelos quais as atividades transcorrem, pois compreende-se que todos os colaboradores podem se envolver no processo de segurança da informação.

Para tanto, as atividades de 1 a 14 descrevem os procedimentos decorrentes da proposta vinculada a este estudo e estão definidas a seguir:

ATIVIDADE 1: Necessidade de Analisar e Estabelecer o Contexto

DESCRIÇÃO

Identificar a necessidade da análise e estabelecer o contexto para gestão dos riscos. Inclui a definição dos critérios básicos necessários para a avaliação dos riscos e a definição dos limites.

RESPONSÁVEL

- Diretoria;
- Gerente da área envolvida.

ENTRADA

- Processos de negócio;
- Estratégias;
- Objetivos;
- Características externas e internas;
- Regulamentações;
- Outras informações relevantes para a definição do contexto da gestão dos riscos.

SAÍDA

Documento formal contendo:

- Identificação da necessidade de análise de riscos;
- Especificações dos critérios de aceitação de riscos;
- Escopo e limites do processo com despacho para alta direção.

FERRAMENTAS/MODELOS

Memorando, Ofício ou outra forma instituída pela Organização.

ATIVIDADE 2: Aprovar e comunicar áreas e pessoas envolvidas

DESCRIÇÃO

A diretoria deve autorizar a análise de segurança identificada, estabelecendo:

- A comunicação com as áreas envolvidas;
- As pessoas envolvidas no processo das atividades;
- Período para execução;
- Resultados esperados;
- Custos.

RESPONSÁVEL

Diretor da área.

ENTRADA

Saída da Atividade 1.

SAÍDA

Autorização com despacho para a área que sofrerá a análise detalhando os itens acima.

FERRAMENTAS/MODELOS

Memorando, Ofício, e-mail ou outra forma instituída pela Organização.

ATIVIDADE 3: Definir projeto de análise

DESCRIÇÃO

Executar análises e avaliações de riscos determinando os responsáveis pelas atividades, estabelecendo:

- Inventário de ativos de TI;
- Relatórios das análises de riscos;
- Plano de comunicação;
- Cronograma;
- Custo do projeto.

RESPONSÁVEL

O responsável pela área de segurança da informação.

ENTRADA

- Relatórios;
- Fluxogramas;

- Organogramas.

SAÍDA

- Divisão do projeto em atividades;
- Estimativa de custos
- Cronograma.

FERRAMENTAS/MODELOS

Nota técnica ou outra forma instituída pela Organização.

ATIVIDADE 4: Identificar a Necessidade de Análise e Estabelecer o Contexto

DESCRIÇÃO

Inventariar todos os ativos, compondo alinhamento com os objetivos estratégicos, ocorrendo por meio de reuniões com responsáveis pelos ativos.

RESPONSÁVEL

- Equipe técnica de TI;
- Responsáveis pelos ativos.

ENTRADA

- Lista com características dos ativos com os responsáveis por nível operacional;
- Cadastramento dos ativos sendo os responsáveis a equipe técnica de TI;
- Declarar contexto de escopo.

SAÍDA

Documento formal contendo:

- Listagem de ativos e das suas características, além de seus dependentes e responsáveis;
- Cadastramento de informações nas ferramentas.

FERRAMENTAS/MODELOS

Ferramentas específicas para Gestão de Riscos.

ATIVIDADE 5: Revisar Ameaças, Probabilidades e Criticidade dos Ativos

DESCRIÇÃO

Determinar as ameaças, probabilidades e criticidade nos ativos, condicionados aos objetivos do negócio.

RESPONSÁVEL

- Equipe técnica de TI;
- Responsáveis por ativos;
- Área/departamento responsável pelo ativo ou sistema.

ENTRADA

Lista de ativos e suas características definindo ameaças, probabilidades e criticidade.

SAÍDA

Documento formal contendo:

- Atualização de inventário de ativos de TI.

FERRAMENTAS/MODELOS

Automatização da Gestão de Riscos ou processador de planilhas.

ATIVIDADE 6: Criar Questionário de Análise e Enviar aos Responsáveis

DESCRIÇÃO

Trata-se de um método com produção de questionário ou listas de checagem, contendo boas práticas de mercado, considerando cada um dos ativos de escopo e seus aspectos.

RESPONSÁVEL

Equipe técnica de TI.

ENTRADA

Atualizações do inventário.

SAÍDA

- Questionários dos impactos associados a controles e probabilidades de ocorrência;
- Plano de tratamento de riscos baseado em boas práticas.

FERRAMENTAS/MODELOS

Automatização da Gestão de Riscos ou processador de planilhas.

ATIVIDADE 7: Executar as Análises nos Ativos Selecionados

DESCRIÇÃO

Os riscos são analisados por meio de avaliações pelos controles definidos nos questionários, considerando comparação com as evidências dos ativos. Definidos no

escopo, sistemas ou processo, sendo estes alvos dos cálculos para índices de riscos, seguindo as orientações presentes na metodologia.

RESPONSÁVEL

- Equipe técnica de TI;
- Responsáveis pelos ativos.

ENTRADA

- Atualizações do inventário com automatização de coletores;
- Atribuir índices para cada risco;
- Atribuir prazo de execução para aplicação de questionários desenvolvidos.

SAÍDA

- Análises de riscos e acompanhamento de análises;
- Ativos listados com indicação de índices.

FERRAMENTAS/MODELOS

Automatização da Gestão de Riscos ou processador de planilhas.

ATIVIDADE 8: Gerar Relatórios de Análise de Riscos

DESCRIÇÃO

Redigir relatórios, com histórico de execução dos resultados que foram obtidos, as principais ameaças, índices por ativos dos riscos, controles priorizados e correções sugeridas.

RESPONSÁVEL

- Equipe técnica de TI;
- Responsáveis pelos ativos.

ENTRADA

Produção dos relatórios das análises de riscos consolidado.

SAÍDA

Relatórios Gerencial e Operacional de análises de riscos.

FERRAMENTAS/MODELOS

Automatização da Gestão de Riscos ou processador de planilhas.

ATIVIDADE 9: Avaliar Riscos/Gerar Relatórios de Riscos Aceitos ou Residuais

DESCRIÇÃO

Os riscos listados, assim como os controles sugeridos para minimização, precisam ser avaliados. A consolidação dos riscos será um auxílio nas tomadas de decisões por meio da identificação de custos e impactos.

RESPONSÁVEL

- Equipe técnica de TI;
- Equipes de operações dos ativos.

ENTRADA

Relatórios Gerencial e Operacional sobre análises de riscos.

SAÍDA

- Identificação e validação de controles implementados;
- Relatórios de riscos aceitos e residuais.

FERRAMENTAS/MODELOS

Automatização da Gestão de Riscos ou processador de planilhas.

ATIVIDADE 10: Gerar Plano de Tratamento de Riscos

DESCRIÇÃO

Plano de tratamento criado para sugestões de controles buscando minimizar riscos, incluindo estimativas dos custos, das atividades rotineiras que geram impactos, ações necessárias e prazos.

RESPONSÁVEL

Equipe técnica de TI.

ENTRADA

Relatórios Operacional e de riscos aceitos e/ou residuais.

SAÍDA

Plano de Tratamento de Riscos.

FERRAMENTAS/MODELOS

Automatização da Gestão de Riscos ou processador de planilhas.

ATIVIDADE 11: Aprovar Plano de Tratamento e Riscos Residuais ou Aceitos

DESCRIÇÃO

Diretoria aprova o plano de tratamento definindo ou ajustando as atividades, considerando ainda restrições, como orçamento. O plano pode e deve ser atualizado, assim como seus relatórios de riscos residuais e aceitos, buscando garantias de boa comunicação dos envolvidos.

RESPONSÁVEL

Diretoria.

ENTRADA

Proposta de plano de tratamento de riscos e de riscos residuais.

SAÍDA

Ajuste e aprovação do plano, e relatório de riscos residuais e aceitos.

FERRAMENTAS/MODELOS

Definido pela Instituição.

ATIVIDADE 12: Formular Plano de Metas

DESCRIÇÃO

O plano de metas surge após o plano de tratamento e inclui indicadores para avaliações das ações a serem desenvolvidas pela equipe operacional, implementando controles já sugeridos e aprovados.

RESPONSÁVEL

Equipe técnica de TI.

ENTRADA

Plano de metas aprovado e relatório de contexto e escopo.

SAÍDA

Plano de metas para as áreas e responsáveis pelos ativos do escopo.

FERRAMENTAS/MODELOS

Definido pela instituição.

ATIVIDADE 13: Executar Implantação dos Controles Selecionados

DESCRIÇÃO

Cada ativo recebe um tratamento específico, portanto, trata-se de uma atividade bem variada. As identificações de riscos, normalmente, relacionam-se a quatro tipos de ativos, aqueles considerados tecnológicos, processuais, ambientais ou humanos. Assim, o plano de tratamento localiza os controles a serem aplicados. A Fundação Nacional de Saúde pode indicar controles e avaliações de maneira periódica, considerando as implantações de controles. O *workflow* pode monitorar essas tarefas.

RESPONSÁVEL

Área responsável pelos ativos.

ENTRADA

Planos de tratamento e metas.

SAÍDA

- Controle para redução de riscos implementados e indicadores criados durante a implementação;
- Definir *workflow* para monitorar essas tarefas.

FERRAMENTAS/MODELOS

Automatização da Gestão de Riscos ou processador de planilhas.

ATIVIDADE 14: Consolidar Resultados e Verificar Pendências

DESCRIÇÃO

Os resultados precisam ser consolidados, para tanto, após as análises de riscos, considera-se as ligações e dependências de um ativo com outro entre sistemas de processos, acordando com escopo e contexto. As pendências também devem ser avaliadas e dadas como entrada para os próximos ciclos.

RESPONSÁVEL

- Equipe técnica de TI;
- Gestor de Segurança da Informação.

ENTRADA

Lista de ativos, bem como os índices de riscos correspondentes a cada ativo, sistema ou processo.

SAÍDA

Consolidação dos resultados considerando objetivos do escopo.

FERRAMENTAS/MODELOS

Produção de nota técnica ou outra ferramenta dada pela Instituição.

7 ESTRATÉGIA DE IMPLANTAÇÃO DOS PROCESSOS

O processo proposto para a gestão de risco de segurança da informação na Funasa foi desenvolvido de forma que as características essenciais possam ser utilizadas em outros âmbitos com alterações mínimas em suas definições básicas. A divisão por níveis hierárquicos permite que essa estrutura possa ser migrada ou direcionada conforme a abrangência de atuação.

Para as ações listadas a seguir, é sugerida a utilização de instrumento legal compatível para a oficialização e comunicação às partes interessadas.

7.1 DEFINIÇÃO DE RECURSOS HUMANOS PARA ATUAÇÃO NO NÍVEL TÁTICO

A criação formal de uma área com atribuições voltadas a segurança da informação pode ser inviabilizada por uma série de fatores. No entanto, a definição dos recursos humanos que ficarão responsáveis pela operacionalização das ações é primordial para o sucesso da implantação.

No caso da FUNASA além das equipes que participavam do processo durante o ciclo anual de gestão de riscos, tínhamos uma pequena equipe dedicada de gestor e 3 analista de segurança da informação que tinham como atribuição a coordenar e operacionalizar todas as ações de SIC da Fundação.

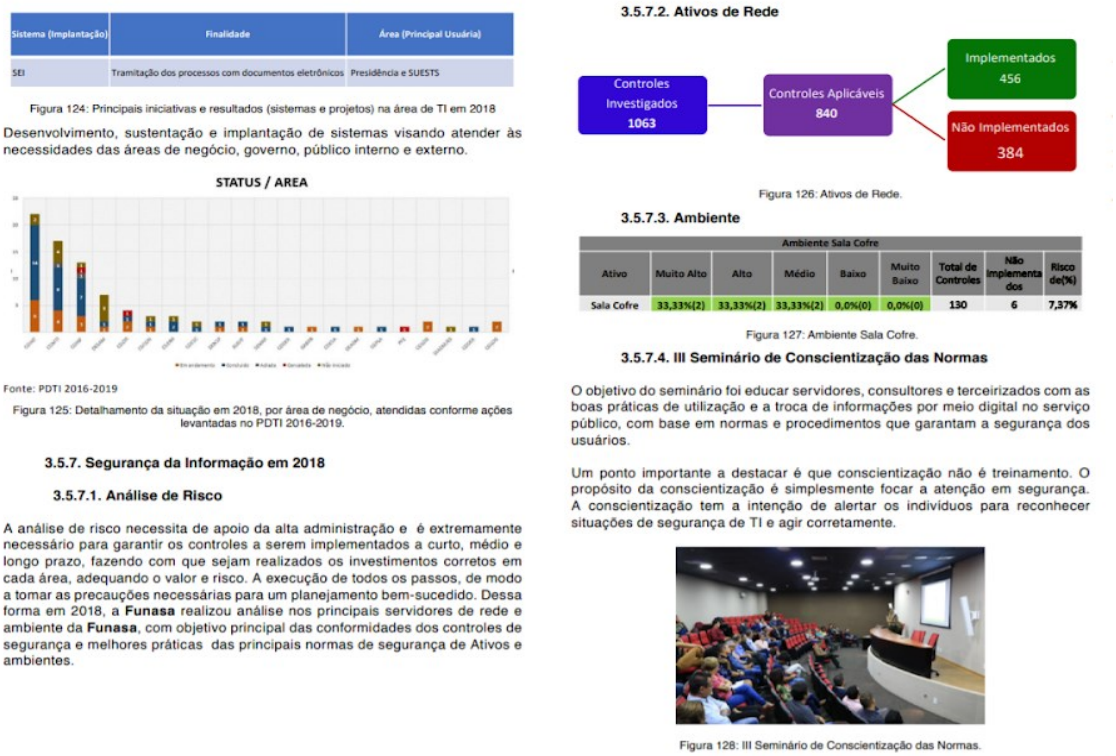
7.2 CRIAÇÃO DE PROCEDIMENTOS PARA AS ATIVIDADES DO PROCESSO

A documentação dos procedimentos para execução das atividades definidas no processo proposto permitirá a padronização das ações e formatação de resultados. Mesmo que seja alterada a estrutura organizacional da Funasa, a criação dos procedimentos pode ser realizada por meio da instituição de um grupo de trabalho específico, por meio de projeto a ser definido no Plano Diretor de Tecnologia da Informação (PDTI) ou, ainda, utilizando profissionais já existentes no quadro da Funasa.

Os resultados da implantação na Funasa em 2018 foram apresentados no Relatório de Gestão 2018. O detalhamento e consolidação dos dados tem acesso restrito, mas os modelos que apoiaram a implantação dos resultados podem ser

socializados com entes da Administração Pública Federal, por meio de solicitação no correio eletrônico do Órgão: seguranca.informacao@funasa.gov.br.

Figura 9: Relatório de Gestão 2018



Sistema (Implantação)	Finalidade	Área (Principal Usuária)
SEI	Tramitação dos processos com documentos eletrônicos	Presidência e SUESTS

Figura 124: Principais iniciativas e resultados (sistemas e projetos) na área de TI em 2018

Desenvolvimento, sustentação e implantação de sistemas visando atender às necessidades das áreas de negócio, governo, público interno e externo.

STATUS / AREA

Fonte: PDTI 2016-2019

Figura 125: Detalhamento da situação em 2018, por área de negócio, atendidas conforme ações levantadas no PDTI 2016-2019.

3.5.7. Segurança da Informação em 2018

3.5.7.1. Análise de Risco

A análise de risco necessita de apoio da alta administração e é extremamente necessário para garantir os controles a serem implementados a curto, médio e longo prazo, fazendo com que sejam realizados os investimentos corretos em cada área, adequando o valor e risco. A execução de todos os passos, de modo a tomar as precauções necessárias para um planejamento bem-sucedido. Dessa forma em 2018, a **Funasa** realizou análise nos principais servidores de rede e ambiente da **Funasa**, com objetivo principal das conformidades dos controles de segurança e melhores práticas das principais normas de segurança de Ativos e ambientes.

3.5.7.2. Ativos de Rede

Figura 126: Ativos de Rede.

3.5.7.3. Ambiente

Ambiente Sala Cofre								
Ativo	Muito Alto	Alto	Médio	Baixo	Muito Baixo	Total de Controles	Não implementados	Risco de(%)
Sala Cofre	33,33%(2)	33,33%(2)	33,33%(2)	0,0%(0)	0,0%(0)	130	6	7,37%

Figura 127: Ambiente Sala Cofre.

3.5.7.4. III Seminário de Conscientização das Normas

O objetivo do seminário foi educar servidores, consultores e terceirizados com as boas práticas de utilização e a troca de informações por meio digital no serviço público, com base em normas e procedimentos que garantam a segurança dos usuários.

Um ponto importante a destacar é que conscientização não é treinamento. O propósito da conscientização é simplesmente focar a atenção em segurança. A conscientização tem a intenção de alertar os indivíduos para reconhecer situações de segurança de TI e agir corretamente.

Figura 128: III Seminário de Conscientização das Normas.

Fonte: www.funasa.gov.br

A análise de risco necessita de apoio da alta administração e é extremamente necessário para garantir os controles a serem implementados a curto, médio e longo prazo, fazendo com que sejam realizados os investimentos corretos em cada área. Para isso, é importante a execução de todos os passos de modo a tomar as precauções necessárias para um planejamento bem-sucedido. Dessa forma, em 2018 a Funasa realizou análise nos principais servidores de rede e ambiente da Instituição, com objetivo principal de atender as conformidades dos controles de segurança e melhores práticas das normas de segurança de ativos e de ambientes. O detalhamento do procedimento aplicado no ano de 2018 está disponível no estudo de caso.

8 ESTUDO DE CASO DO CICLO 2018

ATIVIDADE 1 - IDENTIFICAR A NECESSIDADE DE ANÁLISE E ESTABELECER O CONTEXTO

A necessidade estabelecida para o ciclo de gestão de riscos de 2018 foi atender as conformidades dos controles de segurança e adotar melhores práticas das principais normas de segurança de ativos e ambientes, a fim de garantir a disponibilidade e integridade dos ativos. A análise de risco referente ao ciclo 2018 teve priorização da alta administração dos ativos relacionados com os dois sistemas mais críticos (Siga e Sei), fazendo com que fossem realizados os investimentos corretos em cada área, adequando valor e risco. A priorização foi motivada pelo esforço de se realizar uma análise de riscos em todos os ativos de tecnologia da informação para situação, considerada inviável por esforço, custo e prazo.

As normas utilizadas foram NBR ISO/IEC 27001, NBR ISO/IEC 27002, NBR ISO/IEC27005, ISO 31000 e ISO Guia 73.

ATIVIDADE 2 - APROVAR E COMUNICAR ÁREAS E PESSOAS ENVOLVIDAS

Seguindo o processo de GRC foi definida a área de Logística – CGLOG e Tecnologia da Informação:

- Coordenador responsável pela Logística e coordenador responsável pela área de TI;
- Relação de ativos de TI.

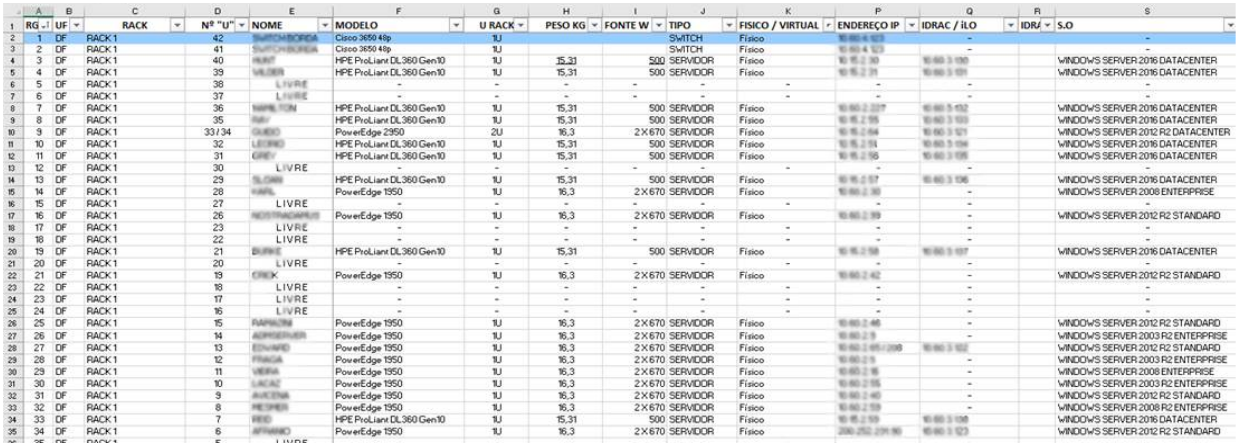
Ativo	Tipo de Ativo
Servidor Banco de Dados 1	Tecnologia
Servidor Banco de Dados 2	Tecnologia
Servidor Sistemas 3	Tecnologia
Servidor Sistemas 4	Tecnologia
Sala Cofre	Ambiente
Backup	Processo

ATIVIDADE 3 - DEFINIR PROJETO DE ANÁLISE

O projeto foi definido pelos principais ativos de Tecnologia da Funasa: servidores de banco de dados e servidores responsáveis pelos principais sistemas da Funasa, sala cofre e backup dos ativos.

ATIVIDADE 4 - INVENTARIAR ATIVOS

O inventário de ativo de TI foi realizado por meio de planilha de controle da equipe de infraestrutura e os gestores foram definidos pela relevância para o funcionamento dos principais sistemas.



RG	UF	RACK	Nº "U"	NOME	MODELO	U RACK	PESO KG	FONTE W	TIPO	FISICO / VIRTUAL	ENDEREÇO IP	IDRAC / iLO	IDRAC	S.O
1	DF	RACK 1	42	[illegible]	Cisco 3650 48p	1U			SWITCH	Físico	[illegible]	-		-
2	DF	RACK 1	41	[illegible]	Cisco 3650 48p	1U			SWITCH	Físico	[illegible]	-		-
3	DF	RACK 1	40	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
4	DF	RACK 1	39	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
5	DF	RACK 1	38	LIVRE	-	-	-	-	-	-	-	-		-
6	DF	RACK 1	37	LIVRE	-	-	-	-	-	-	-	-		-
7	DF	RACK 1	36	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
8	DF	RACK 1	35	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
9	DF	RACK 1	33 / 34	[illegible]	PowerEdge 2950	2U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2012 R2 DATACENTER
10	DF	RACK 1	32	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
11	DF	RACK 1	31	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
12	DF	RACK 1	30	LIVRE	-	-	-	-	-	-	-	-		-
13	DF	RACK 1	29	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
14	DF	RACK 1	28	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2008 ENTERPRISE
15	DF	RACK 1	27	LIVRE	-	-	-	-	-	-	-	-		-
16	DF	RACK 1	26	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2012 R2 STANDARD
17	DF	RACK 1	23	LIVRE	-	-	-	-	-	-	-	-		-
18	DF	RACK 1	22	LIVRE	-	-	-	-	-	-	-	-		-
19	DF	RACK 1	21	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
20	DF	RACK 1	20	LIVRE	-	-	-	-	-	-	-	-		-
21	DF	RACK 1	19	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2012 R2 STANDARD
22	DF	RACK 1	18	LIVRE	-	-	-	-	-	-	-	-		-
23	DF	RACK 1	17	LIVRE	-	-	-	-	-	-	-	-		-
24	DF	RACK 1	16	LIVRE	-	-	-	-	-	-	-	-		-
25	DF	RACK 1	15	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2012 R2 STANDARD
26	DF	RACK 1	14	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2003 R2 ENTERPRISE
27	DF	RACK 1	13	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2012 R2 STANDARD
28	DF	RACK 1	12	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2003 R2 ENTERPRISE
29	DF	RACK 1	11	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2008 ENTERPRISE
30	DF	RACK 1	10	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2003 R2 ENTERPRISE
31	DF	RACK 1	9	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2012 R2 STANDARD
32	DF	RACK 1	8	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	-		WINDOWS SERVER 2008 R2 ENTERPRISE
33	DF	RACK 1	7	[illegible]	HPE ProLiant DL360 Gen10	1U	15,31	500	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2016 DATACENTER
34	DF	RACK 1	6	[illegible]	PowerEdge 1950	1U	16,3	2 X 670	SERVIDOR	Físico	[illegible]	[illegible]		WINDOWS SERVER 2012 R2 STANDARD

ATIVIDADE 5 - REVISAR AMEAÇAS, PROBABILIDADES E CRITICIDADE DOS ATIVOS

No projeto inicial ficou definido que após a disponibilização dos relatórios de Análise de Risco para cada área, a equipe de segurança da informação iria monitorar a evolução de tratamento de cada área.

Cada mês era disponibilizado um relatório de acompanhamento com a evolução da análise de risco.

A priorização dos controles e criticidades dos ativos foram definidos no início do projeto.

Ativo de Desenvolvimento								
Ativo	Muito Alto	Alto	Médio	Baixo	Muito Baixo	Total de Controles	Não Implementados	Risco de(%)
Andreas	0,00%(0)	24,27%(25)	55,34%(57)	17,48%(18)	2,91%(3)	236	103	52,82%
Barbosa	0,00%(0)	24,27%(25)	55,34%(57)	17,48%(18)	2,91%(3)	236	103	52,82%
Santos	0,00%(0)	24,27%(25)	55,34%(57)	17,48%(18)	2,91%(3)	236	103	52,82%
Silva	0,00%(0)	24,27%(25)	55,34%(57)	17,48%(18)	2,91%(3)	236	103	52,82%
Souza	0,00%(0)	24,27%(25)	55,34%(57)	17,48%(18)	2,91%(3)	236	103	52,82%
Emil	0,00%(0)	20,72%(23)	60,36%(67)	16,22%(18)	2,70%(3)	236	111	51,81%

Ambiente Sala Cofre								
Ativo	Muito Alto	Alto	Médio	Baixo	Muito Baixo	Total de Controles	Não Implementados	Risco de(%)
Sala Cofre	33,33%(2)	33,33%(2)	33,33%(2)	0,0%(0)	0,0%(0)	130	6	7,37%

ATIVIDADE 6 - CRIAR QUESTIONÁRIOS DE ANÁLISE E ENVIAR AOS RESPONSÁVEIS

As análises eram coletadas de forma automática nos servidores, porém no ambiente da sala cofre e do processo de backup, foram gerados questionários para coleta dos controles.

2.1.0001 Ameaça: Acesso físico não autorizado

PSR	ID do Controlo	Nome do Controlo	P	S	R	Componente do Ativo	Nível do Risco
60	MOD_PT.00002847	Exercícios de simulação de incêndios devem ser realizados periodicamente.	4	5	3	Sala Cofre - Data Center	Muito Alto
36	MOD_PT.00002827	Uma área de recepção intermediária ("Clear Zone") deve ser construída isolada do Data Center.	4	3	3	Sala Cofre - Data Center	Alto
27	MOD_PT.00002792	Os sistemas de controle de acesso do Data Center devem ser contingenciados por geradores alternativos de energia.	3	3	3	Sala Cofre - Data Center	Médio

2.1.0002 Ameaça: Contaminação ambiental

PSR	ID do Controlo	Nome do Controlo	P	S	R	Componente do Ativo	Nível do Risco
36	MOD_PT.00002827	Uma área de recepção intermediária ("Clear Zone") deve ser construída isolada do Data Center.	4	3	3	Sala Cofre - Data Center	Alto

2.1.0003 Ameaça: Dano a instalações

PSR	ID do Controlo	Nome do Controlo	P	S	R	Componente do Ativo	Nível do Risco
48	MOD_PT.00002815	Os equipamentos críticos do Data Center devem ser contingenciados por geradores alternativos de energia.	4	4	3	Sala Cofre - Data Center	Alto
36	MOD_PT.00002827	Uma área de recepção intermediária ("Clear Zone") deve ser construída isolada do Data Center.	4	3	3	Sala Cofre - Data Center	Alto

2.1.0004 Ameaça: Dano a pessoas

PSR	ID do Controlo	Nome do Controlo	P	S	R	Componente do Ativo	Nível do Risco
60	MOD_PT.00002846	Saídas de emergência devem ser construídas de modo a facilitar a evacuação do Data Center.	4	5	3	Sala Cofre - Data Center	Muito Alto
60	MOD_PT.00002847	Exercícios de simulação de incêndios devem ser realizados periodicamente.	4	5	3	Sala Cofre - Data Center	Muito Alto

Controle: é a medida de segurança necessária para a redução do risco, que pode ser uma política, boa prática, procedimento, estruturas organizacionais ou funções de software. Incluem-se ainda dispositivos de hardware voltados a segurança. Os controles visam reduzir ou eliminar as vulnerabilidades existentes, inibir a ação de agentes de ameaça ou, ainda, minimizar os impactos causador por incidentes.

ID: é o identificador único de cada controle.

Componentes de ativos: é o local onde o controle não está implementado.

ATIVIDADE 7 - DISTRIBUIÇÃO DOS NÍVEIS DE RISCO POR ATIVO

Ativo	Tipo de Ativo	Muito Alto	Alto	Médio	Baixo	Muito Baixo	% Total Aplicável
Servidor Banco de Dados 1- Amato	Tecnologia	27	26	18	1	0	8,57
Servidor Banco de Dados 2- Barbosa	Tecnologia	0	26	77	18	3	14,76
Servidor Sistemas 3 -Emil	Tecnologia	0	23	67	18	3	13,21
Servidor Sistemas 4- Behring	Tecnologia	0	28	36	5	0	8,21
Sala Cofre	Infraestrutura	2	2	2	0	0	0,71
Backup Sidoc e SCDWEB	Processo	0	0	2	0	0	0,24
Consolidado		29	105	202	42	6	46,00

ATIVIDADE 8 - NÚMEROS CONSOLIDADOS POR ATIVOS DE CONTROLES

Ativo	Tipo de Ativo	Controles Implementados	Controles não implementados	Risco %
Servidor Banco de Dados 1- Amato	Tecnologia	65	72	52,55
Servidor Banco de Dados 2- Barbosa	Tecnologia	103	124	54,63
Servidor Sistemas 3 -Emil	Tecnologia	98	111	53,11
Servidor Sistemas 4- Behring	Tecnologia	70	69	49,64
Servidor Banco de Dados 1-Amato	Infraestrutura	96	6	5,88
Backup Sidoc e SCDWEB	Processo	24	2	7,69
Total		456	384	

ATIVIDADE 9 - AVALIAR RISCOS / GERAR RELATÓRIOS DE RISCOS ACEITOS OU RESIDUAIS

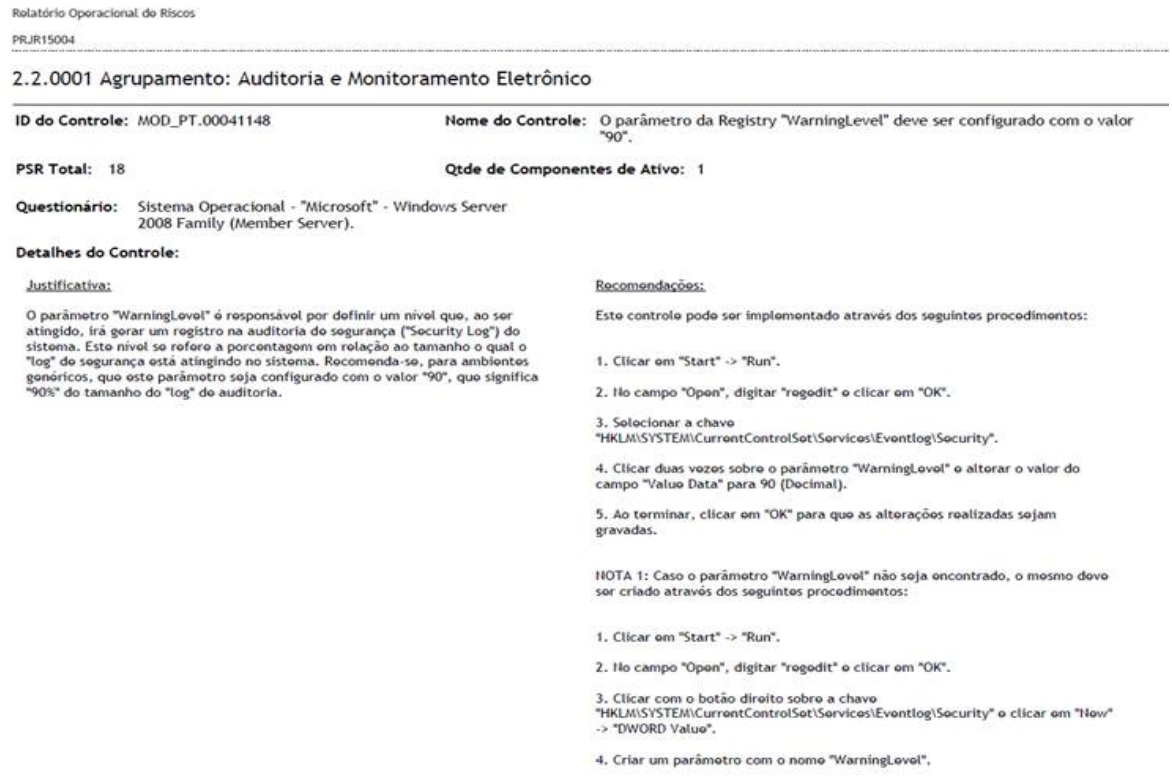
Após a criação dos relatórios das análises de risco, os mesmos foram enviados para as devidas áreas (Banco – Desenvolvimento – Infraestrutura) para mitigar os controles.

Essa análise das áreas consistia em verificar poderia ser ACEITO OU CORRIGIDO.

ATIVIDADE 10 - GERAR PLANO DE TRATAMENTO DE RISCOS

O Relatório foi enviado para as equipes contendo as recomendações para o tratamento dos riscos de cada ativo de TI.

O Relatório operacional de risco foi elaborado para auxiliar o responsável técnico a realizar o tratamento necessário para mitigar o risco, inclusive detalhando como esta alteração pode ser realizada, conforme o exemplo a seguir:



Relatório Operacional de Riscos

PRJR15004

2.2.0001 Agrupamento: Auditoria e Monitoramento Eletrônico

ID do Controle: MOD_PT.00041148 **Nome do Controle:** O parâmetro da Registry "WarningLevel" deve ser configurado com o valor "90".

PSR Total: 18 **Qtde de Componentes de Ativo:** 1

Questionário: Sistema Operacional - "Microsoft" - Windows Server 2008 Family (Member Server).

Detalhes do Controle:

Justificativa:

O parâmetro "WarningLevel" é responsável por definir um nível que, ao ser atingido, irá gerar um registro na auditoria de segurança ("Security Log") do sistema. Este nível se refere a porcentagem em relação ao tamanho o qual o "log" de segurança está atingindo no sistema. Recomenda-se, para ambientes genéricos, que este parâmetro seja configurado com o valor "90", que significa "90%" do tamanho do "log" de auditoria.

Recomendações:

Este controle pode ser implementado através dos seguintes procedimentos:

1. Clicar em "Start" -> "Run".
2. No campo "Open", digitar "regedit" e clicar em "OK".
3. Selecionar a chave "HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security".
4. Clicar duas vezes sobre o parâmetro "WarningLevel" e alterar o valor do campo "Value Data" para 90 (Decimal).
5. Ao terminar, clicar em "OK" para que as alterações realizadas sejam gravadas.

NOTA 1: Caso o parâmetro "WarningLevel" não seja encontrado, o mesmo deve ser criado através dos seguintes procedimentos:

1. Clicar em "Start" -> "Run".
2. No campo "Open", digitar "regedit" e clicar em "OK".
3. Clicar com o botão direito sobre a chave "HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security" e clicar em "New" -> "DWORD Value".
4. Criar um parâmetro com o nome "WarningLevel".

ATIVIDADE 11 - EXECUTAR AS ANÁLISES NOS ATIVOS SELECIONADOS

Conforme escopo inicial após definição dos ativos críticos a Funasa, foram realizadas as análises de forma automática dos Ativos e de forma manual (questionário) o processo de backup e análise de infraestrutura da sala cofre.

ATIVIDADE 12 - FORMULAR PLANO DE METAS

As metas foram estabelecidas por nível de risco e o tratamento por meses, priorizando do mais alto para o mais baixo:

1º Mês	2º Mês	3º Mês	4º Mês	5º Mês
Muito Alto	Alto	Médio	Baixo	Muito Baixo

Todos os meses os relatórios eram consolidados com percentual de controles aplicados e controles aceitos e repassados para as equipes.

ATIVIDADE 13 - EXECUTAR IMPLANTAÇÃO DOS CONTROLES SELECIONADOS

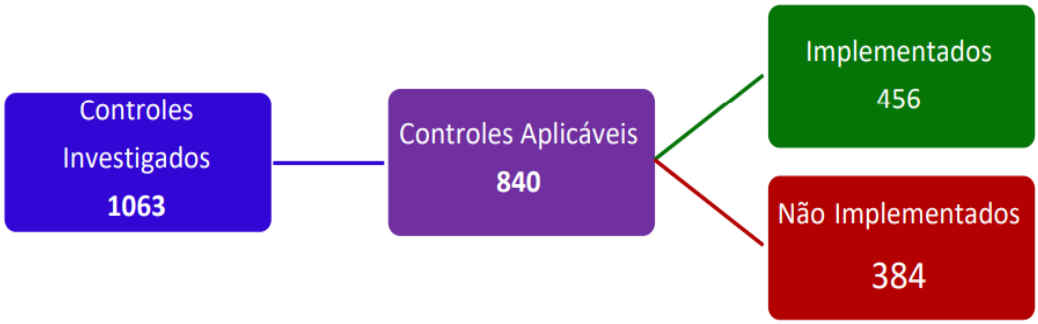
O segmento que teve a implantação prejudicada e que deveria receber a maior atenção foi o de Banco de Dados, com riscos muito altos, e apresentado insuficiência de profissionais para aplicação dos controles estabelecidos.

Ativo	Tipo de Ativo	Muito alto	Alto	Médio	Baixo	Muito Baixo	% Total Aplicável
Servidor Banco de Dados 1-Amato	Tecnologia	27	26	18	1	0	8,57

Este fato originou alguns incidentes de disponibilidade e performance, devidamente registrados e associados a não implantação dos controles. Os incidentes reforçaram a importância da Gestão de Riscos de Tecnologia da Informação, subsidiando o Gestor acerca das fraquezas do ambiente pelo qual ele responde.

ATIVIDADE 14 - CONSOLIDAR RESULTADOS E VERIFICAR PENDÊNCIAS

A consolidação dos riscos foi divulgada de maneira que não comprometa a segurança das informações, mas que cumpra a publicidade do assunto.



O documento final foi assinado pela equipe técnica e ratificado pelo gestor de TI. Foi recomendado que os 384 controles “Não Implementados” deverão entrar no ciclo de 2019, fortalecendo as ações de melhoria contínua.

CONSIDERAÇÕES FINAIS

Este trabalho apresentou uma visão geral sobre a metodologia para gestão de riscos utilizada pela Funasa e a aplicação prática no Órgão. Nos últimos anos, a Administração Pública Federal não mediu esforços para proteger seus ativos dado o grande crescimento do uso da internet. Com essa proteção as empresas de todos os ramos de atuação evitam perda de tempo e dinheiro.

Condicionada às normativas legislativas, a Fundação Nacional de Saúde aplica sua metodologia de Gestão de Riscos seguindo os principais requisitos previstos por meio das providências dadas pela Associação Brasileira de Normas Técnicas (ABNT), ainda se propondo a considerar como boas práticas as normas 27002 e 27005. Neste contexto, importa destacar que este estudo conclui-se contemplando seu principal objetivo de documentar a metodologia utilizada pela Funasa para Gestão de Segurança da Informação.

A Funasa aplica sua metodologia para segurança da informação desdobrando-a por meio de um planejamento que envolve tratamento, monitoramento e controle de riscos, identificando e direcionando esses tratamentos de acordo com os tipos de riscos, entendendo ainda que algumas oportunidades podem surgir e com elas pode-se trabalhar para aprimoramentos, melhorias, ganhos, dentre outros impactos positivos.

As identificações quanto aos requisitos da metodologia, no que tange a Segurança da Informação e Comunicação na Funasa, apresentam-se obedecendo um fluxo que envolve os três principais níveis dentro da organização. Assim, o processo proposto no fluxograma da Figura 8 perfaz os três principais níveis dentro da organização.

Portanto, estão concluídos os dois principais objetivos que motivaram o tema deste estudo: a descrição e documentação da metodologia utilizada pela Funasa para o processo de Gestão de Riscos para Segurança da Informação e Comunicações (GRSIC) e a edição de uma proposta para aplicação ou complementação a metodologia utilizada pela Funasa para GRSIC.

Como sugestão para trabalhos futuros, a proposta construída na seção 6 e apresentada no fluxograma 8 pode ser aplicada de forma prática gerando resultados

tangentes e convergentes à metodologia do processo de Gestão de Riscos e Segurança da Informação e Comunicação da Funasa.

REFERÊNCIAS

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de software:** como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408.Rio de Janeiro: Campus, 2002.

ASCIUTTI, C. A. **Alinhando ABNT-NBR-ISO/IEC 17799 e 27001 para a administração pública.** USP, 2006. Disponível em: https://www.security.usp.br/palestras/Normas-Encontro-USP-Seguranca-Computacional-II-V-1-02.pdf

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (NBR 27002). **Tecnologia da informação – técnicas de segurança:** código de prática para a gestão da segurança da informação**.** Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (NBR 27001). **Tecnologia da informação – técnicas de segurança:** requisitos**.** Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (NBR 27005). **Tecnologia da informação - técnicas de segurança: -** gestão de riscos de segurança da informação**.** Rio de Janeiro, 2008.

BORAN, Sean. ***IT security cookbook***, 1996. Disponível em: http://www.boran.com/security/. Acesso em: 1 jun. 2019.

BRASIL. Departamento de Segurança da Informação e Comunicações. **Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC. 2013.** Disponível em: http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf. Acesso em: 15 mai. 2019.

BRASIL. Instrução Normativa GSI nº 1, 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.** Disponível em: https://www.governodigital.gov.br/documentos-e-arquivos/legislacao/14_IN_01_gsidsic.pdf. Acesso em: 15 mai. 2019.

BRASIL. **Norma Complementar nº 04/IN01/DSIC/GSIPR**. Disponível em: http://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf. Acesso em: 15 mai. 2019.

FERREIRA, Fernando Nicolau Freitas. ARAÚJO, Márcio Tadeu de. **Políticas de segurança da informação:** guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2008.

KRAUSE, Micki e TIPTON, Harold F. **Handbook of information security management**. Auerbach Publications, 1999.

HAMPSHIRE, M. C. S.; Tomimura, C. T. **Proposta de implementação da análise de risco em um projeto de implantação da segurança da informação**. São Paulo: Centro Tecnológico da Marinha , 2004.

GABBAY, M. S. **Fatores influenciadores na implementação de ações de gestão de segurança da informação:** um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte. Tese (mestrado) – Universidade Federal do Rio Grande do Norte, 2003.

NAKAMURA, Emilio Tissato & GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** 482 p. São Paulo: Novatec, 2007.

NIC.BR / CETIC.BR. **Pesquisa sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras - TIC Empresas 2017** Disponível em: https://www.cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-empresas-brasileiras-tic-empresas-2017. Acesso em: 10 mai. 2020

SÊMOLA, M. **Gestão da segurança da informação:** visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2003.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Governança pública:** referencial básico de governança aplicável a órgãos e entidades da administração pública e ações indutoras de melhoria. Brasília: TCU, Secretaria de Planejamento, Governança e Gestão**,** 2014.

VELLANI, K. H. **Strategic security management**:: risk assessment guide for decision makers. 2006.

WEILL, Peter; ROSS, Jeanne W. **Governança de TI, tecnologia da informação.** São Paulo: M. Books, 2006.