FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Paulo Eduardo de Oliveira

ARSI: UMA FERRAMENTA PARA GESTÃO DE RISCO EM PEQUENAS E MÉDIAS EMPRESAS

Americana, SP

2017

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Paulo Eduardo de Oliveira

ARSI: UMA FERRAMENTA PARA GESTÃO DE RISCO EM PEQUENAS E MÉDIAS EMPRESAS

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Esp. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação.

Americana, SP.

2017

AO49a OLIVEIRA, Paulo Eduardo de

ARSI: uma ferramenta para gestão de risco em pequenas e médias empresas. / Paulo Eduardo de Oliveira. – Americana, 2017.

46f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Esp. Edson Roberto Gaseta

1. Segurança em sistemas de informação 2. Gestão de risco I. GASETA, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

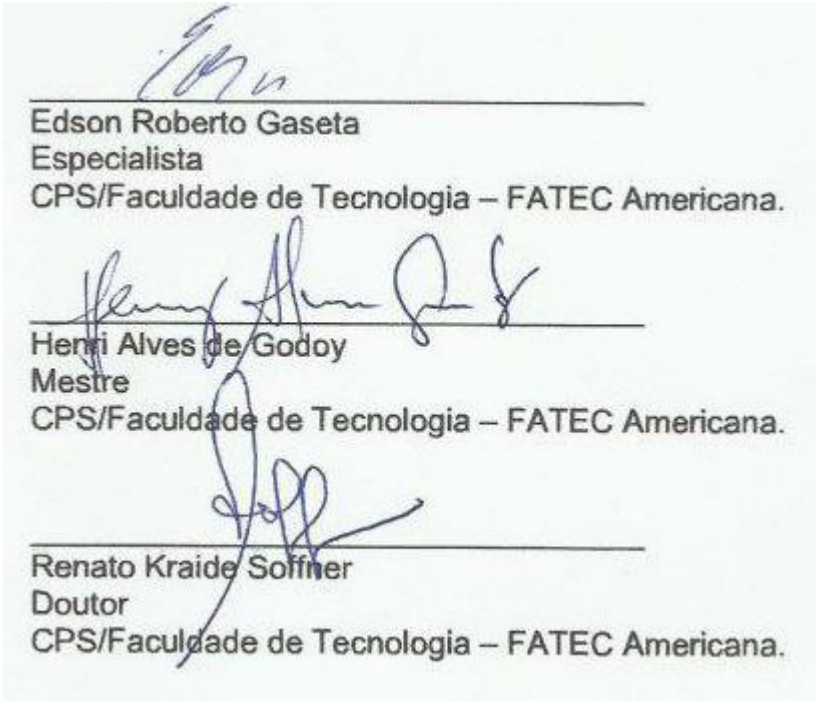
Paulo Eduardo De Oliveira

ARSI: UMA FERRAMENTA PARA GESTÃO DE RISCO EM PEQUENAS E MÉDIAS EMPRESAS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CPS/Faculdade de Tecnologia – FATEC/ Americana.
Área de concentração: Segurança da Informação.

Americana, 14 de Dezembro de 2017.

Banca Examinadora:



Edson Roberto Gaseta
Especialista
CPS/Faculdade de Tecnologia – FATEC Americana.

Henri Alves de Godoy
Mestre
CPS/Faculdade de Tecnologia – FATEC Americana.

Renato Kraide Soffner
Doutor
CPS/Faculdade de Tecnologia – FATEC Americana.

AGRADECIMENTOS

Em primeiro lugar à faculdade FATEC Americana por fornecer o conhecimento necessário para desenvolvimento desse projeto e também aos companheiros de sala.

Aos meus pais, Paulino e Maria, a quem devo minha eterna gratidão por todos esses anos batalhando. Embora seja muito difícil retribuir toda essa dedicação, espero algum dia ser capaz de recompensá-los e, principalmente, ser motivo de orgulho.

À minha namorada, Sara, e aos meus irmãos, Julio e Ana, agradeço por todos os momentos compartilhados. Gostaria de destacar e também agradecer por todo o apoio, companheirismo, paciência, e por cada uma das atitudes que vieram a me auxiliar e incentivar durante o desenvolvimento desta monografia.

Agradeço também meu orientador, Prof. Esp. Edson Roberto Gaseta, por cada segundo de dedicação, e por todo auxílio durante o semestre, e também por todo seu companheirismo.

DEDICATÓRIA

Aos meus amigos e familiares por me dar apoio para conclusão do curso.

RESUMO

Atualmente informação é considerada um dos ativos com mais importância para uma organização, e ao ser classificada com esse alto grau de relevância, a mesma estará sujeita em diversas ocasiões a ameaças. Para proteger esse ativo de ameaças, é utilizada a Gestão de Riscos de Segurança da Informação na qual são definidos os controles necessários para manter os riscos gerenciados. Atualmente, as organizações lidam com uma grande quantidade de ameaças que, em sua maioria, podem eventualmente concretizar-se devido à falta de um processo adequado para a análise e gestão dos riscos. Neste sentido, este trabalho de graduação tem o objetivo de estudar ferramentas para a realização da gestão do risco em pequenas e médias organizações e com base nos pontos falhos encontrados nessas ferramentas e nas informações adquiridas e as diretrizes fornecidas pela Norma ABNT ISO 27005, é desenvolvida a ferramenta ARSI. Os métodos científicos utilizados são a pesquisa descritiva e o básico, enquanto que a abordagem utilizada engloba pesquisas exploratória e explicativa. A partir dessa análise são apresentadas as metodologias utilizadas pelo software, considerações finais do trabalho e sugestões para trabalhos futuros.

Palavras Chave: Segurança da Informação; Gestão de Riscos; Análise de Risco.

ABSTRACT

Currently, information is considered one of the most important assets for an organization, and when classified with this high degree of relevance, it will be subject to threats on several occasions. To protect this asset from threats, Information Security Risk Management is used in which the necessary controls are defined to maintain the risks managed. Currently, organizations deal with a large number of threats that can for the most part be realized due to the lack of a proper process for risk analysis and management. In this sense, this undergraduate work has the objective to study tools for the accomplishment of the risk management in small and medium organizations and based on the flaws found in these tools and in the information acquired and the guidelines provided by the ISO 27005 Standard ABNT, is developed the ARSI tool. The scientific methods used are descriptive and basic research, while the approach used is exploratory and explanatory. From this analysis are presented the methodologies used by the software, final considerations of the work and suggestions for future work.

Keywords: Information Security; Risk Management; Risk Analysis.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ARSI	Arsi Risco em Segurança da Informação
GPL	General Public License
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NBR	Norma Brasileira de Regras
SGSI	Sistema de Gestão da Segurança da Informação
SI	Segurança da Informação
TI	Tecnologia da Informação
URL	Uniform Resource Locator

1 INTRODUÇÃO

O Gerenciamento de Risco dentro de uma organização vem se tornando um tema cada vez mais recorrente, que por meio de um processo visa planejar, organizar, dirigir e controlar os recursos humanos e materiais, com o objetivo de minimizar os riscos, que podem afetar a produção ou o bem estar da organização.

O estudo será realizado com base na norma ISO (International Organization for Standardization) 27005. Esta descreve um processo de Gestão de Riscos e fornece orientações para a construção de um SGSI (Sistema de Gestão da Segurança da Informação).

Com base na norma, dar-se-á início a um estudo de Gestão do Risco, com a construção de uma ferramenta, abordando desde os passos iniciais da Segurança da Informação, até a documentação dos riscos.

O **objetivo geral** é analisar todo o processo de Gestão de Risco nas organizações, registrando a origem dos riscos, classificando e documentando os mesmos.

Como **objetivos específicos** pretende-se descrever como a Gestão de Risco é realizada, projetando uma nova abordagem, rápida e eficaz para pequenas e médias empresas facilitando o registro dos riscos.

O **método científico** utilizado foi à pesquisa descritiva, utilizada para registrar o conhecimento adquirido e correlacionar as tecnologias existentes nos *softwares* em pesquisa. Baseado no resultado dessa pesquisa foi elaborado uma ferramenta, para organizações poderem descrever sobre os riscos de cada ativo, seus causadores e os mecanismos de controle para mitigar o mesmo.

O **problema** encontrado foi que muitas vezes, por falta de recursos ou conhecimento, as organizações se veem obrigadas a desprezar todo o processo de Gestão de Risco, o que no futuro, quando realmente exposto ao risco, poderá gerar um grande impacto na organização.

O estudo **justifica-se**, com o desenvolvimento de uma ferramenta para pequenas organizações, sendo possível, documentar e registrar todos os ativos da

organização, assim como calcular o risco que cada ativo está exposta, registrando controles para combater os riscos caso, os mesmos se concretizem.

A **pergunta** que se buscou responder foi: Como funciona o processo de registrar, classificar e organizar riscos de Segurança da Informação nas organizações?

O trabalho foi estruturado em cinco capítulos, sendo que a partir do segundo conceitua-se a Segurança da Informação e seus aspectos disponibilidade, integridade e confidencialidade.

O terceiro capítulo é mostrado os fatores de Gestão de Riscos da Segurança da Informação, baseando-se na norma ISO 27005 analisando e entendendo como é realizado o processo de análise e avaliação dos riscos.

Durante o quarto capítulo, é apresentado um estudo de caso, que em pesquisa foi relacionado os principais *softwares* de para a Gestão do Risco, levantando seus problemas e pontos falhos.

Com base nas informações conseguidas nos capítulos anteriores e na pesquisa realizada, é descrito sobre a criação de um *software* para a Gestão de Segurança da Informação, reservando assim o capítulo cinco para às considerações finais.

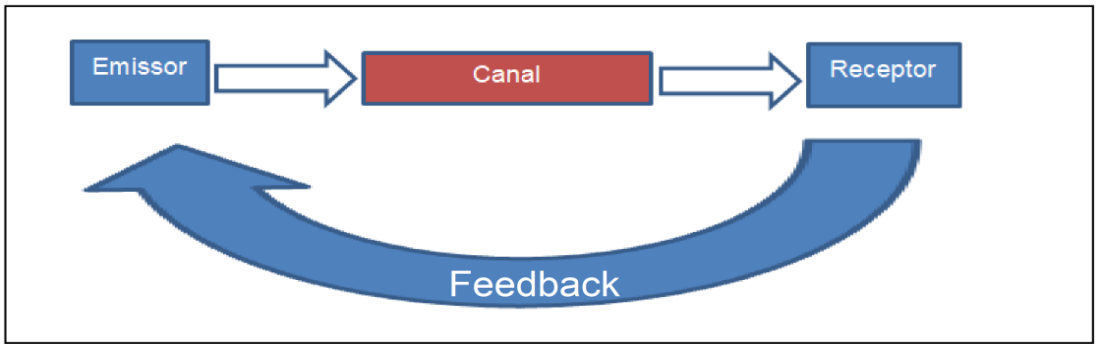
2 SEGURANÇA DA INFORMAÇÃO.

A informação é um conjunto organizado de dados, que ao ser assimilado gera uma mensagem sobre um determinado fenômeno ou evento. Para uma organização, a informação permite resolver problemas, tomar decisões, ou tomar conhecimento sobre acontecimentos, conforme Fontes (2006).

> Informação trata-se de um recurso capaz de mudar o mundo, além de possuir a importante capacidade de fazer com que os seres humanos tenham conhecimento e consigam manter-se informados do que ocorre ao redor do universo. Quando analisada atentamente a história da humanidade revela que o ser humano apenas tornou-se o que é, alcançando o estágio atual, devido a sua eficácia em transformar o recurso informação em outros diversos bens essenciais para a manutenção da vida humana.

O ciclo de vida de uma informação conforme exposto na Figura 1, é chamado de processo de comunicação, em que a informação parte de um emissor, sendo transmitida por um canal de comunicação, até chegar a seu receptor, que é aquele quem decodifica a mensagem, fornecendo o *feedback* ao emissor.

Figura 1 - Processo de comunicação



Fonte: Adaptado pelo autor.

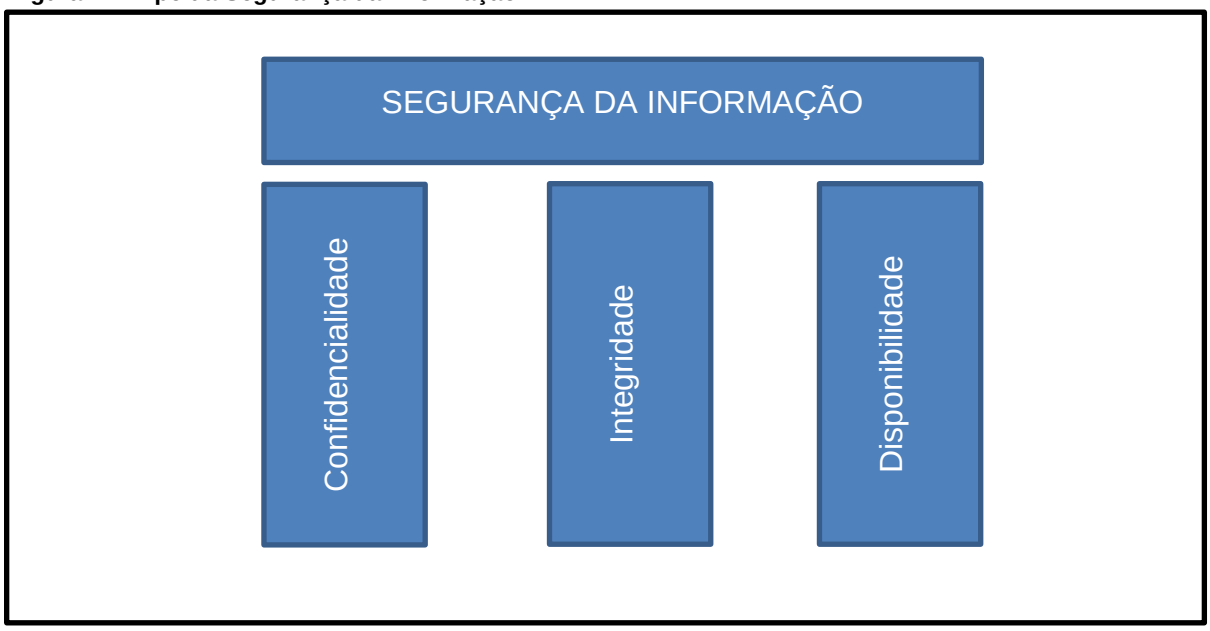
Para que seja possível compreender o conceito de Segurança da Informação (SI), é necessária a elucidação dos elementos e conceitos que compõem a mesma.

Segundo Lyra (2008, p.3)

> [...] Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão alcançada. Esse conjunto de informações hoje é chamado de tripé da Segurança da Informação, sendo eles Confidencialidade, Integridade e disponibilidade [...]

Ao se tratar de Segurança da Informação, deve-se levar em consideração o conjunto: Confidencialidade, integridade e disponibilidade. Também chamado de tripé da Segurança da Informação conforme demonstrado na Figura 2, assim toda ação que tenha como objetivo comprometer qualquer item deste conjunto estará se projetando contra a Segurança da Informação.

Figura 2 - Tripé da Segurança da Informação



Fonte: Adaptado de Lyra (2008).

Confidencialidade é um conceito que faz com que a informação tenha sigilo no mundo corporativo, é muito importante, pois a confidencialidade da informação protege o capital intelectual e por consequência as vantagens competitivas da organização.

> Através da confidencialidade, deve-se assegurar que a informação somente seja acessada ou adquirida por quem está realmente autorizado a tal. “Refere-se à proteção da informação considerada privilegiada contra divulgação não autorizada” (FERREIRA; ARAÚJO, 2008, p.62).

Atualmente toda empresa investe dinheiro e seus recursos para criar conhecimentos de negócio e de operação, recursos esses que podem ser humanos ou tecnológicos, entretanto mantê-los de forma confidencial, pode gerar altos gastos a organização. Esse processo é o motor que possibilita transformar os recursos investidos em lucro do acionista.

Ou seja, confidencialidade significa garantir que a informação estará disponível apenas para quem tem permissão para a mesma.

A **Integridade** visa garantir que a informação armazenada ou que está sendo transferida está correta, e é apresentada corretamente para quem fez a requisição, como afirma Lyra, (2008, p.3).

> Para que seja garantida a Integridade da informação, esta não pode ter sido modificada indevidamente, sendo assim, necessita-se garantir sua credibilidade e exatidão. “A informação deve estar correta, ser verdadeira e não estar corrompida”.

A partir da explosão da Internet, toda organização comunica-se seja internamente ou externamente o tempo todo e para todos os lugares do mundo, transmitindo e recebendo arquivos, essa transferência só acontece quando há um emissor e um receptor da informação.

Durante esse processo a informação pode trafegar em canais de desconhecidos podendo assim, ser interceptada por um alguém mal intencionado, ou até mesmo ser corrompida por efeitos como eletromagnetismo, para evitar isso se cria mecanismos de mitigação e controle de perda de pacotes. Considerando-se o gigantesco e crescente volume de mensagens e dados que circulam atualmente nas empresas e na internet como um todo, a integridade da informação aparece como indispensável, inclusive quando se trata de uma organização.

A falta de integridade da informação em uma rede gera ineficiência no

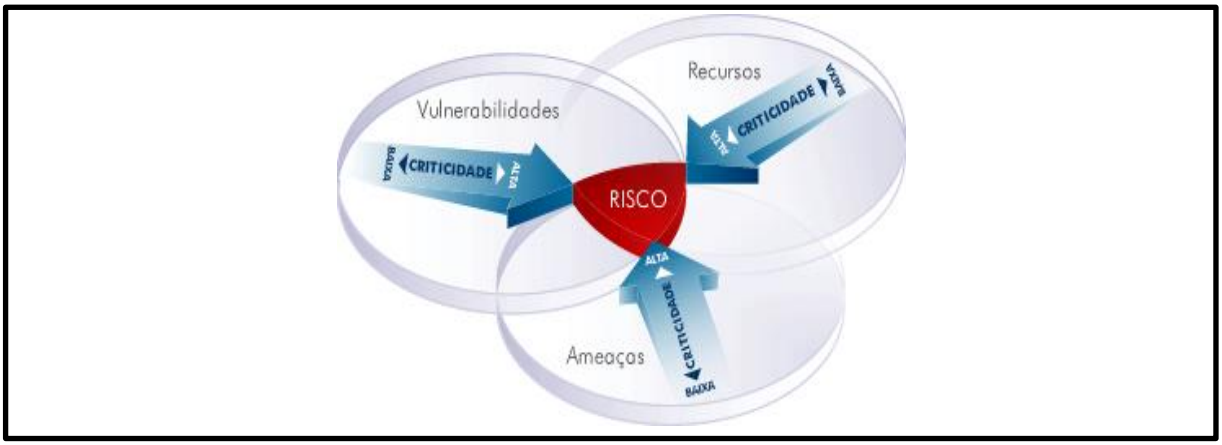
desenvolvimento de atividades, gerando assim, mais custo para ser abatido na receita e, em consequência, trazendo uma menor margem de lucro para a organização.

Por fim a **Disponibilidade** está ligada à questão operacional da empresa, de uma maneira muito mais direta do que a integridade como cita Brandão e Fraga (2007, p.3) “Disponibilidade garante que a informação estará acessível aos usuários legítimos quando solicitada”.

Em diversas organizações praticamente todos os processos de trabalho de uma empresa dependem de chegada ou busca de algumas informações na internet. Quando a informação está indisponível, os processos que dela dependem simplesmente ficam paralisados, assim impactando diretamente na lucratividade do negócio. Ou seja, disponibilidade significa garantir que a informação possa ser obtida sempre que for necessário, estando sempre disponível para quem precisar dela.

Em contrapartida ao tripé da Segurança da Informação demonstrado na Figura 1, aplica-se o risco e seus agentes causadores, como demonstrados na Figura 3.

Figura 3 - Agentes causadores de risco.



Fonte: UFCG.[1]

Os agentes causadores do risco na Segurança da Informação, quando juntos formam o risco.

[1] Disponível em: <http://www.dsc.ufcg.edu.br/~pet/jornal/outubro2011/materias/profissoes.html> acesso em: 11 Set.2017

2.1 Vulnerabilidade

O termo Vulnerabilidade, normalmente é utilizado para designar um ponto fraco ou falha existente em um determinado sistema, que poderá ser explorada de forma proposital ou inadvertidamente, causando prejuízo ao sistema em questão.

Neste contexto Beal (2005), acredita que “vulnerabilidades determinam se um ativo de informação, ambiente está exposto à determinada ameaça”.

Como exemplo de vulnerabilidade, pode-se citar a existência de permissões de acesso inadequadas, o que pode levar a ameaça, ao acesso não autorizado das informações. Entretanto, um ativo também pode estar vulnerável a fatores externos, tais como fogo, inundações, entre outros desastres naturais. Dessa forma, é importante a existência de um ambiente de TI (Tecnologia da Informação) estável, tanto para os *hardwares* quanto para os *softwares*.

2.2 Ameaça

A Ameaça é uma circunstância ou evento cuja verificação ou concretização se traduz em um conjunto de impactos negativos sobre um recurso, que apresenta uma ou mais vulnerabilidades passíveis de serem exploradas pela ameaça em questão.

Segundo Beal (2005, p. 14), ameaça é a “expectativa de acontecimento acidental ou proposital, causado por um agente, que pode afetar um ambiente, sistema ou ativo de informação”.

2.3 Recursos

Os Recursos podem ser classificados como humanos (funcionários) ou tecnológicos (maquinários) e são usados pela organização para produzir o produto vendido pela organização.

Beal (2005, p. 18), classifica recursos como “seus usuários e a gerência que os supervisiona, inclusive a infraestrutura de TI e todos os outros sistemas de informação em uma organização”.

Recursos podem conter vulnerabilidades, em caso de recursos tecnológicos dá-se como exemplo um *firewall* mal configurado, este deve ser classificado como recurso falho.

Nos recursos humanos, grande parte das vulnerabilidades é dada por uma prática chamada de engenharia social, como elucida Mitnick (2005).

> O engenheiro social emprega as mesmas técnicas persuasivas que usamos no dia-a-dia. Assumimos papéis. Tentamos obter credibilidade. Cobramos obrigações recíprocas. Mas, ao contrário da maioria de nós, o engenheiro social aplica essas técnicas de maneira manipuladora, enganosa, altamente antiética e em geral com efeito devastador.

Ou seja, Engenharia Social é a capacidade de uma pessoa, classificada como agente ou ameaça externa, utilizar por meio da exploração da confiança das pessoas, enganação, ou troca da sua personalidade, assim fingindo ser um profissional de determinada área, e ganhando acesso a informações confidenciais da organização.

2.4 Mecanismos de Controle

Para combater o risco, deve-se criar Mecanismos de Controles, esses visam assegurar a informação, caso alguma ameaça explore uma vulnerabilidade. Lyra (2008, p.8) classifica controle como: “qualquer mecanismo utilizado para diminuir as fraquezas (ou vulnerabilidades) de um ativo de Segurança da Informação”.

Como exemplo, dar-se um mecanismo de criptografia, em que caso de uma vulnerabilidade dar acesso às informações para um desconhecido, a mesma estaria criptografada, assim sendo impossível a leitura dos dados sem acesso de chave de criptografia.

Os controles podem ser divididos em físicos ou lógicos:

Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (que garante a existência da informação) que a suporta.

Exemplos de controles de segurança físicos: Portas com trancas, paredes blindadas, guardas e outros.

Controles lógicos: impedem ou limitam o acesso à informação, que está em ambiente controlado, na qual a ausência desse controle o ativo ficaria exposto a alteração não autorizada por elemento mal intencionado.

Exemplos de controles de segurança lógicos: Senhas seguras, firewall de autenticação, e outros.

2.5 Risco

Para Dantas (2011, p.41) o Risco é compreendido como:

> [...] algo que cria oportunidades ou produz perdas. Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas. [...]

O potencial risco é associado à exploração de uma ou mais vulnerabilidades de um recurso ou conjunto, que por parte de uma ou várias ameaças, geram impacto negativo nos recursos afetados, e, por consequência na atividade e negócio da organização.

Beal (2005, p. 14) conceitua impacto como “efeito ou consequência de um ataque ou incidente para a organização”.

Assim as consequências geradas pelo risco são chamadas de impacto sobre o projeto ou o ativo. Esse impacto tem relação direta com o tempo gerencial a ele dedicado ou aos custos relacionados ao mesmo.

Em uma exploração de vulnerabilidade através de uma falha de *software*, na qual pessoas não autorizadas tenham acesso a informações, aumentará a probabilidade de impacto.

Como exemplo de impacto pode-se citar: Divulgação indevida, roubo, uso ilegal da informação, dentre outros.

Este caso trata-se de um risco de gravidade alta, bem como um impacto alto, os quais tendem a intensificar, caso não haja esforço para minimizar o tempo de ocorrência do risco, assim como cita Lyra (2008, p.7). ”Quanto maior o for o valor do

ativo, e o seu tempo exposição ao risco, maior será o impacto de um eventual incidente que possa ocorrer”.

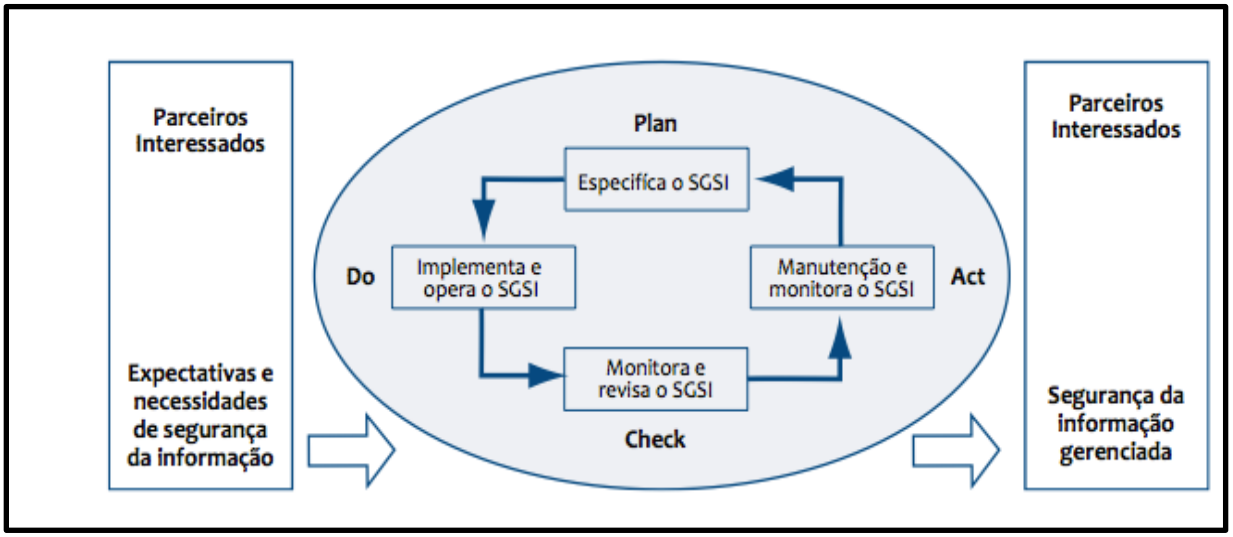
Então conhecendo o risco e seus agentes causadores, podem-se ser criados métodos para controlá-lo, Esses métodos são estudados na Gestão do Risco.

3 GESTÃO DO RISCO

Primeiramente deve-se compreender como funciona o processo de Gerenciamento de Risco, o mesmo está diretamente ligado aos perigos e oportunidades que afetam a criação, preservação e mantimento dos ativos de TI, sendo definido como um processo conduzido em uma organização, por equipes do SGSI (Sistema de Gestão da Segurança da Informação)

Segundo a normativa Brasileira ISO/IEC 27005 ABNT (2011), um Sistema de Gestão da Segurança da Informação deve-se utilizar o PDCA, como demonstrado na Figura 4, para estruturar os processos do sistema.

Figura 4 - PDCA aplicado à SGSI



Fonte: (ABNT, 2011)

O ciclo PDCA é um método de gestão, que orienta o processo de tomada de decisão, além de estabelecer as metas, meios e ações necessárias para executá-las e acompanhá-las garantem a sobrevivência e crescimento do negócio.

Segundo Dantas (2011, p.79). “Esta fase alcança as atividades que previnem e corrigem as falhas e deficiências encontradas durante o monitoramento e a revisão (análise crítica). É nela que são executadas as ações preventivas e corretivas”.

O processo do PDCA na Gestão do Risco inicia-se através de duas partes interessadas em se chegar à Segurança da Informação, primeiramente definem os requisitos e as expectativas de segurança, em seguida, é iniciado um procedimento cíclico de gestão baseado no ciclo do PDCA, que é composto de quatro etapas.

Deve-se dar início com a etapa Plano (*Plan*), estabelecendo as políticas, dos objetivos, dos processos e dos procedimentos do SGSI, que tenham relevância no processo de Gestão de Riscos e a melhoria da Segurança da Informação e que produzam resultados de acordo com as políticas e objetivos estabelecidos em uma organização.

A segunda etapa fazer (*Do*) envolve a implantação e a operação da política, dos controles, das fases e dos procedimentos estabelecidos na primeira etapa.

Na terceira etapa chamada de checagem (*Check*), é realizada a avaliação, quanto aos objetivos estabelecidos na primeira etapa, verificando e registrando possíveis ações a serem corrigidas que ocorrem no próximo passo.

Na quarta etapa ação (*Act*), cabe a execução das ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI ou outra informação pertinente que foi encontrada durante o passo anterior, para alcançar a melhoria contínua do SGSI.

O resultado esperado após algumas rotações do ciclo PDCA, mantendo e melhorando o resultado do ciclo anterior, é um sistema de gestão da Segurança da Informação solidamente implantado.

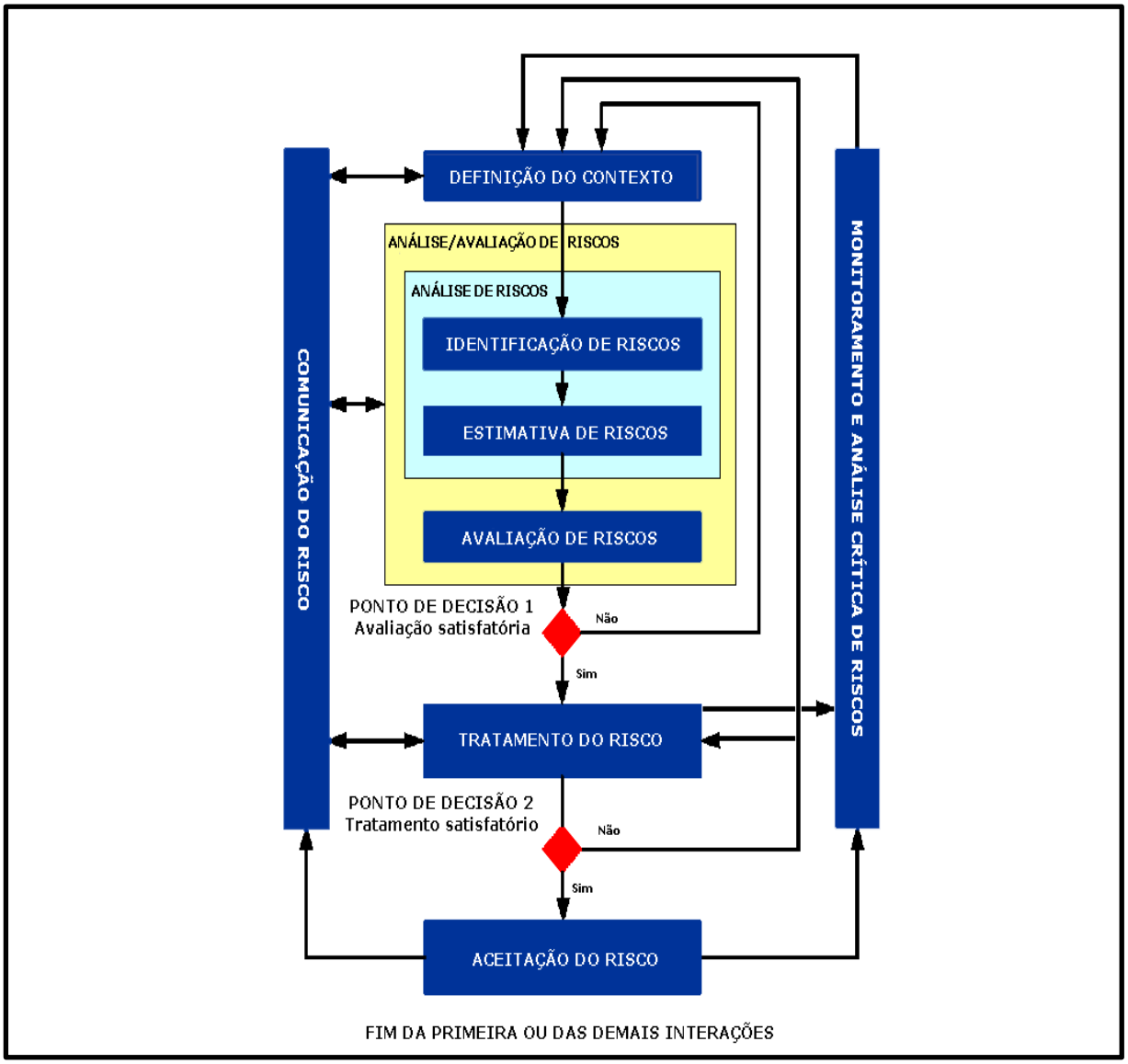
3.1 Processos de Gestão de Riscos

Embora seja impossível uma organização prever e se prevenir de todos os ataques é possível se prevenir de ataques conhecidos, e se tornar capaz de responder rapidamente as ameaças.

A Gestão de Risco trabalha exatamente em definir um conjunto de ações estratégicas, como identificação, administração, condução e prevenção dos riscos ligados a uma determinada atividade.

O ponto de partida para a implementação de um sistema de Gestão dos Riscos em Segurança da Informação em uma organização é a definição do contexto. De acordo com as diretrizes fornecidas na figura 5, a seguir, fornecida pela ISO/IEC 27005 ABNT (2011).

Figura 5 - Processo de Gestão de Riscos



Fonte: (ABNT ISO/IEC 27005:2011)

Essas diretrizes fornecidas devem estar contidas dentro da fase Plano no ciclo

PDCA. No devido momento abordaremos apenas a etapa de análise/avaliação de riscos, pois contém a metodologia para a estimativa de riscos.

3.2 Definição do Contexto

A definição do contexto em Segurança da Informação tenta definir os parâmetros básicos, para identificar os ativos que necessitam da Gestão de Risco assim criando um escopo do nosso sistema na qual podem estar presentes os riscos.

> É nesta fase que são identificados o cenário (ambiente interno e externo), as metas da avaliação e são definidos os critérios segundo os quais os riscos serão avaliados (DANTAS, 2011)

Para a definição de contexto deve ser levado em questão todas as informações relevantes sobre a organização, que sejam realmente pertinentes para manter o bem estar das informações da organização.

Outro importante aspecto é a definição dos critérios que serão usados na determinação dos riscos do projeto. Estes critérios envolvem a categorização das consequências de segurança e os métodos usados para a análise e avaliação dos riscos.

3.3 Identificação dos Riscos

Segundo Dantas (2011), “é nesta fase que os eventos são identificados com as suas probabilidades e consequências, ou seja, é a fase da identificação dos riscos, uma vez que os riscos são medidos pelas suas probabilidades e consequências”.

Nesta etapa ocorre a busca, descrição, e reconhecimento de riscos, gerando uma documentação dos riscos e ameaças relacionadas a possíveis eventos que possam aumentar, diminuir, acelerar ou atrasar o funcionamento dos itens adotados no contexto.

É de grande importância que todos os riscos sejam identificados, pois os riscos não identificados não serão analisados nem tratados.

3.4 Estimativas de Riscos

Na etapa de Análise de Riscos, são reunidos todos os dados do ativo, esse conjunto irá auxiliar na tomada de decisão sobre quais riscos serão tratados e as formas de tratamento dos mesmos. Esse conjunto contém uma metodologia que envolve a origem dos riscos, suas consequências e as probabilidades de ocorrência dos mesmos gerando assim uma classificação do risco ou ativo.

Dantas (2011, p.80) descreve algumas atividades para a identificação dos riscos.

> Para se analisarem os riscos são desenvolvidas as seguintes atividades: a identificação dos riscos; a identificação dos requisitos legais e de negócios que são relevantes para os ativos identificados; a valoração dos ativos identificados, considerando a classificação dos seus requisitos e as expectativas de perda de confidencialidade, integridade e disponibilidade; a identificação das principais ameaças e vulnerabilidades; a avaliação da possibilidade de ameaças e vulnerabilidades ocorrerem.

Essas atividades são definidas como uma metodologia de estimativa, esta pode ser qualitativa, quantitativa ou uma combinação de ambas, dependendo das circunstâncias.

A estimativa qualitativa utiliza uma escala com atributos qualificadores que descrevem a magnitude das potenciais consequências e a probabilidade destas consequências ocorrerem. A estimativa quantitativa adota uma escala de valores numéricos tanto para consequências, quanto para a probabilidade.

Ou seja, a análise de risco registra a probabilidade de aquilo acontecer e o impacto que isso acarretará se acontecer.

3.5 Análises de Riscos

A Análise de Riscos é uma estimativa das fontes e as causas dos riscos de cada ativo, assim como suas consequências que podem ser positivas ou negativas, e a probabilidade de que essas consequências possam ocorrer, Portanto, a etapa de

Análise de Riscos pretende entender e classificar a probabilidade de que o risco venha a acontecer e o impacto no negócio que isso irá gerar se acontecer.

Dantas (2011) sugere que nesta etapa, “os riscos sejam identificados, analisados e avaliados de acordo com critérios previamente estabelecidos”.

3.6 Tratamentos, Comunicação e Monitoramento.

Ao lado dessa sequência temos processos auxiliares, esses devem funcionar interativamente, fornecendo e compartilhando informações com os parceiros interessados, como demonstrados na Figura 4. Este processo é chamado de Comunicação do Risco.

A Análise Crítica é a atividade realizada para determinar a adequação, de um objetivo específico, fazendo com que o processo de gestão entre em um *loop*, então se caso o ativo definido no contexto, não atenda os requisitos de tratamento, o ativo irá retornar ao início do processo.

Nesse momento o monitoramento irá se unir a análise crítica formando um processo contínuo de verificação, supervisão, observação crítica da situação para identificar mudanças.

Dantas (2011) descreve monitoramento como “quando ocorre o monitoramento de todas as atividades de controle, de modo a se fazerem as alterações necessárias ao gerenciamento dos riscos de TI”.

É Importante visar que a probabilidade e impacto estabelecidos podem a qualquer momento mudar, conforme ocorre o processo de comunicação, assim mudando completamente o risco. Com isso pode-se notar a dificuldade de trabalhar com diversos ativos, em um processo longo, podendo ser alterado a qualquer momento, para isso utilizamos ferramentas que auxiliam essa tarefa.

4 FERRAMENTAS DE GESTÃO DE RISCO

Para esta pesquisa foram selecionados *softwares* populares para ajudar o setor de TI na tarefa de avaliar, dimensionar e documentar os riscos.

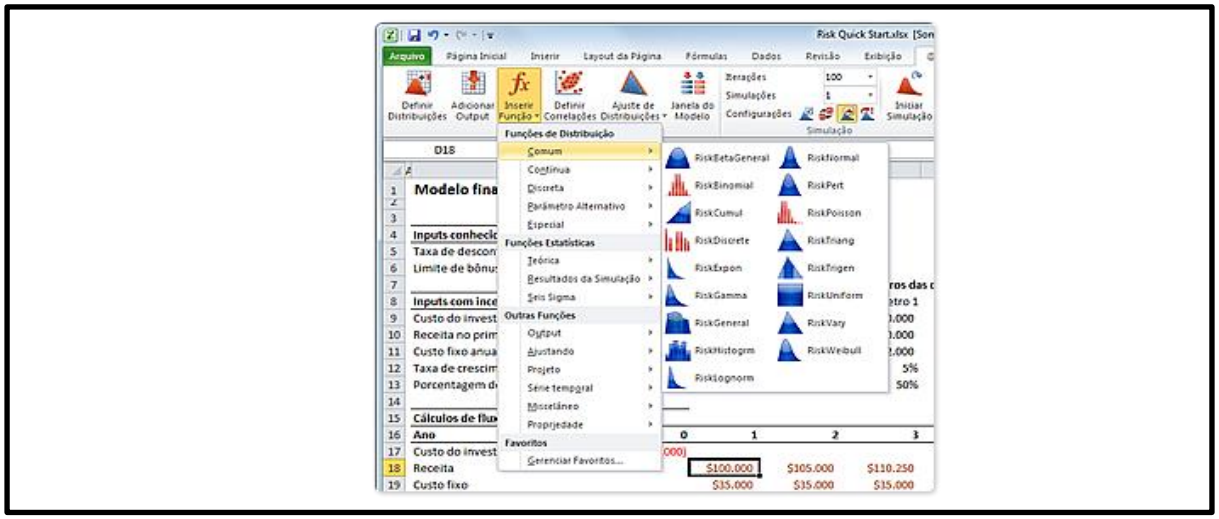
Todos os *softwares* foram estudados com base em suas versões de testes, também importante frisar que empresas que realizam análises e matriz de risco habitualmente podem ter sua própria ferramenta interna, e não serão analisadas aqui.

4.1 Ferramentas de Gestão de Riscos.

O sistema @Risk exibido na Figura 6, é desenvolvido pela empresa Palisade, trata-se de um complemento para a ferramenta Microsoft Excel, acrescentando funções que permite a efetuação de cálculos, voltados para gestão da Segurança da Informação, permitindo rastrear diversos cenários futuros, em seguida, são informados as probabilidades e riscos associados a cada cenário.

Dando assim, condições de avaliar se deseja aceitar ou evitar o risco, e com base nisso, tomar as melhores decisões possíveis em situações de incerteza.

Figura 6 - Sistema @Risk



Fonte: Paralisade [2]

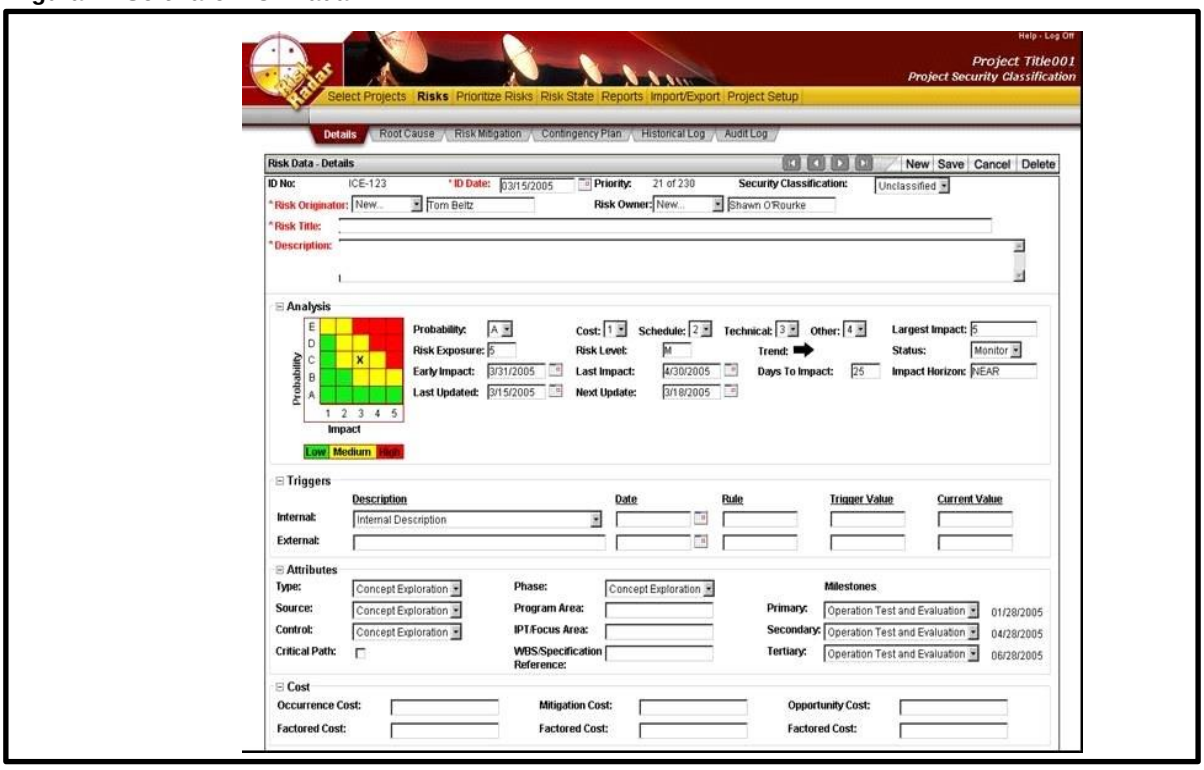
Durante todo o uso do *software*, coloca-se em consideração o fácil gerenciamento das informações inseridas, na qual um usuário com conhecimentos básicos na em Microsoft Excel, teria facilidades ao utilizar a ferramenta.

[2] Disponível em: <http://www.palisade-br.com/risk/> Acesso em: 21 set.2017.

Em contraproposta a essas facilidades, pode-se colocar a forma de armazenamento das informações, cuja uma simples chave de acesso garante o acesso aos dados. Também se pode colocar em questão a dificuldade de cadastro de um alto número de ativos, tornando a tarefa a ser realizada repetitiva e exaustiva.

O Risk Radar desenvolvido pela empresa Radar Enterprise é um banco de dados de gerenciamento de riscos que visa identificar, priorizar e comunicar os riscos da Segurança da Informação como demonstrado na Figura 7.

Figura 7 - Software Risk Radar



Fonte: Risk Radar. [3]

[3] Disponível em: <https://www.projectmanagement.com/tools/329924/Risk-Radar-Enterprise->. Acesso em: 23 set.2017

Após realizar a utilização do *software*, foi registrada dificuldade na utilização da interface gráfica, assim como uma excessiva quantidade informação requerida para um ativo, o que torna a tarefa a ser realizada repetitiva e cansativa.

O Módulo Risk Manager, demonstrado na Figura 8 pode ser integrado com diversos scanners de vulnerabilidades como Qualys, Nessus e Rapid7. Desta forma o *software* recebe automaticamente os ativos e as vulnerabilidades coletadas por meio de varreduras do scanner. As informações são agregadas ao Módulo Risk Manager, centralizando e facilitando análise, avaliação e tratamento dos riscos tecnológicos.

Figura 8 - Software Módulo Risk Manager

Fonte: Módulo Risk Manager[4]

Desenvolvida pela empresa Módulo, a ferramenta Módulo Risk Manager possui diversas características o que o classifica como melhor *software* dentre os testados. Oferecendo uma solução inovadora de gestão da Segurança da Informação através do monitoramento contínuo e proativo. A solução automatiza o inventário, a coleta de

[4] Disponível em: <http://www.modulo.com.br/gestao-de-riscos- corporativos-e-operacionais/)>. Acesso em: 23 set.2017.

dados dos ativos tecnológicos, a análise e a geração de relatórios com métricas e indicadores, além de programar um *workflow* para tratamento dos riscos.

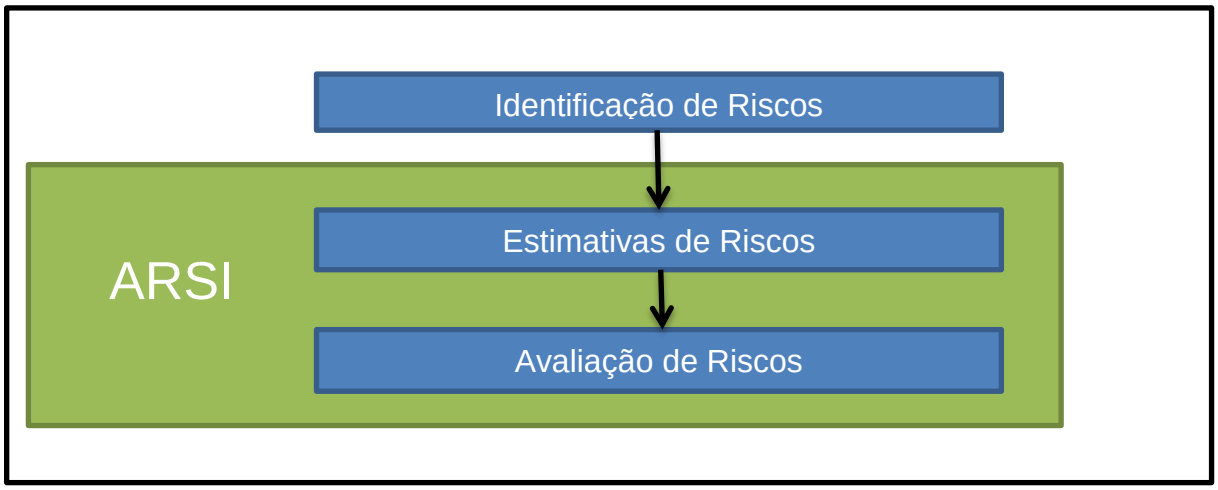
Embora classificado como melhor *software*, analisado até aqui, o mesmo possui um preço elevado, o que o torna inviável para pequenas e médias organizações, além de conter muitas funções avançadas, sendo assim necessário um profissional especializado para utilizá-lo.

5 ESTUDO DE CASO - DESENVOLVIMENTO DA FERRAMENTA

Após analisar os aplicativos existentes no mercado, notou-se alguns problemas, como a falta de um software de fácil acesso para pequenas organizações, e que não exija conhecimento muito abrangente do assunto.

Partindo do resultado desta pesquisa, foi desenvolvido um *software* chamado ARSI (Arsi Risco em Segurança da Informação), que alinhado ao seu processo descrito fornece uma rápida resposta aos riscos. Esta abordagem segue as diretrizes da norma ABNT ISO 27005 e o seu processo de Gestão de Risco, mas especificamente no processo de estimativas e Avaliação de Riscos como demonstrado na Figura 9.

Figura 9 - Processo de SI abordado pela ferramenta ARSI



Fonte: Próprio Autor

Cada organização pode vir a apresentar peculiaridades no que tange a técnicas e controles para Gestão de Riscos de Segurança da Informação e comunicações necessitando assim de requisitos auxiliares nos cadastros dos ativos em questão.

A solução encontrada para esse problema é um banco de dados com requisitos e métricas pré-cadastradas, tornando possível a utilização de uma métrica em diversos ativos de uma empresa.

O *software* utiliza a linguagem PHP (*Php Hypertext Preprocessor*) como *backend*, trabalhando com o framework *laravel*, e a linguagem SQL (*Structured Query Language*) para conexão com o banco de dados. Para a exportação do relatório e utilizada a biblioteca *PHPtoPDF* transformando a tela do *software* em PDF, possibilitando o compartilhamento de informações.

A arquitetura está separada em camadas distintas, esse padrão é chamado de MVC (Model - View - Controller):

A camada modelo (*Model*) é quem faz o acesso ao banco de dados, sendo responsável pela parte de gravação, edição e consultas ás informações que forem gravadas no banco de dados.

O Controle *(Controller) é* a camada que trata do cálculo e da probabilidade e impacto dos riscos dos ativos, esta pode ser alterada a qualquer momento, caso a metodologia utilizada, venha a ser alterado futuramente, toda essa função é executada no *backend* através da linguagem PHP.

Agregado a camada controle é utilizada a biblioteca MPDF, responsável em codificar os dados para o formato de PDF. Assim como a extensão *google charts tools,* que deve converter alguns dados da aplicação para gráficos, tornando mais fácil a leitura.

A camada de visualização (*View*), irá tratar da *interface* com o usuário, nesta camada foi utilizado o *framework Bootstrap 4*, fornecendo componentes HTML, CSS, Javascript.

Embora o *software* trabalhe sobre o protocolo HTTP (*Hypertext Transfer Protocol*), não é recomendada a disponibilização de acesso para a rede externa (internet), apenas a rede interna da organização, visto que a o *software* se apresenta em fase inicial, e concentra todos os riscos da sua organização.

5.1 Métricas

As métricas adotadas aqui são embasadas nos exemplos fornecidos pela ISO/IEC 27005 ABNT (2011). Esta metodologia faz uso de uma série de parâmetros

para calcular uma pontuação (*score*), que irá definir o grau de risco de uma determinada vulnerabilidade.

O sistema possui uma funcionalidade para calcular a relação probabilidade de impacto dentro das informações inseridas pelo usuário, gerando as informações de cálculo de risco através da seguinte fórmula:

Risco = Probabilidade x Impacto

Também é possível realizar a validação e o cálculo do risco conforme a seguinte escala de probabilidade de ameaças: Baixa, Média ou Alta. Para cada uma das escalas, obtêm-se os seguintes valores a serem representados: Baixa (de 1 a 4), Média (maior que 4 até 9) e Alta (maior que 9 até 25).

Para seguir as definições de valores dos níveis dos riscos, deverá ser seguida a tabela 1 - Matriz de Nível de Risco, a qual apresenta a localização dos valores em que eles se enquadram, para cada um dos níveis.

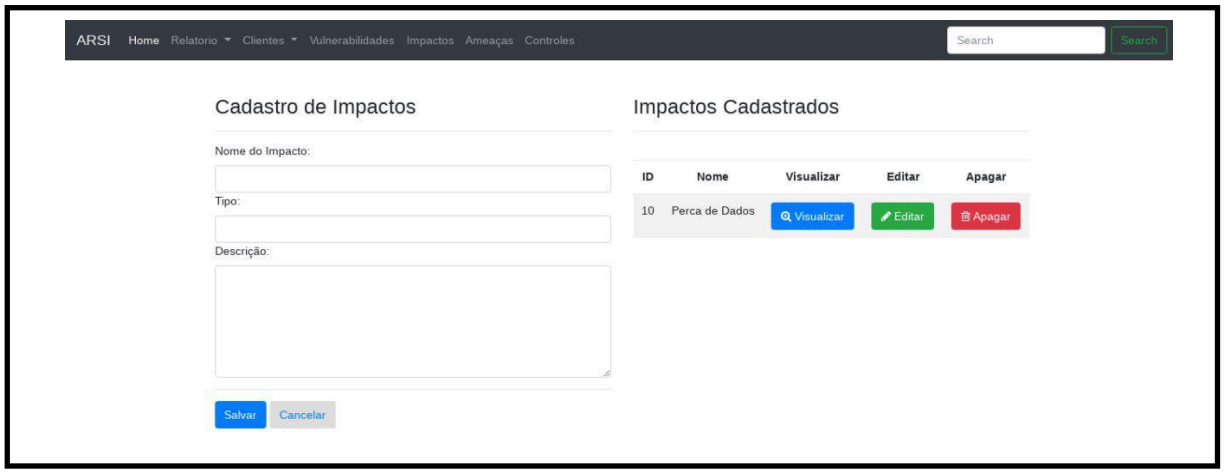
Tabela 1 – Matriz de Risco

Risco = Probabilidade x Impacto						
PROBABILIDADE	1	5	4	3	2	1
	2	10	8	6	4	2
	3	15	12	9	6	3
	4	20	16	12	8	4
	5	25	20	15	10	5
		5	4	3	2	1
IMPACTO						

Fonte: Próprio Autor

Outras métricas a serem inseridas no *software* são: Controles, ameaças, vulnerabilidades e riscos conhecidos. Cada um conta com uma página para cadastro e visualização, sendo possível cadastrar um nome, tipo e descrição de cada métrica como demonstrado na Figura 10.

Figura 10 - Tela de cadastro de impactos ARSI



Fonte: Próprio Autor

5.2 Instalação e Utilização

O *software* ARSI pode ser obtido gratuitamente na plataforma de apoio digital Github disponível a todos através da licença GPL *(General Public License).* Após realizar o download, devemos iniciá-lo através da *interface* de comando como demonstrado na Figura 11. Ao final da instalação será exibido a URL (*Uniform Resource Locator*) de acesso ao *software*.

Figura 11 – Instalação e Inicialização

Fonte: Próprio Autor

Ao se realizar o primeiro acesso, será exibida a tela de configuração da aplicação, na qual informações para a conexão com o banco de dados serão requeridas, conforme demonstrado na Figura 12.

Figura 12 - Configuração da base de dados

Fonte: Próprio Autor

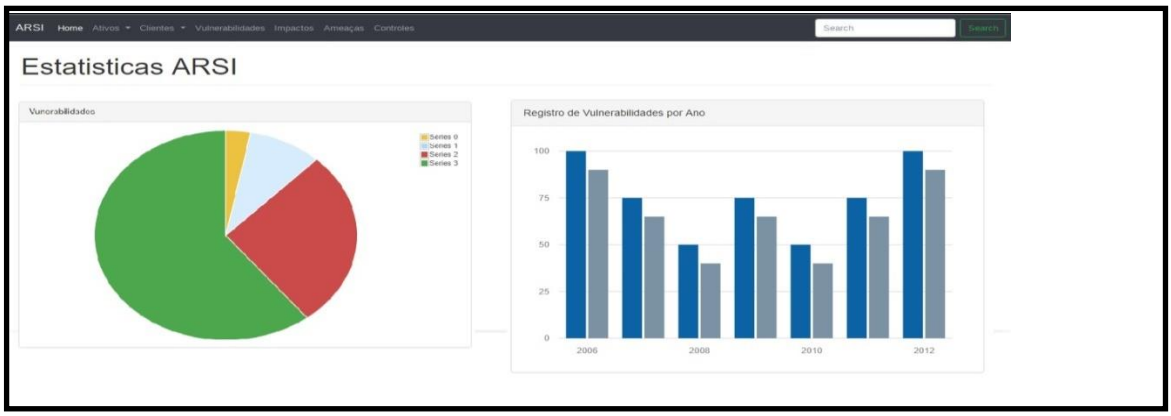
Caso a máquina na qual o sistema será instalado não atenda os requisitos mínimos para instalação, será exibida uma tela com o requisito recusado, caso contrário, como demonstrado na Figura 13 à instalação é concluída.

Figura 13 - Requisitos Mínimos

Fonte: Próprio Autor

Ao acessar a tela inicial da aplicação é demonstrado alguns gráficos, em que é possível analisar quais as métricas com mais ocorrências até o devido momento, como demonstrado na Figura 14.

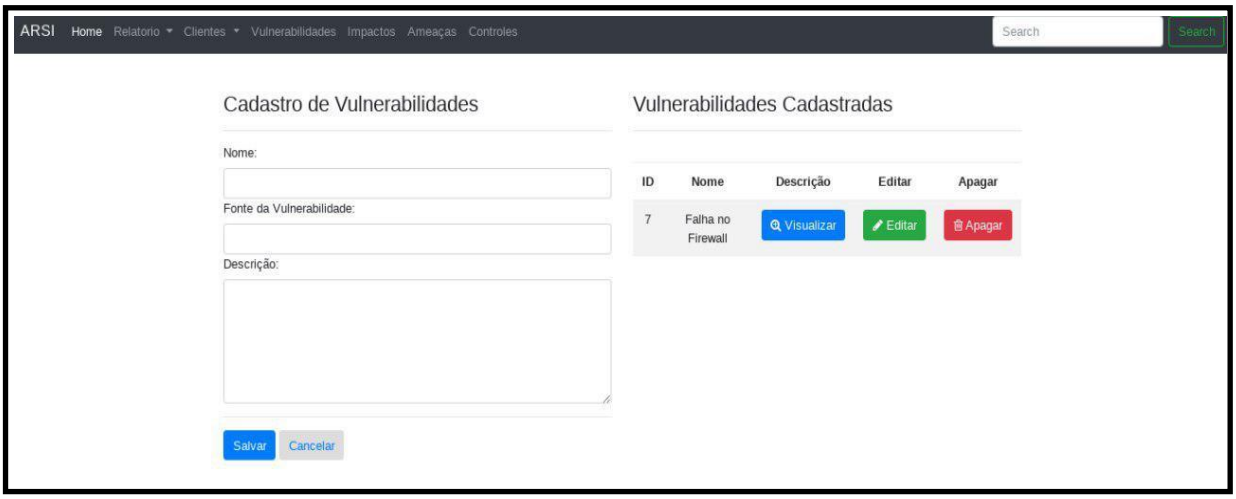
Figura 14 - Tela Inicial da Aplicação



Fonte: Próprio Autor

Em todo o superior da tela, é exibido o menu da aplicação, o primeiro passo para utilização do software é o cadastro das métricas, como exemplo na Figura 15, sendo possível o cadastro de uma vulnerabilidade.

Figura 15 - Tela de Cadastro das Métricas

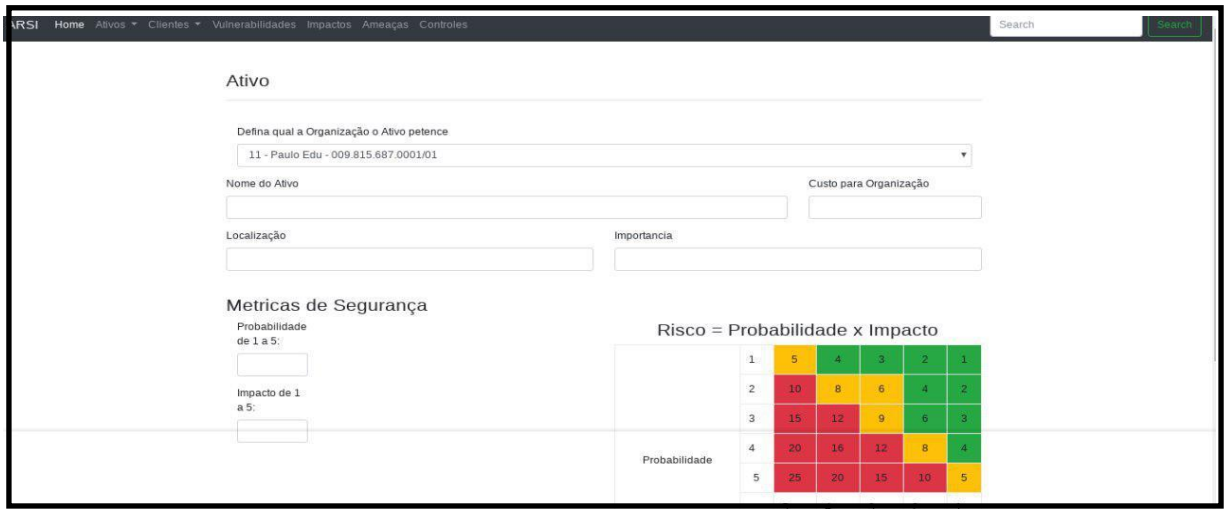


Fonte: Próprio Autor

Ao se preencher os campos exibidos, pode-se salvar os dados através de um botão no final da página, As informações cadastradas, serão exibidas na tabela ao lado, nesta também é possível editar e deletar as informações.

Após o cadastro de ao menos uma métrica no *software*, já podemos dar início ao cadastro de nossos ativos, acessando a aba novo ativo e preenchendo os campos, como exibidos na Figura 16.

Figura 16 - Tela de cadastro de ativos ARSI



Fonte: Próprio Autor

O primeiro passo é definir a qual organização o ativo pertence, definindo também um nome, custo, localização dentro da organização, e importância do ativo para a organização.

Em seguida pode-se calcular uma métrica quantitativa, deve-se inserir a probabilidade do risco ocorrer e o impacto caso o mesmo ocorra, classificando-os de 1 a 5.

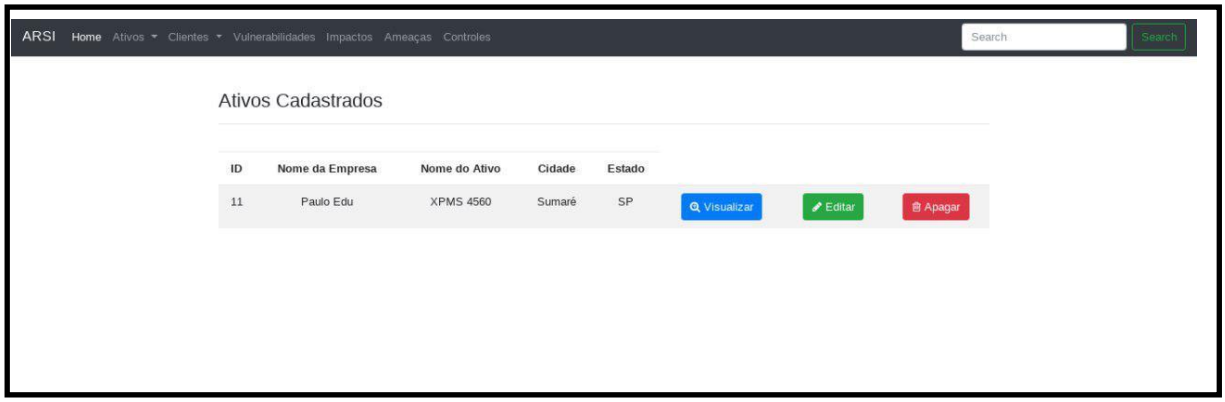
Logo após, pode-se selecionar as métricas cadastradas previamente no software e finalizar o cadastro do ativo clicando no botão salvar, como demonstrado na Figura 17.

Figura 17 - Associação de métricas e ativos ARSI

Fonte: Próprio Autor

A visualização do ativo cadastrado, pode ser acessada através do sub menu, da aba ativos, assim sendo possível, como demonstrado na Figura 18 é possível, apagar, editar e compartilhar o ativo.

Figura 18 - Visualização dos Ativos



Fonte: Próprio Autor

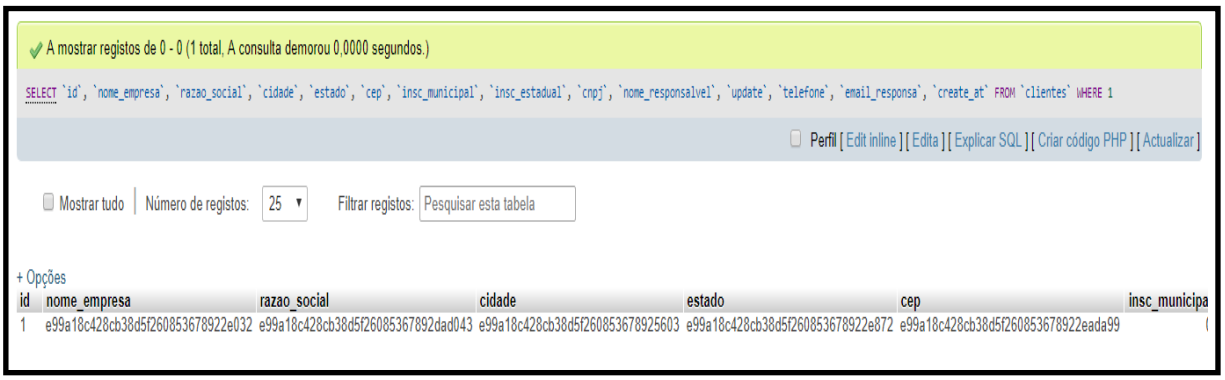
5.3 Segurança

Ao desenvolver um *software* que trabalhe com informações sensíveis devem-se tomar medidas de segurança, pois ao se centralizar todas as informações críticas da organização em um único lugar, geramos um novo risco.

Para controlar este risco, deve-se tomar algumas medidas de seguranças,

implantada em nosso *software*. Toda e qualquer informação que for inserida no *software*, automaticamente passa por uma função de encriptação do tipo SHA1(*Secure Hash Algorithm 1*), tornando todo e qualquer um dos dados salvos criptografado e ilegível fora do *software*, como demonstra a Figura 19.

Figura 19 - Banco de dados criptografado



Fonte: Próprio Autor

Muitas vezes, as informações presentes no *software* necessitam de ser compartilhadas, assim sendo possível através da exportação de arquivos no formato PDF, conforme documento demonstrado no Apêndice A, dessa maneira qualquer pessoa que deseja visualizar deve ter uma senha para o acesso ao arquivo.

CONSIDERAÇÕES FINAIS

Em virtude dos conceitos de segurança e risco estudados até aqui, pode-se concluir que praticar a Gestão do Risco é essencial para mitigar o risco e ter um tempo de resposta, caso o mesmo venha a ocorrer.

Com o intuito de se criar uma nova abordagem para realizar a Gestão de Risco, foi utilizado um processo fornecido pela NBR ISO/IEC 27001 ABNT (2005), chamado de PDCA, que visa manter um processo em um ciclo, sempre criando melhorias para o ciclo anterior. Mesclando com as diretrizes fornecidas pela ABNT ISO/IEC 27005 (2011), chamado de processo de Gestão de Risco. Este que visa ordenadamente definir o escopo da organização, identificar os riscos, analisá-los e tratá-los caso necessário.

Em um estudo de caso, foram levantadas três principais ferramentas que auxiliam na Gestão de Risco onde em todos foi possível observar pontos que dificultam o acesso para organizações que estão iniciando suas atividades.

Baseando-se nos pontos falhos observados, foi desenvolvida uma nova ferramenta para Gestão de Risco, focando em facilidades na utilização para pequenas e médias organizações.

Com esta ferramenta, pequenas e médias empresas, tem seus passos inicias para resolver o problema levantado, já agora é possível que a organização evite gastos com compras, ou desenvolvimento de ferramentas próprias. Além de não exigir um profissional, especializado para dar início ao processo de Gestão do Risco.

Embora esse processo já forneça o essencial para Gestão do Risco, é importante lembrar que com o crescimento da organização, novas exigências serão necessárias ao se cadastrar cada ativo. Então, desde que, dentro da GPL, nada impede de que o sistema seja modificado para atender as novas necessidades.

O *software* ARSI embora já atenda as necessidades levantadas, ainda carece de muitas atualizações, como uma documentação que demonstre como utilizar a mesma, um ambiente virtual com a ferramenta já instalada disponível para *download,* facilitando assim a instalação para leigos, dentre outras.

Portanto pode-se concluir que um processo de Gestão de Risco, se aplicado corretamente, pode salvar ou diminuir o impacto gerado na organização. Também notou-se que utilizar um *software* para auxiliar esta gestão além agilizar o processo de documentação do risco, torna mais fácil as atualizações e acesso as informações.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:** Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação. Rio de Janeiro: ABNT, 2005. 120 p.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS**. ABNT NBR ISO/IEC 27001**: Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de Segurança da Informação- Requisitos. Rio de Janeiro: ABNT, 2006. 34 p.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

Brandão, José Eduardo Malta de Sá. Fraga, Joni da Silva. **Gestão de Risco**, 1 Instituto de Pesquisa Econômica Aplicada (IPEA), Brasília DF, 2011. 43p.

DANTAS, Marcus Leal. **Segurança da Informação:** Uma Abordagem Focada em Gestão de Riscos. Olinda: Livro Rápido, 2011. 150 p.

IMONIANA, Joshua Onome**. Auditoria de sistema de informação**. 2º edição. São Paulo: Atlas S.A.. 2013. 203p.

FERREIRA, F.; ARAUJO, M. **Política de segurança da informação:** Guia prático para elaboração e implementação. 2. ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

FONTES, Edilson. **Praticando a Segurança da Informação.** Rio de Janeiro: Brasport, 2008. 283p.

LYRA, Mauricio Rocha. **Segurança e Auditoria em Sistema de Informação**. Rio de Janeiro: Ciência Moderna. 2008. 240p.

MITNICK, K.; SIMON, W. **A arte de enganar.** São Paulo: Makron Books, 2003. 203p.

MODULO. **Soluções para gestão integrada.** Disponível em: < http://www.modulo.com.br/gestao-de-riscos- corporativos-e-operacionais/)>. Acesso em: 23 set.2017.

PARALISADE. **Fabricante do software líder mundial em análise de risco e de decisão,** (2017)**.** Disponível em: <http://www.palisade-br.com/risk/> . Acesso em: 21 set.2017.

RISK RADAR ENTERPRISE. **Risk Radar® Enterprise (RRE) is an easy-to-use web application**. Disponível em: < https://www.projectmanagement.com/tools/329924/Risk-Radar-Enterprise->. Acesso em: 23 set.2017

APÊNDICE A – PDF exportado pela ferramenta ARSI.

ARSI

Dados da Organização

Nome:

Razão Social:

Cidade:

Estado:

CNPJ:

Responsável:

Telefone:

Dados do Ativo

Nome:

Localização:

Importância:

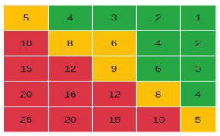
Valor:

Matriz de Risco

Probabilidade:

Impacto:

Risco:



Vulnerabilidades

Descrição:

Impacto

Descrição:

Ameaças

Descrição:

Controles

Descrição: