UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

DHIÊGO RHUBENS LIMA SAMPAIO

UM ESTUDO SOBRE RISCOS DE SEGURANÇA DA INFORMAÇÃO NO CAMPUS DA UFC EM QUIXADÁ COM BASE NA NORMA ISO/IEC 27005

QUIXADÁ
2014

DHIÊGO RHUBENS LIMA SAMPAIO

UM ESTUDO SOBRE RISCOS DE SEGURANÇA DA INFORMAÇÃO NO CAMPUS DA UFC EM QUIXADÁ COM BASE NA NORMA ISO/IEC 27005

Trabalho de Conclusão de Curso submetido à Coordenação do Curso Bacharelado em Sistemas de Informação da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Bacharel.

Área de concentração: computação

Orientador Prof. Alberto Sampaio Lima

QUIXADÁ
2014

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Campus de Quixadá

S181e Sampaio, Dhiêgo Rhubens Lima
Um estudo sobre riscos de segurança da informação no campus da UFC em Quixadá com base na norma ISO/IEC 27005. – 2014.
51 f. : il. color., enc. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Sistemas de Informação, Quixadá, 2014.
Orientação: Prof. Dr. Alberto Sampaio Lima
Área de concentração: Computação

1. Tecnologia - Serviços de informação 2. Sistemas de informação gerencial – Medidas de segurança 3. Tecnologia da Informação I. Título.

CDD 658.4038

DHIÊGO RHUBENS LIMA SAMPAIO

UM ESTUDO SOBRE RISCOS DE SEGURANÇA DA INFORMAÇÃO NO CAMPUS DA UFC EM QUIXADÁ COM BASE NA NORMA ISO/IEC 27005

Trabalho de Conclusão de Curso submetido à Coordenação do Curso Bacharelado em Sistemas de Informação da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Bacharel.

Área de concentração: computação

Aprovado em: _____ / maio / 2014.

BANCA EXAMINADORA

_____
Prof. Dr. Alberto Sampaio Lima (Orientador)
Universidade Federal do Ceará-UFC

_____
Prof. Ms. José Moraes Feitosa
Universidade Federal do Ceará-UFC

_____
Prof. Dr. Lincoln Souza Rocha
Universidade Federal do Ceará-UFC

Dedico este trabalho à minha amada mãe Derlene Ferreira Lima, pois sem ela eu não teria chegado até aqui. E também dedico ao prof. Alberto Sampaio Lima, por ter me acolhido como seu orientando em um momento conturbado para mim.

"O homem verdadeiro faz o que quer, não o que deve."
(*George R. R. Martin*)

RESUMO

A falta de segurança é um termo que vem ultrapassando os limites de uma organização, porque pode ser administrado a pessoas, tecnologia, processos e inclusive a informação. Dificuldades decorrentes da ausência de confidencialidade, autenticidade, integridade e disponibilidade em sistemas de informação levam à exigência de implantar ações de segurança nas organizações. Este trabalho utiliza um modelo introdutório de verificação de riscos da segurança da informação, suficiente para identificar os riscos de impacto com alta potencialidade em uma organização. A gestão de riscos é responsável pelo processo de avaliação de riscos para identificar os riscos e seus elementos, categorizando-os em níveis. É indicado pela norma ISO/IEC 27005 começar o processo de gestão de riscos a partir de uma análise com uma alta perspectiva visando os riscos cruciais do negócio. Partindo dos resultados dessa abordagem inicial é viável a definição das propriedades, detalhando os possíveis riscos em potencial. O aspecto desse trabalho tem as regras da ISO/IEC 27005 como base.

Palavras chave: Segurança da Informação. Normas e padrões de segurança. Gestão de riscos de segurança da informação.

SUMÁRIO

1 INTRODUÇÃO

No mundo atual, onde a informação possui um valor altamente significativo e pode representar grande poder para quem a possui, a proteção da informação e do conhecimento é de vital importância para a sobrevivência das organizações.

Os sistemas de informação são a chave para o acesso a vastas quantidades de dados corporativos, tornando-se um alvo atraente para invasores (*hackers*), repórteres e espiões. As organizações dependem da exatidão da informação fornecida pelos seus sistemas. Se essa confiança for destruída, o impacto para a entidade pode ser comparável à própria destruição do sistema. Dessa forma, é importante proteger os dados tanto de corrupções acidentais quanto propositais. Os sistemas de informação são caros tanto no desenvolvimento quanto para manutenção, e a administração deve proteger esse investimento como qualquer outro recurso valioso.

Sistemas que ofereçam serviços adequados e no tempo certo são a chave para a sobrevivência da maioria das organizações atuais. Sem seus computadores e sistemas de comunicação, as empresas ficariam incapazes de fornecer serviços, processar faturas, contatar fornecedores e clientes ou efetuar pagamentos. Os sistemas de informação também armazenam dados sigilosos, os quais se tornados públicos causariam embaraço e em alguns casos o fracasso da organização.

Os bens de tecnologia da informação (TI) são particularmente atrativos para invasores e ladrões, por serem portáteis, apresentarem uma relação valor/peso bastante elevada e poderem ser facilmente vendidos.

Segundo Beal (2005), devido à amplitude com que dados, informação e conhecimento agregam valor a processos, produtos e serviços, os mesmos constituem recursos cada vez mais críticos para o alcance dos objetivos organizacionais. A informação é como qualquer outro ativo das organizações e quando a mesma é sigilosa, torna-se necessária a proteção contra ameaças. (conforme afirma a norma NBR 27002). As principais garantias de um sistema seguro são:

- Confidencialidade - Garantir que somente pessoas autorizadas tenham acesso àquela informação.

- Integridade - Mesmo que com conteúdo duvidoso, garantir que a informação chegue ao seu destino sem algum tipo de modificação.
- Disponibilidade - Informações solicitadas devem estar disponíveis para acesso a qualquer momento em que o usuário permitido desejar.

A ISO/IEC 27002 (2005) afirma que os sistemas de informação das organizações estão expostos a diversos tipos de ameaças à segurança, incluindo sabotagem, vandalismo, danos causados por código malicioso, *hackers* e etc. Muitas organizações não dão a devida importância à questão da segurança da informação e na maioria das vezes o preço pago é muito alto.

Em uma auditoria de 2012 feita nas Organizações Públicas Federais sobre a governança de tecnologia da informação (TI), foi constatado pelo Tribunal de Contas da União que na maioria dos órgãos públicos não constava a segurança da informação em suas ementas. A auditoria apontou que apenas 37% deles constava com uma gestão de segurança da informação, além disso 90% não fazem análise dos riscos aos quais a informação crítica para o negócio está submetida, considerando os objetivos de disponibilidade, integridade, confidencialidade e autenticidade. E apenas 6% possuem plano de continuidade de negócio (aprovado e publicado).

Perante esses dados é admissível dizer que a gestão de risco de segurança da informação (GSRI) dos órgãos federais públicos não é uma prática comum. Esta situação pode ser explicada por diversos fatores, primeiro que a aplicação da gestão de risco é uma modalidade nova, as organizações públicas realizam as mudanças de ferramentas de gestão de um modo mais lento do que as organizações privadas. Depois vem a vontade e apoio da direção dos órgãos de implantar a GRSI.

Neste contexto, enfocamos a GRSI como um fator de vital importância dentro de uma organização. O sucesso de sua implantação e funcionamento está diretamente ligado ao sucesso na preservação dos valores agregados na informação.

A proposta deste projeto visa a necessidade de uma estratégia de análise de riscos apropriado para identificar os riscos com potencialidade alta de impacto e que ainda assim seja de baixo custo.

Segundo a norma ISO/IEC 27005, risco de segurança da informação é calculado em função da combinação da possibilidade de um incidente e de sua consequência. Isto posto, riscos podem ser administrados mudando-se a possibilidade de que determinado incidente ocorra, como também a natureza de suas consequências.

Este trabalho apresentou um processo de *Gestão de Riscos de Segurança da Informação*, tendo como base principal a norma ISO/IEC 27005 e considerando as características do campus da UFC em Quixadá. Tal análise é realizada com um enfoque de alto nível que visa os riscos cruciais que envolvem o negócio. Após a análise é possível definir as prioridades, detalhamentos dos riscos e uma cronologia de ações a serem executadas, necessário para a continuidade do negócio.

2 OBJETIVOS

2.1 Objetivo geral

- Proceder um estudo preliminar de avaliação de riscos para a UFC campus de Quixadá.

2.2 Objetivos específicos

- Proceder à revisão bibliográfica sobre o processo de gestão de riscos;
- Desenvolver materiais para um estudo de avaliação com enfoque de alto nível;
- Aplicar os materiais propostos em estudo de caso.

3 REVISÃO BIBLIOGRÁFICA

3.1 Segurança da Informação

A informação sempre foi de grande relevância para a tomada de decisão e, portanto, para qualquer ato de gestão. Atualmente, o volume de informação disponível conheceu um crescimento exponencial. Não existe falta de informação, mas sim excesso de dados. Uma consequência desta realidade é a exigência de organizar essa mesma quantidade de dados. E é para isso que existem os sistemas de informação.

De acordo com FILHO (2008), “informação” compreende qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento. Nesse sentido, a informação digital é um dos principais, senão o mais importante, produto da era atual. A informação pode ser manipulada e visualizada de diversas maneiras. Assim, à medida que a informação digital circula pelos mais variados ambientes, percorrendo diversos fluxos de trabalho, ela pode ser armazenada para os mais variados fins, possibilitando-a ser lida, modificada ou até mesmo apagada.

Segundo a ISO/IEC 27002 (2005), a informação é um importante ativo como qualquer outro nas organizações, sendo essencial para os negócios. Dessa forma, é necessário se possuir uma proteção adequada para a mesma. A informação pode existir em diversas formas, entretanto em qualquer que seja a forma de apresentação ou o meio através do qual é compartilhada ou armazenada, é de suma importância que ela esteja sempre segura.

Considerar informação como um ativo não explica o sentido da palavra informação, apenas exalta um de seus atributos. Ainda falta uma definição para o termo informação. A palavra informação é derivativa da palavra informar, a qual vem do latim “*informare”*, (FERREIRA, 1996) que significa dar forma, criar, apresentar, colocar em ordem. Observasse que ao buscar o conceito de informação em sua origem latina, o dicionário da língua portuguesa estabelece a funcionalidade do termo.

Oliveira (2001) afirma que a informação é um recurso vital para a empresa e integra, quando devidamente estruturada, os diversos subsistemas e, portanto, as funções das várias unidades organizacionais da empresa. No dicionário online *priberam,* informação consiste no ato ou efeito de informar, e também em forma de notícia, seja ela dada ou recebida.

Segundo WEBSTER (1995/1999), todos os observadores têm conhecimento de um crescimento maciço do fluxo de informação que está ultrapassando fronteiras, das facilidades de telecomunicações, das comunicações entre computadores de todos os níveis, de trocas entre mercados de ações e segmentos corporativistas, do acesso às bases de informação internacional e das mensagens de telex.

KUMAR (1997, p. 21) acredita que “a informação designa hoje a sociedade pós-industrial. É o que a gera e sustenta”. Para o autor, a sociedade pós-industrial poderia ser

caracterizada por uma sociedade de serviços, que oferece oportunidades de emprego para profissionais liberais e de nível técnico. Existe um considerável crescimento da distribuição global da informação de massa sendo veiculada. As organizações precisam saber usar a informação e tirar o melhor proveito dela para se colocarem em posição competitiva, acompanhando os novos tempos, mudando suas características gerenciais e estratégicas e com elas todo o seu capital intelectual.

A informação deve ser tratada como qualquer outro produto que esteja disponível para consumo. Ela deve ser desejada, para ser necessária. Para ser necessária, deve ser útil. E como tudo que é útil, precisa ser protegida.

O termo segurança apresenta diversidades em seu significado, sendo objeto dos mais variados estudos. Em Dicionário da Língua Portuguesa, a palavra segurança é definida com os seguintes significados:

> 1) Ato ou efeito de segurar; 2) Estado, qualidade ou condição de seguro; 3) Condição daquele ou daquilo em que se pode confiar; 4) Certeza, firmeza, convicção; 5) Confiança em si mesmo, autoconfiança; 6) Caução, garantia, seguro; 7) Protesto, afirmação; 8) Prenhes das fêmeas dos quadrúpedes; 9) Pessoa encarregada da segurança pessoal de alguém ou de empresa, guarda-costas. (FERREIRA, 1996, p. 1563)

Entende-se que a informação é todo o dado que possui valor para a pessoa ou organização, sendo assim ela é um bem e deve ser protegida, portanto, subentende-se que a informação é um importante patrimônio, sendo o ponto crucial para sobrevivência das organizações.

A ABNT 27002 define informação como sendo um ativo e ao mesmo tempo conceitua ativo como “qualquer coisa que tenha valor para a organização” (ABNT, 2007). Por consequência, informação pode ser entendida como qualquer coisa que tenha valor para a organização. Este conceito, associado ao que foi desenvolvido por Siqueira, a partir da teoria de Shannon, leva ao entendimento da informação como estrutura de um sistema. Vale lembrar que Fernandes (2008) considera que sistema pode ser definido como:

> Um conjunto de partes inter-relacionadas formando um todo, que exibe várias propriedades estruturais e processuais (comportamentais) que persistem ao longo de um tempo. O ambiente de um sistema é tudo com o qual o sistema interage, e também pode ser chamado de seu universo. (FERNANDES, 2008).

De acordo com Promon (2005, p.6),

> Engana-se quem pensa que as ameaças à segurança da informação estão relacionadas apenas com os sistemas e redes corporativas, conforme comentado até agora, numa área tipicamente denotada por segurança lógica ou digital. O conceito de segurança da informação vai muito além; pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associados aos diversos ativos da informação de uma corporação, independentemente de sua forma ou meio em que são compartilhados ou armazenados, digital ou impresso. O objetivo da segurança é garantir a confidencialidade, a integridade e a disponibilidade desses ativos de informação de uma corporação.

Ainda segundo Promon (2005, p.6),

> As fronteiras da segurança da informação vão muito além da segurança lógica. Permeiam também a segurança física, que tem por objetivo prevenir acesso não autorizado, dano e interferência às informações, equipamentos e instalações físicas da organização. O campo da segurança física inclui a utilização de dispositivos que interagem com o mundo físico, em contraste e complementação aos dispositivos lógicos. Alguns exemplos desses dispositivos incluem câmeras de vídeo, catracas, sensores de presença, leitores de cartão de identificação.

Para segurança da informação são válidos os conceitos de informação sob enfoque pragmático, semântico e sintático. Pode-se afirmar que a segurança da informação tem alcance holístico quanto ao conceito de seu objeto de estudo. Em síntese, para a segurança da informação, o entendimento sobre informação pode receber contribuições das ciências exatas, das ciências sociais e das ciências humanas.

Sêmola (2003) define segurança da informação como sendo "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

Beal (2005) entende como segurança da informação o "processo de proteger informações das ameaças para a sua integridade, disponibilidade e confidencialidade". Porém, segurança da informação não pode ser encarada como "guardar em um cofre todas as informações disponíveis", mas sim elaborar uma boa política de proteção evitando riscos e vulnerabilidade.

Filho (2008) afirma que a segurança da informação compreende um conjunto de medidas que visam a proteger e preservar informações e os sistemas de informações, assegurando-lhes integridade, disponibilidade, não repúdio, autenticidade e confidencialidade. Esses elementos constituem os cinco pilares da segurança da informação e, portanto, são essenciais para assegurar a integridade e confiabilidade em sistemas de informações. Tais pilares, juntamente com mecanismos de proteção, objetivam prover suporte à restauração de sistemas informações, adicionando-lhes capacidades de detecção, reação e proteção.

O autor ainda afirma que os componentes criptográficos da segurança da informação tratam da confidencialidade, integridade, não repúdio e autenticidade. Ressaltou que o uso desses pilares é feito em conformidade com as necessidades específicas de cada organização. Assim, o uso desses pilares pode ser determinado pela suscetibilidade das informações ou sistemas de informações, pelo nível de ameaças ou por quaisquer outras decisões de gestão de riscos. É importante se perceber que esses pilares são essenciais no mundo atual, onde se tem ambientes de natureza pública e privada conectados a nível global. Dessa forma, torna-se necessário dispor de uma estratégia, levando em conta os pilares acima mencionados, a fim de compor uma arquitetura de segurança que venha consolidar os objetivos dos cinco pilares. Neste contexto, as organizações e, mais amplamente, os países incluem em suas metas:

- Forte uso de criptografia;
- Incentivo à educação em questões de segurança;
- Disponibilidade de tecnologia da informação com suporte à segurança;
- Infraestrutura de gestão de segurança;
- Disponibilidade de mecanismos de monitoramento de ataques, capacidade de alerta e ações coordenadas.

Segurança possui sentido mais amplo do que defesa. O caráter da segurança é abrangente, enquanto o da defesa é específico. A defesa contém em si mesma a sua finalidade, enquanto a segurança é disperso e necessita de um foco para se tornar eficiente. A norma ISO/IEC 27002 define a segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio.

A concepção de segurança adotada pela ISO/IEC 27002, pode ser entendida como um ato de proteção para defender a informação que está em um ambiente de perigo, risco ou incerteza. Para obter segurança é necessária a implementação de controles. Os controles devem ser selecionados e implementados para assegurar que os riscos sejam reduzidos a um nível aceitável pela organização. Nesse ponto, há exigência de que seja realizada uma análise

de custo benefício, pois os custos para implementação de controles não podem superar o valor da informação que se pretender proteger com tal controle.

A ISO/IEC 27002 define controle da seguinte forma:

> Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica de gestão ou legal. Controle é também usado como um sinônimo para proteção ou contra medida.

Tal definição de controle leva ao entendimento de segurança como se fosse única alternativa para direcionar as ações de segurança da informação. Uma possível explicação para escolha desta concepção de segurança pode estar no seguinte texto:

> A informação e os processos de apoio, sistemas e redes são importantes ativos para os negócios. Definir, alcançar, manter e melhorar a segurança da informação podem ser atividades essenciais para assegurar a competitividade, o fluxo de caixa, a lucratividade, o atendimento aos requisitos legais e a imagem da organização junto ao mercado.
> As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por códigos maliciosos, "*hackers"* e ataques de "*denial of service"* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. (ABNT, 2007, p. ix).

A partir das informações apresentadas, pode-se entender que a segurança da informação possui seus princípios básicos, assim sendo a confidencialidade, integridade e disponibilidade das informações. De acordo com todos os aspectos citados, os benefícios que serão visados no trabalho consistem em reduzir os riscos de ataques que possam comprometer os princípios básicos, como por exemplo: dano físico, eventos naturais, falhas técnicas, ações não autorizadas, comprometimento de funções, fraudes, erros, sabotagens, roubo de informações e diversos outros problemas.

Por fim, pode-se afirmar que segurança é um instrumento de suma importância para proteção das pessoas e organizações contra ameaças às informações que a elas pertençam ou que estejam sob sua incumbência.

3.2 Normas e Padrões de Segurança

A ISO/IEC 27002 é um código de práticas para a gestão de segurança da informação. Esta norma pode ser vista como um prelúdio para o desenvolvimento de diretrizes e princípios gerais sobre metas geralmente aceitas para a gestão da segurança da informação.

A gestão da segurança da informação necessita de um planejamento adequado ao negócio da organização. Deve ser elaborado um plano estratégico de segurança que atenda a toda a organização. O plano deve identificar o cenário da organização aonde a segurança da informação deverá atuar.

Segundo Fontes (2000) não existe solução certa ou errada. Existe solução mais adequada a cada organização. Independentemente de como você rotule o seu planejamento de segurança, não deixe de fazê-lo. Como qualquer outro planejamento, ele é o rumo a ser seguido com os objetivos definidos.

A gestão da segurança deve abranger todos os aspectos do trabalho diário: a avaliação do ambiente organizacional, a valoração do risco e a análise de incidentes de segurança. Todos os processos de gestão da segurança se baseiem no plano estratégico da organização. O plano apresenta os princípios e diretrizes que norteiam a organização no cumprimento de sua missão.

É importante destacar a definição de controle e os seus componentes, conforme descrito na ISO/IEC 27002: a definição de controle compreende a forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

De acordo com a norma ISO/IEC 27002:20008, existem 11(onze) seções de controle de segurança da informação, os quais são dispostos abaixo com seus respectivos objetivos:

- Política de segurança da informação: Prover uma orientação e apoio a direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

- Organização da segurança da informação: Gerenciar a segurança da informação dentro da organização.
- Gestão de ativos: Alcançar e manter a proteção adequada dos ativos da organização.
- Segurança em recursos humanos: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de furto ou roubo, fraude ou mal uso de recursos.
- Segurança física e do ambiente: Prevenir o acesso físico não autorizado, danos e interferência com as instalações e informações da organização.
- Gerenciamento das operações e comunicações: Garantir a operação segura e correta dos recursos de processamento da informação.
- Controle de acesso: Controlar o acesso à informação com base nos requisitos de negócio e segurança da informação.
- Aquisição, desenvolvimento e manutenção de sistemas de informação: Garantir que segurança é parte integrante de sistemas de informação.
- Gestão de incidentes de segurança da informação: Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.
- Gestão de continuidade de negócio: Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se forem o caso.
- Conformidade: Evitar violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação.

Embora o conteúdo da política de segurança possa variar de acordo com o tipo da instituição, ela deverá abranger, sempre que cabível, os controles relacionados acima. Segundo a ISO/IEC 27002, a ordem dos controles não significa o seu grau de importância. Dependendo das circunstâncias, todas as seções podem ser importantes. Portanto, convém que

cada organização que utilize esta norma identifique quais são os itens aplicáveis, quão importantes eles são e a sua aplicação para os processos específicos do negócio.

3.3 Gestão de Riscos de Segurança da Informação

O risco é entendido como alguma coisa que cria possibilidades ou produz danos. No que se refere à segurança, os riscos são entendidos como circunstâncias que geram ou agregam a potencialidade de perdas e danos. É possível calculá-lo por meio da probabilidade de um evento acontecer e causar perdas.

Várias definições são encontradas para definir o risco, no entanto, a definição adotada neste trabalho é o que foi estabelecido pela norma *ISO/IEC Guide 73:2002*, que o define como "a combinação da probabilidade de um evento e suas consequências. "

Também é importante evidenciar a definição de risco de segurança da informação e seus componentes, segundo a ISO/IEC 27005,

> Riscos de segurança da informação é a possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira prejudicando a organização. É medido em função da combinação da probabilidade de um evento e de sua consequência.

Existem 4 (quatro) elementos que são primordiais para o processo de gestão de riscos, a partir do conceito citado é possível compreendê-los. De acordo com a ISO/IEC 27002:

• **Ativo** - qualquer coisa que tenha valor para a organização;

• **Ameaça** – Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

• **Vulnerabilidade** – Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

• **Consequência** – Está relacionada a perdas operacionais relativas à proteção de ativos.

A norma ISO/IEC 27005 convém que a gestão de riscos de segurança da informação possa contribuir para:

> • Identificação de riscos;
> •Análise/avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
> • Comunicação e entendimento da probabilidade e das consequências destes riscos;
> • Estabelecimento da ordem prioritária para tratamento do risco;
> • Priorização das ações para reduzir a ocorrência dos riscos;
> • Envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e mantidas informadas sobre a situação da gestão de riscos;
> • Eficácia do monitoramento do tratamento do risco;
> • Monitoramento e a análise crítica regular de riscos e do processo de gestão dos mesmos;
> • Coleta de informações de forma a melhorar a abordagem da gestão de riscos;
> • Treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.

Riscos de segurança da informação são as possibilidades de uma ameaça explorar vulnerabilidades dos ativos, comprometendo a confidencialidade, integridade e disponibilidade das informações de uma organização (ABNT NBR ISO/IEC 27005, 2008). Já Oliveira (2006) classifica os riscos como sendo uma oportunidade, uma incerteza ou uma ameaça. Esta última como sendo de maior preocupação, pois está atrelada à ocorrência de efeitos negativos como, por exemplo, perda financeira, fraude, roubo, comprometimento da imagem, infração legal, indisponibilidade de serviços, dentre outros (VASILE; STUPARU; DANIASA, 2010).

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visam à identificação, avaliação e priorização de riscos, seguido pela aplicação coordenada e econômica dos recursos para minimizar, monitorar e controlar a probabilidade e o impacto de eventos negativos, reduzindo o risco a um nível aceitável.

Devido à importância do processo de gestão de riscos para as organizações, algumas normas internacionais foram criadas com o intuito de nortear os conceitos e práticas de gestão de riscos. Dentre estas normas, pode-se citar a ISO/IEC 27005, que discute - *Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação*. A utilização de normas de segurança da informação garante que a organização está seguindo as diretrizes dos processos de gestão da segurança da informação e possibilita com que a organização seja reconhecida pela utilização de boas práticas em gestão da segurança da informação.

A norma internacional ISO/IEC 27005 é parte da série de normas da ISO/IEC 27000, a qual é uma série bem estabelecida de normas de gestão de segurança da informação e é aceita em todo o mundo. O âmbito de aplicação destas normas pode ser na organização como um todo, ou em partes, como os processos de um departamento, uma aplicação de TI ou

uma infraestrutura de TI (BECKERS *et al*, 2011). Esta norma internacional fornece diretrizes para o processo de Gestão de Riscos de Segurança da Informação de uma organização, atendendo particularmente aos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI).

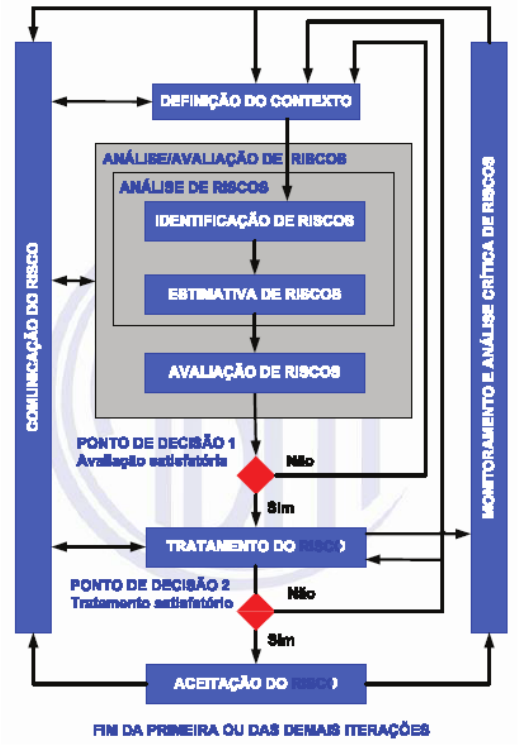
A ISO/IEC 27005 define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização (LUND; SOLHAUG; STØLEN, 2010).

Neste contexto, o processo de gestão de riscos é definido por oito atividades, como pode ser observado na Figura 1. Para cada atividade da norma são propostas diretrizes para implementação que serão brevemente descritas a seguir (ABNT NBR ISO/IEC 27005, 2008).

3.3.1 O processo de Gestão de Riscos

O procedimento e atividades da gestão de risco de segurança da informação (GRSI) está descrito na norma ISO/IEC 27005. As atividades do processo se inicia com a atividade de definição do contexto, seguidas de análise/avaliação de riscos, tratamento do risco, aceitação do risco, comunicação do risco, por final o monitoramento e análise crítica de riscos. Segue na Figura 1 a ligação entre as atividades do processo de GRSI.

Figura 1 – Processo de gestão de riscos de segurança da informação



Fonte: ABNT NBR ISO/IEC 27005

A seguir será descrita cada uma das atividades do processo.

3.3.1.1 Definição do contexto

A definição do contexto designa o alvo cujo a gestão de risco vai proceder. Como entrada a atividade recebe todas as informações relevantes sobre a organização para a definição do contexto da gestão de riscos de segurança da informação. E gera como saída:

- Especificação dos critérios básicos, critérios esses que se dividem em critérios para avaliação de riscos, critérios de impacto e critérios para aceitação do risco;
- O escopo e os limites do processo de GRSI;
- A organização responsável pelo processo.

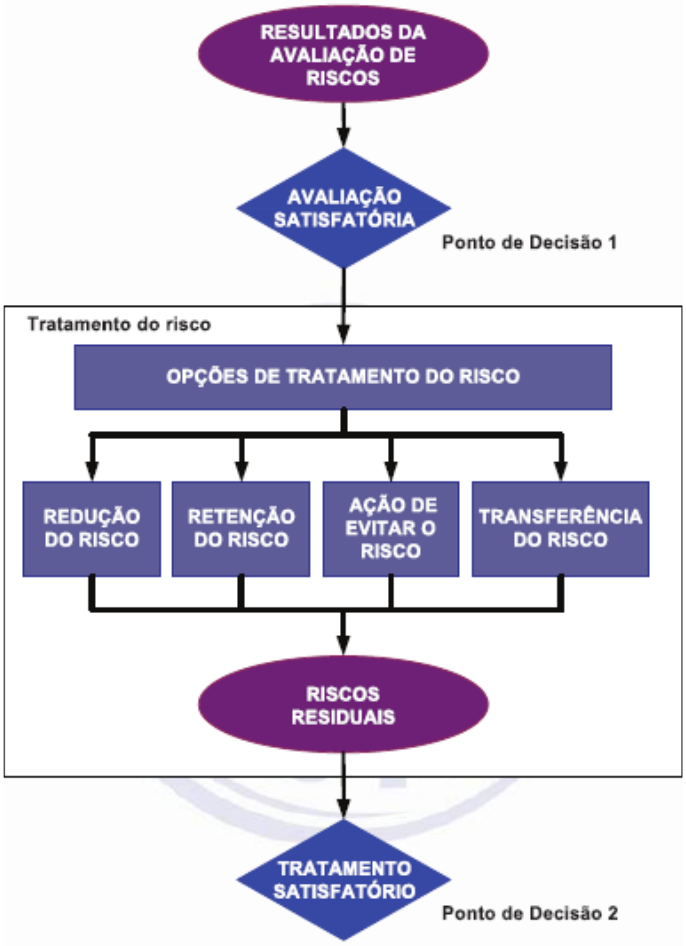
3.3.1.2 Análise/avaliação de riscos de segurança da informação

A análise/avaliação de riscos tem o papel de identificar, quantificar ou descrever qualitativamente os riscos, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização. Esta atividade recebe como entrada os critérios básicos, o escopo e os limites, e a organização do processo de GRSI que se está definindo. Como saída é gerada uma lista de riscos avaliados, ordenados por prioridade de acordo com os critérios de avaliação de riscos.

3.3.1.3 Tratamento do risco de segurança da informação

O tratamento do risco convém em controles para reduzir, reter, evitar ou transferir os riscos, os mesmo sejam selecionados e o plano de tratamento do risco seja definido. Como entrada a atividade recebe uma lista de riscos ordenados por prioridade (de acordo com os critérios de avaliação de riscos) e associados aos cenários de incidentes que os provocam. Na saída é gerado um plano de tratamento do risco e os riscos residuais, sujeitos à decisão de aceitação por parte dos gestores da organização. A Figura 2 mostra a atividade de tratamento do risco.

Figura 2 – A atividade de tratamento do risco



Fonte: ABNT NBR ISO/IEC 27005

3.3.1.4 A aceitação do risco de segurança da informação

Esta atividade convém que a decisão de aceitar os riscos seja realizada e formalmente registrada, juntamente com a responsabilidade pela decisão. Como entrada recebe o plano de tratamento do risco e a análise/avaliação do risco residual sujeito à decisão dos gestores da organização relativa à aceitação do mesmo. Como saída é gerado uma lista de riscos aceitos, incluindo uma justificativa para aqueles que não satisfaçam os critérios normais para aceitação do risco.

3.3.1.5 Comunicação do risco de segurança da informação

Esta atividade é onde as informações sobre os riscos são trocadas e/ou compartilhadas entre o tomador de decisão e as outras partes interessadas. Tem como entrada todas as informações sobre os riscos obtidas através das atividades de gestão de riscos (ver

Figura 1). E como saída o entendimento contínuo do procedimento de GRSI da organização e dos resultados obtidos.

3.3.1.6 Monitoramento e análise crítica de riscos de segurança da informação

A última atividade do processo de GRSI convém que todos os riscos e seus fatores (isto é, valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorados e analisados criticamente, a fim de se identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de se manter uma visão geral dos riscos.

Recebe como entrada todas as informações sobre os riscos obtidas através das atividades de gestão de riscos (ver Figura 1). E tem como saída um alinhamento contínuo da gestão de riscos com os objetivos de negócios da organização e com os critérios para a aceitação do risco. No final do processo de GRSI, o mesmo tem que ser continuamente monitorado, analisado criticamente e melhorado, quando necessário e apropriado.

4 PROCEDIMENTOS METODOLÓGICOS

Para a realização do presente trabalho, foi adotado como metodologia inicial uma pesquisa bibliográfica de gestão da segurança da informação, segurança da informação, norma de segurança da informação, gestão de riscos da segurança da informação.

A pesquisa bibliográfica inicial propiciou um aprofundamento sobre os conceitos registrados acerca do tema proposto, apresentando a importância da segurança da informação e da gestão de riscos da segurança da informação nas organizações. O estudo realizado teve como ênfase as normas ISO/IEC 27002– *Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação* e a ISO/ IEC 27005 - *Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação.*

Como fase subsequente, foi realizada uma pesquisa aplicada, buscando resultados que pudessem ser utilizados na solução de problemas que ocorrem na realidade.

A partir de todas as etapas de pesquisas completas o trabalho foi direcionado ao processo de gestão de riscos de segurança da informação ao campus da UFC em Quixadá. Foi utilizada uma metodologia com um enfoque de alto nível.

5 MÉTODO PARA A GESTÃO DE RISCO DE SEGURANÇA DA INFORMAÇÃO

A ISO/IEC 27005 possui regras para o procedimento de gestão de riscos de segurança da informação (GRSI) de uma organização, que foca principalmente nas características de um sistema de gestão de segurança da informação (SGSI) conforme a norma ISO/IEC 27002. Com isso seu processo de GRSI é alinhado com o processo de SGSI de acordo com as diretrizes da ISO 27002.

O material para a execução do procedimento foi criado com um enfoque de alto nível como proposto no projeto de pesquisa, o mesmo tem como objetivo verificar os requisitos de segurança da informação da organização para que aconteça a criação de um SGSI. A estimativa qualitativa dos riscos foi a mais propícia em termos de análise de baixo custo, fácil compreensão e maior velocidade em comparação a estimativa quantitativa.

No estudo sugerido, a organização é tratada de forma completa, onde a perspectiva tecnológica é vista como avulsa das questões de negócio, ou seja, tem como foco o negócio e o ambiente operacional e pouco sobre os componentes tecnológicos. No decorrer da análise os riscos serão classificados por categorias, e o objetivo do tratamento de riscos é de indicar controles organizacionais voltados as características de gerência. Logo, os riscos classificados como graves vão ter seus componentes detalhados em outras iterações do processo de avaliação de riscos.

O material foi desenvolvido para todas as etapas do processo de GRSI em conformidade com a norma ISO/IEC 27005, como mostrado a seguir:

- Definição do contexto: Definição de escopo, critério de riscos e de todas as informações relevantes (ativos, ameaças, vulnerabilidades e etc.);

- Análise/avaliação de riscos: Identificação dos riscos, estimativa de riscos e avaliação de riscos;

• Tratamento do risco: Utiliza a ação definida na avaliação dos riscos e é iniciado apenas se a avaliação for satisfatória;

As atividades restantes do processo de GRSI, aceitação do risco, comunicação do risco, e monitoramento e análise crítica dos riscos, continuaram com as mesmas orientações da ISO/IEC 27005.

5.1 Definição do contexto

Um dos cruciais fatores para o sucesso da gestão de risco de segurança da informação (GRSI) é a atividade de definição de contexto, onde abrange a definição de escopo e a definição dos critérios de riscos.

5.1.1 Definição do escopo

O processo de GRSI inclui algumas decisões em termos de compreensão. O escopo é um conjunto de ativos, ameaças e vulnerabilidades que serão cobertos pelo sistema de gestão de risco. Um fator crucial para uma organização que está implantando um processo de GRSI é o tamanho do escopo. Pequenos escopos podem não ser eficazes por não conter todos os ativos importantes da organização, já os escopos gigantescos podem gerar processos que nunca acabam.

A ISO 27005 traz consigo um documento como um dos meios para se definir o escopo da organização, conforme é mostrado abaixo:

> **I – Análise da organização**
> **Propósito principal da organização:** O seu propósito pode ser definido como a razão pela qual a organização existe (sua área de atividade, seu segmento de mercado etc.)
> **Negócio:** O negócio de uma organização, definido pelas técnicas e know-how de seus funcionários, viabiliza o cumprimento de sua missão. É específico à área de atividade da organização e frequentemente define sua cultura.
> **Missão:** A organização atinge seu propósito ao cumprir sua missão. Para bem identifica-la, convém que os serviços prestados e/ou produtos manufaturados sejam relacionados aos seus públicos-alvo.
> **Valores:** Valores consistem de princípios fundamentais ou de um código de conduta bem definido, aplicados na rotina de um negócio, Podem incluir os recursos humanos, as relações com agentes externos (clientes e outros), a qualidade dos produtos fornecidos ou dos serviços prestados.
> **Organograma:** A estrutura da organização é esquematizada em seu organograma. Convém que essa representação deixe claro quem se reporta a quem, destacando também a linha de comando que legitima a delegação de autoridade. Convém que inclua também outros tipos de relacionamentos, os quais, mesmo que não sejam baseados em uma

autoridade oficial, criam de qualquer forma caminhos para o fluxo de informação.
Estratégia: Ela requer a expressão formalizada dos princípios que norteiam a organização. A estratégia determina a direção e o desenvolvimento necessários para que a organização possa se beneficiar das questões em pauta e das principais mudança sendo planejadas.
II – Restrições que afetam a organização: Convém que todas as restrições que afetam a organização e determinam o direcionamento da segurança da informação sejam consideradas.
III – Legislações e regulamentações aplicáveis à organização: Convém que os requisitos regulatórios aplicáveis à organização sejam identificados. Eles consistem nas leis, decretos, regulamentações específicas que dizem respeito à área de atividade da organização ou regulamentos internos e externos. Englobam também contratos, acordos e, mais genericamente, qualquer obrigação de natureza legal ou regulatória.
IV – Restrições que afetam o escopo: Ao identificar as restrições é possível enumerar aquelas que causam um impacto no escopo e determinar quais são passíveis de intervenção. Elas complementam e talvez venham a corrigir as restrições da organização discutidas mais acima.
V – Identificação de ativos: Para estabelecer o valor de seus ativos, uma organização precisa primeiro identifica-los (num nível de detalhamento adequado).

5.1.2 Critérios de risco

De acordo com a ISO 27005, dependendo do escopo e dos objetivos da gestão de riscos, diferentes métodos podem ser aplicados. Um método de GRSI apropriado, seja ele escolhido ou desenvolvido, tem que conter os critérios básicos de risco, tais como: critérios de avaliação de riscos, critérios de impacto e critérios de aceitação do risco.

5.1.2.1 Critérios de avaliação de riscos

A ISO 27005 convém que os critérios de avaliação de risco sejam desenvolvidos para avaliar os riscos de segurança da informação na organização, considerando alguns dos itens a seguir: Valor estratégico do processo que trata as informações de negócio; criticidade dos ativos de informação envolvidos; importância do ponto de vista operacional e dos negócios, da disponibilidade, confidencialidades e da integridade, etc. A Tabela 1 mostra uma forma de avaliar e priorizar os riscos. O primeiro elemento da Tabela é o cenário, onde será descrito a ameaça. Após tem o nível de risco (NR) que será de grande importância para a avaliação e priorização dos riscos. O restante dos itens são adaptados de acordo com as necessidades da organização e também ajudam na definição da ordem de prioridade.

Cenário	
NR	
Influencia no custo operacional?	
Atinge algum ativo crítico?	
Atinge algum processo crucial?	

Tabela 1 – Critérios de avaliação de riscos

5.1.2.2 Critérios de impacto

Os critérios de impacto são desenvolvidos e especificados em função do conjunto de danos ou custos à organização causados por um evento relacionado com a segurança da informação. Responsável por determinar o impacto das consequências de um incidente, levando em conta o valor de reposição do ativo e a consequência para o negócio público relacionada à perda do ativo.

A Tabela 2 mostra uma forma de avaliar o impacto do risco nas organizações.

Critério	Valor de reposição do ativo	Consequência para o negócio público relacionada à perda do ativo.
Alta		
Média		
Baixa		

Tabela 2 – Critérios de impacto

5.1.2.3 Critérios de aceitação do risco

Segundo a ISO 27005, convém que os critérios para a aceitação do risco sejam desenvolvidos e especificados e dependam frequentemente das políticas, meta e objetivos da organização, assim como dos interesses das partes interessadas. Após a aceitação do risco, se algum incidente ocorrer com relação ao mesmo, a culpa é do gerente de TI.

Na Tabela 3 o NR variará de 1 a 25, classificando os riscos em baixo, médio e alto. Essas categorias podem ser ajustadas de acordo com as necessidades da organização. Os critérios restantes são a descrição do risco, o porquê da aceitação e as observações.

Nível de risco	Descrição	Aceitabilidade	Observações
Alto (15-25)			
Médio (4 – 12)			
Baixo (1 – 4)			

Tabela 3 – Critérios de aceitação de risco

5.2 Análise/avaliação de riscos

5.2.1 Análise de riscos

Os critérios para a avaliação dos riscos são desenvolvidos nessa fase. Segundo a ISO 27005, a análise de riscos convém que os ciscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização. Cabe à organização selecionar seu próprio método para a análise/avaliação de riscos baseado nos objetivos e na meta da análise/avaliação de riscos.

No processo de análise de risco, os ativos, ameaças, vulnerabilidades e riscos serão analisados por uma perspectiva mais complexa. O estudo é qualitativo, para definir o nível de risco (NR) é necessário a multiplicação do nível de probabilidade (NP) daquele risco vir a acontecer pelo nível de impacto (NI) do mesmo. Ambos os valores serão estimados na atividade de estimativa de riscos. Cada ativo identificado será relacionado as ameaças, vulnerabilidades e impacto, cujos dados podem ser armazenados em tabelas, como mostrado na Tabela 4.

ANÁLISE DE RISCOS		
Identificação de riscos	Ativo	
	Ameaça	
	Vulnerabilidade	
	Impacto	
Estimativa de riscos	Nível de Probabilidade	
	Nível de Impacto	
	Nível de Risco	

Tabela 4 – Análise de Riscos

5.2.2 Identificação de riscos

Como o próprio nome já diz, é nesta fase que os ativos dentro do escopo estabelecido são identificados e relacionados com as ameaças, vulnerabilidades e consequências, ou seja, é a fase da identificação dos riscos, uma vez que os riscos são identificados é possível medir seu nível de risco.

5.2.2.1 Identificação dos ativos

Segundo a norma da ISO 27005, na identificação dos ativos convém que os ativos dentro do escopo estabelecido sejam identificados. A mesma sugere a seguinte classificação de ativos:

• Ativos primários: informações e processos de negócio;

• Ativos de suporte e infraestrutura: *hardware*, *software*, rede, recursos humanos, instalações físicas e estrutura da organização.

5.2.2.2 Identificação das ameaças

A norma ISO/IEC 27002 define ameaças como a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização. De maneira geral, as ameaças são tidas como agentes ou condições que exploram as vulnerabilidades e provocam danos. As ameaças são identificadas de maneira imprecisa, por categoria por exemplo: origem natural ou humana, causa acidental ou ocasional, dano físico ou comprometimento da informação. A ameaça pode causar diversos tipos de danos na segurança relacionado à perda de disponibilidade, confidencialidade ou integridade dos ativos de informação.

5.2.2.3 Identificação das vulnerabilidades

As vulnerabilidades são fragilidades que podem provocar danos ao serem exploradas pelas ameaças. E o papel desta atividade é identificar essas vulnerabilidades. As vulnerabilidades podem ser procurada nas seguintes áreas: organização; processos e procedimentos; rotinas de gestão; recursos humanos; ambiente físico; configuração do sistema de informação; hardware, software ou equipamentos de comunicação; dependência de entidades externas.

5.2.2.4 Identificação das consequências

De acordo com a ISO 27005, a identificação das consequências convém que as consequências que a perda de confidencialidade, de integridade e de disponibilidade podem ter sobre os ativos sejam identificadas. A mesma propõe que as organizações identifiquem as consequências operacionais de cenários de incidentes em função de (mas não limitado a):

- Investigação e tempo de reparo;
- Tempo (de trabalho) perdido;
- Oportunidade perdida;
- Saúde e Segurança;
- Custo financeiro das competências específicas necessárias para reparar o prejuízo;
- Imagem, reputação e valor de mercado.

5.2.3 Estimativa de riscos

Um estudo para a estimativa pode ser qualitativo ou quantitativo ou então uma combinação de ambos, dependendo das necessidades. Na prática, a estimativa qualitativa é utilizada em primeiro lugar frequentemente para conseguir uma indicação geral do nível de risco e para demonstrar os grandes riscos. Isso ocorre porque realizar análises qualitativas é menos complexo do que análises quantitativas. Esta atividade compreende 3 atividades: avaliação das consequências, avaliação da probabilidade dos incidentes e estimativas dos níveis de risco.

5.2.3.1 Avaliação das consequências

Para avaliar as consequências e adquirir seu nível de impacto (NI) é levado em conta o valor de reposição do ativo e a consequência do negócio público relacionada à perda do ativo. Como mostrado na Tabela 5.

Valor de reposição do ativo	Consequência para o negócio público relacionada à perda do ativo	Nível de impacto
Baixa	Baixa	1
	Média	2
	Alta	3
Média	Baixa	2
	Média	3
	Alta	4
Alta	Baixa	3
	Média	4
	Alta	5

Tabela 5 – Definição do nível de impacto.

5.2.3.2 Avaliação da probabilidade de incidentes

Para avaliar a ocorrência de um cenário de incidente é levado em conta a probabilidade da ameaça e a facilidade de exploração da vulnerabilidade. Como mostrado na Tabela 6.

Critério	Probabilidade da ameaça	Facilidade de exploração da vulnerabilidade
Baixo		
Médio		
Alto		

Tabela 6 – Avaliação da probabilidade dos incidentes.

Em seguida com o resultado dessa combinação é possível definir o nível de probabilidade (NP) do cenário de incidente:

Probabilidade da ameaça	Facilidade de exploração da vulnerabilidade	NP
Baixo	Baixo	1
	Médio	2
	Alto	3
Médio	Baixo	2
	Médio	3
	Alto	4
Alto	Baixo	3
	Médio	4
	Alto	5

Tabela 7 – Definição do nível de probabilidade do cenário de incidente

5.2.3.3 Estimativa do nível de risco

O nível de risco é calculado com a multiplicação do nível de impacto pelo nível de probabilidade. De 1 a 4 é nível baixo, de 4 a 14 é nível médio e de 15 a 25 é nível alto.

5.2.4 Avaliação de riscos

O principal papel desta atividade é a tomada de decisão sobre as ações futuras, por meio da determinação de prioridades para o tratamento do risco. Isso só acontece depois de comparar os riscos com os critérios de avaliação de riscos e com os critérios de aceitação de risco, no qual foi definido no início do processo. A atividade de avaliação de risco gerará uma lista de riscos ordenados por prioridade de tratamento.

6 ESTUDO DE CASO

Com o objetivo de validar o método proposto, foi executado um estudo de caso no campus da *Universidade Federal do Ceará* (UFC) em Quixadá. A UFC Quixadá possui cerca de mil universitários, divididos em 4 cursos da área da *Tecnologia da Informação*, com 40 professores, 4 coordenadores e 2 diretores. Sua estrutura conta com 2 blocos e 1 centro de convivência; cerca de 20 salas de aulas; 5 laboratórios de informática com cerca de 30 computadores em cada laboratório e 1 auditório.

Por conta de limitações relacionadas ao acesso às informações gerenciais de TI, o presente estudo foi realizado envolvendo três serviços públicos e de amplo conhecimento de professores e alunos do campus da UFC em Quixadá.

Participaram das etapas desta pesquisa dois professores e cerca de 30 alunos do campus da UFC em Quixadá, cujos nomes não serão divulgados por questão de confidencialidade.

Passo 1. Definição do contexto

1.1 Definição do escopo

a. Identificação da organização

Negócio público: Universidade

Missão: A missão da Universidade é formar profissionais da mais alta qualificação, gerar e difundir conhecimentos, preservar e divulgar os valores éticos, científicos, artísticos e culturais, constituindo-se em instituição estratégica para o desenvolvimento do Ceará, do Nordeste e do Brasil.

Estratégia:

Consolidar-se como instituição de referência no ensino de graduação e pós-graduação (*stricto e lato sensu*), de preservação, geração e produção de ciência e tecnologia, e de integração com o meio, como forma de contribuir para a superação das desigualdades sociais e econômicas, por meio da promoção do desenvolvimento sustentável do Ceará, do Nordeste e do Brasil.

Localidade:

A UFC está localizada no Bairro Cedro da cidade de Quixadá, interior do Ceará.

b. Limites do escopo:

A gestão de riscos nesta pesquisa foi limitada a alguns dos ativos de informação específicos de acesso dos alunos, professores e coordenação.

c. Ativos de informação:

Cada ativo de informação possui 1 processo fundamental: Gerenciamento de presenças e plano de aula, avaliação institucional e gerenciamento das atividades complementares. Os ativos citados a seguir dão suporte a estas atividades:

• Sistema Integrado de Gestão de Atividades Acadêmicas (SIGAA): Sistema completo de muitas funcionalidades, responsável por matrículas, plano de aula, documentos para aula, gerenciamento das presenças e notas dos alunos.

• Sistema de Presenças e Planos de Aula (SIPPA): É um sistema responsável pelo armazenamento das presenças dos alunos em sala de aula, disponibilização de plano de aula e documentos para aula, gerenciamento das notas dos alunos.

• Sistema de Avaliação Institucional (SAVI): Sistema utilizado pelos alunos para avaliação dos professores.

• Sistema de Atividades Complementares (SISAC): Sistema responsável pelo gerenciamento das atividades complementares dos alunos.

1.2. Critérios Básicos

a. Critério para avaliação de risco:

• A Tabela 14 será utilizada como referencial para ordenar a prioridade dos riscos.

• Os riscos graves serão os incidentes que envolverem a perda de autenticidade, confidencialidade, integridade e disponibilidade das informações.

• Riscos que causem dano a imagem da Universidade ou do governo são considerados graves.

• Serão analisados primeiros os cenários de incidentes que tiveram seu NR mais elevado.

b. Critério de impacto

Critério	Valor de reposição do ativo	Consequência para o negócio público relacionada à perda do ativo.
Alta	Ativos de grande valor e de difícil recuperação (dados)	Paralização de processos cruciais da Universidade.
Média	Ativos de valor médio (Computador)	Perda de eficiência em alguns processos
Baixa	Ativos de valor baixo (cabo de fonte)	Mínimo de dano no negócio

Tabela 8 – Critério de impacto

c. Critério para aceitação de risco

Nível de risco	Descrição	Aceitabilidade	Observações
Alto (15-25)	Paralização do serviços no campus por completo. Dano grave a imagem da universidade.	Inaceitável, requer ação imediata para correção do risco.	
Médio (4 – 12)	Alguns processos afetados.	Não pode ser aceito, requer correção para resolver o risco.	
Baixo (1 – 4)	Efeitos menores	Risco aceitável.	

Tabela 9 – Critério para aceitação de risco

Passo 2. Análise/avaliação de riscos

2.1 Tabela de referência

Valor de reposição do ativo	Consequência para o negócio público relacionada à perda do ativo	Nível de impacto
Baixa	Baixa	1
	Média	2
	Alta	3
Média	Baixa	2
	Média	3
	Alta	4
Alta	Baixa	3
	Média	4
	Alta	5

Tabela 10 – Determinação do nível de impacto

Critério	Probabilidade da ameaça	Facilidade de exploração da vulnerabilidade
Baixo	Ameaças rara com ocorrência de 1 vez a cada década	Vulnerabilidades de difícil exploração
Médio	Ameaças com uma frequência variável de 1 ocorrência por semestre.	Vulnerabilidades recém-descobertas
Alto	Ameaças simples que acontecem rotineiramente	Vulnerabilidades facilmente exploradas

Tabela 11 – Avaliação da Probabilidade dos incidentes

Probabilidade da ameaça	Facilidade de exploração da vulnerabilidade	NP
Baixo	Baixo	1
	Médio	2
	Alto	3
Médio	Baixo	2
	Médio	3
	Alto	4
Alto	Baixo	3
	Médio	4
	Alto	5

Tabela 12 – Definição do nível de probabilidade do cenário de incidente

Nível de Risco

O nível de risco é calculado com a multiplicação do nível de impacto pelo nível de probabilidade. Nível baixo(1-4), Nível médio (4-14) e de Nível alto (15-25).

2.2 Análise de risco

ANÁLISE DE RISCOS							
Identificação de riscos					**Estimativa de riscos**		
Número	**Sistema**	**Ameaça**	**Vulnerabilidade**	**Impacto**	**NP**	**NI**	**NR**
1	SIPPA	Comprometimento da disponibilização	Falha nos servidores	Perda da disponibilidade dos dados	4	4	16
2	SIPPA	Falta de conexão no campus	Certificado não confiável	Perda de Disponibilidade e Autenticidade.	4	4	16
3	SIPPA	Erro durante o uso	Falha na visualização dos arquivos.	Perda de Disponibilidade e autenticidade.	2	4	8
4	SIPPA	O sistema não aceitar o upload de um arquivo de código.	O aluno enviar um arquivo sem estar zipado.	Perda de integridade e autenticidade.	2	5	10

5	SIPPA	Má programação ou Falha no Servidor	Perda de arquivos de alunos, causando perda de nota.	Perda de Disponibilidade, Perda de Integridade	4	4	16
6	SIPPA	Sistema permite usuários que já terminaram o curso logar no mesmo	O usuário não autorizado pode fazer reclamações sobre o restaurante universitário sem ao menos está usando o serviço	Perda de Confidencialidade	5	3	15
7	SIPPA	Falha na segurança	Não contém certificado de segurança reconhecido internacionalmente	Perda de Autenticidade, Confidencialidade, Integridade e Disponibilidade.	5	5	25
8	SAVI	Erro durante o uso	Interface de usuário complicada	Perda de eficiência	2	3	6
9	SAVI	Pode ser invadido	Falha na segurança	Perda de Confidencialidade	2	4	8
10	SAVI	Pode ser invadido e derrubado	Falha na segurança	Perda de confidencialidade e disponibilidade	2	5	10
11	SAVI	Disponibilidade do sistema	Interface não muito iterativa	Perda de integridade	4	4	16
12	SAVI	Falha na segurança	Não contém certificado de segurança reconhecido internacionalmente	Perda de Autenticidade, Confidencialidade, Integridade e Disponibilidade.	5	5	25
13	SIGAA	Sistema muitas vezes lento	Problema nos servidores	Perda de Disponibilidade	5	4	20
14	SIGAA	Sistema sair do ar no meio do processo de inscrição nas disciplinas	Perder as disciplinas selecionadas	Perda de Integridade e Disponibilidade	4	4	16
15	SIGAA	Feedback	Sistema complicado	Perda de Disponibilidade	5	3	15
16	SIGAA	Dificulta a utilização	Interface ruim	Mau uso do sistema	5	3	15
17	SIGAA	Sistema indisponível	Não utiliza *captcha*	Perda de Disponibilidade	4	4	16

18	SISAC	Sistemas Indisponível	Falha nos servidores	Perda de Disponibilidade	4	4	16
19	SISAC	Comprometimento no acesso	Não possui a opção de alterar senha	Perda de disponibilidade e tempo.	5	2	10
20	SISAC	Falha na segurança	Não contém certificado de segurança reconhecido internacionalmente	Perda de Autenticidade, Confidencialidade, Integridade e Disponibilidade.	5	5	25

Tabela 13 – Análise de riscos

Nº	**Cenário**	**NR**	**Perda de 4 ativos da informação**	**Perda de 3 ativos da informação**	**Perda de 2 ativos da informação**	**Perda de 1 ativo da informação**	**Priorização do Risco**
7	Falha de segurança no SIPPA devido à falta de um certificado de segurança reconhecido internacionalmente	25	X				1
12	Falha de segurança no SAVI devido à falta de um certificado de segurança reconhecido internacionalmente	25	X				2
20	Falha de segurança no SISAC devido à falta de um certificado de segurança reconhecido internacionalmente	25	X				3
13	Lentidão do SIGAA devido a problemas nos servidores.	20				X	10
1	Comprometimento na						

	disponibilização do SIPPA devido a falha nos servidores	16				X	11
2	Falta de conexão do SIPPA devido a certificado não confiável.	16			X		4
5	Perda de arquivos no SIPPA devido o mal desenvolvimento do sistema ou falha nos servidores.	16			X		5
11	Falta de integridade do SAVI devido a interface não muito iterativa	16				X	12
14	Perder as disciplinas selecionadas no SIGAA no processo de matricula online devido ao sistema ficar fora do ar.	16			X		6
17	SIGAA indisponível devido a não utilização de *captcha*.	16				X	13
18	SISAC indisponível devido a falha nos servidores	16				X	14
6	Acesso irregular de alunos concluintes do curso no SIPPA devido a falta de gerenciamento dos acessos.	15				X	15
15	Falta de *feedback* do SIGAA devido a interface ruim.	15				X	16

16	Má utilização do SIGAA devido a interface ruim	15				X	17
4	Falha na funcionalidade de envio de trabalhos no SIPPA devido a problemas no código.	10			X		7
10	Invasão e queda do SAVI devido a falha na segurança.	10			X		8
19	Comprometimento no acesso do SISAC por não ter a opção de "alterar senha"	10				X	18
3	Falha na visualização dos arquivos do SIPPA	8			X		9
9	Invasão do SAVI devido a falha na segurança.	8				X	19
8	Erro durante o uso do SAVI devido a interface complicada.	6				X	20

Tabela 14 – Critério para a avaliação de risco

Passo 3. Lista de riscos ordenados por prioridade

1	Falha de segurança no SIPPA devido à falta de um certificado de segurança reconhecido internacionalmente.
2	Falha de segurança no SAVI devido à falta de um certificado de segurança reconhecido internacionalmente
3	Falha de segurança no SISAC devido à falta de um certificado de segurança reconhecido internacionalmente
4	Falta de conexão do SIPPA devido a certificado não confiável.
5	Perda de arquivos no SIPPA devido o mal desenvolvimento do sistema ou falha nos

	servidores.
6	Perder as disciplinas selecionadas no SIGAA no processo de matricula online devido ao sistema ficar fora do ar.
7	Falha na funcionalidade de envio de trabalhos no SIPPA devido a problemas no código.
8	Invasão e queda do SAVI devido a falha na segurança.
9	Falha na visualização dos arquivos do SIPPA
10	Lentidão do SIGAA devido a problemas nos servidores.
11	Comprometimento na disponibilização do SIPPA devido a falha nos servidores
12	Falta de integridade do SAVI devido a interface não muito iterativa
13	SIGAA indisponível devido a não utilização de *captcha*.
14	SISAC indisponível devido a falha nos servidores
15	Acesso irregular de alunos concluintes do curso no SIPPA devido a falta de gerenciamento dos acessos.
16	Falta de *feedback* do SIGAA devido a interface ruim.
17	Má utilização do SIGAA devido a interface ruim
18	Comprometimento no acesso do SISAC por não ter a opção de “alterar senha”
19	Invasão do SAVI devido a falha na segurança.
20	Erro durante o uso do SAVI devido a interface complicada.

Tabela 15 – Riscos ordenados por prioridade

Após todo o processo, o resultado final obtido foi uma lista de riscos ordenados por prioridade de tratamento de acordo com a Tabela 15. Assim, os riscos encontrados por meio de uma análise/avaliação de riscos com enfoque de alto nível apontam para os principais problemas de segurança da informação dentro do limite do escopo definido no início.

7 CONSIDERAÇÕES FINAIS

O Campus da *Universidade Federal do Ceará* em Quixadá se dedica a formar profissionais da mais alta qualificação, gerar e difundir conhecimentos, preservar e divulgar os valores éticos, científicos, artísticos e culturais, constituindo-se em instituição estratégica para o desenvolvimento do Ceará, do nordeste e do Brasil.

Realizou-se um estudo de caso envolvendo a análise de riscos de três serviços de TI muito utilizados por professores e alunos do campus da UFC em Quixadá. Foram seguidas todas as etapas do processo de GRSI em conformidade com a norma ISO/IEC 27005.

Os resultados obtidos, ainda que iniciais, indicaram que é possível a existência de um método para análise-avaliação dos riscos, voltado ao foco de alto nível, que seja capaz de atender toda a instituição por completa na sua primeira iteração do processo de GRSI.

Vale ressaltar que a partir da segunda iteração da organização com o processo de *Gestão de Risco*, ela própria tem a obrigação de criar ou adaptar seu próprio método de avaliar os riscos.

A facilidade de compreensão do processo e de seus resultados, a velocidade e o baixo custo em relação a uma análise de alto nível de riscos são as vantagens que essa abordagem abrange. Sabe-se que para tal processo se precisa de uma organização orçamentária da Universidade, um planejamento antecipado dos gastos, e isto reforça a necessidade de um método simples e eficaz que aponte os principais riscos de segurança da informação.

O objetivo deste trabalho não foi apontar os riscos com uma precisão refinada, todavia, os resultados indicam como categorias de riscos que precisar ser refinadas em futuras iterações, a partir de um novo processo de GRSI, seja ele adaptado ou criado do zero. Isto posto, os objetivos desse trabalho foram alcançados já que a proposta de análise/avaliação de riscos colaborou na sistemática de um processo que compreenda a universidade numa concepção genérica.

Por ter envolvido apenas 4 serviços de TI, com uma amostra de participantes limitada, pode existir alguma dificuldade de generalização dos resultados obtidos no estudo de caso. Não foi objetivo desse estudo empírico buscar uma validação estatística. Devido à limitação de acesso a informações gerenciais, os serviços avaliados foram os únicos que puderam ser objeto de estudo frente às limitações citadas.

Adentro do assunto pesquisado ainda ficaram pontos que precisam ser pesquisados. Apresenta-se a seguir uma sugestão para trabalho futuro:

• Aprofundamento das especificidades e restrições do campus da UFC em Quixadá em comparação à segurança da informação.

REFERÊNCIAS

ABNT NBR ISO/IEC 27002:2005 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2005.

ABNT NBR ISO/IEC 27005:2008 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro: ABNT, 2008.

ABNT NBR ISO/IEC 27001:2006 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro: ABNT, 2006.

CAMPOS, André – Sistema de Segurança da Informação: Controlando os Riscos. 2. ed. / André Campos. – Florianópolis: Visual Books, 2007.

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

FERNANDES, Jorge H. C. **Sistemas Complexos**. Universidade de Brasília, Curso de Especialização em Gestão de Segurança da Informação e Comunicações, CEGSIC, Brasília, 2008, Apostila.

FERREIRA, Aurélio Buarque de Holanda, Novo Dicionário da Língua Portuguesa, 2ª edição revista e aumentada, Editora Nova Fronteira – Rio de Janeiro, RJ – 1996.

FILHO, Antonio Mendes da Silva. Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações. 2008.

FONTES, Edison. Segurança da Informação: o usuário faz a diferença. 1a edição. São Paulo: Saraiva, 2006.

KUMAR, Krishan. Da sociedade pós-industrial à pós-moderna: novas teorias sobre o mundo contemporâneo. Rio de Janeiro: J. Zahar,1997.

OLIVEIRA, D.P.R. Sistemas organização e métodos: uma abordagem gerencial. 12.ed. São Paulo: Atlas, 2001

PROMON, Business & Tecnology review. Segurança da Informação – Um diferencial determinante na competitividade das corporações. Rio de Janeiro, 2005.

SÊMOLA, Marcos. Gestão da Segurança da Informação: Uma visão Executiva. Rio de Janeiro: Campus, 2003.

WAZLAWICK, R.S. Metodologia de pesquisa para ciência da computação. Rio de Janeiro : Elsevier, 2008.

WEBSTER, F. Theories of Information Society (4.ª ed.). London: Routledge.1995/1999).

DOCUMENTOS ELETRÔNICOS:

Informações:

Portal UFC, Organograma. Disponível em: <http://www.ufc.br>. Acesso em: 14 de maio de 2014.