UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIENCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIENCIAS DA INFORMAÇÃO
CURSO DE BIBLIOTECONOMIA

GENIELE TRAJANO DA SILVA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: Estudo de caso aplicado a um escritório de advocacia.

João Pessoa
Dezembro 2011

GENIELE TRAJANO DA SILVA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: Estudo de caso aplicado a um escritório de advocacia.

Monografia apresentada ao curso de Biblioteconomia, do Departamento de Ciência da Informação, no Centro de Ciência Sociais Aplicadas (CCSA), da Universidade Federal da Paraíba (UFPB), em cumprimento as exigências e conclusão de curso, Orientado pelo professor Drº Wagner Junqueira de Araújo, como exigência para obtenção de grau de Bacharel em Biblioteconomia.

Orientador: Prof. Dr. Wagner Junqueira de Araújo

João Pessoa

Dezembro 2011

GENIELE TRAJANO DA SILVA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO: Estudo de caso aplicado a um escritório de advocacia.

Trabalho de Conclusão de Curso apresentado ao curso de Biblioteconomia, do Departamento de Ciência da Informação, no Centro de Ciência Sociais Aplicadas (CCSA), da Universidade Federal da Paraíba (UFPB), em cumprimento as exigências e conclusão de curso, como exigência para obtenção de grau de Bacharel em Biblioteconomia.

Aprovada em: ____/____/____

Banca Examinadora

Profº. Drº Wagner Junqueira de Araújo– Orientador UFPB

Profª. Dra. Emeide Nóbrega Duarte– Membro

Profª. Me. Julianne Teixeira e Silva – Membro

Dados Internacionais de Catalogação na Publicação (CIP)

S528g Silva, Geniele Trajano da.

Gestão da segurança da informação: estudo de caso aplicado a um escritório de advocacia./ Geniele Trajano da Silva. – João Pessoa: UFPB, 2011.

59f.: il.

Orientador: Prof. Dr. Wagner Junqueira de Araújo.
Monografia (Graduação em Biblioteconomia) – UFPB/CCSA.

1. Monografia. 2. Gestão da informação. 3. Empresa. 4. Análise de risco. I. Título.

Agradecimentos

São muitos os nomes importantes que devem estar aqui, porém o primeiro deles que merece lugar privilegiado em minha vida e em meu coração, Deus. Agradeço a Deus toda a força de vontade e o persistir dos meus olhos já cansados de ler nas noites em que muitos dormiam. Era no silêncio das madrugadas que sua presença se tornava quase que visível diante da minha fé, me dando força para correr contra o tempo que já se esgotava. Mas uma vez, obrigada Senhor.

Em especial a minha mãe Antônia Trajano que resume todas as coisas boas que tenho e que com o seu modo de amar, me fez forte e capaz de escolher o caminho a trilhar, aquele que sempre me levaria para o bem. Ao meu pai Clóvis Bernardino que mesmo com seu jeito tímido de demonstrar o amor pelos seus filhos, soube educar para a vida, sempre com os pés no chão e pronto para recomeçar sempre que necessário.

Agradeço aos meus irmãos Eudes, Vanderli, Isaac e as minhas irmãs Liete, Ana Paula, Vanuza, Luciana e Itaércia pelos aprendizados que com certeza cada um me passou durante todo esse tempo fora de casa.

Agradeço a minha "família de coração", Edna Lúcia e família, Karim Nascimento e toda sua família, Janine Lucena e toda sua família, Luana Candeia e toda sua família e Patrícia Alves pelas diversas vezes que precisei de um ombro amigo, pois sempre pude contar com todos do meu trabalho que souberam compreender os momentos em que precisei me ausentar para trabalhar nesta pesquisa.

Aos meus amigos da universidade Edcleyton Bruno, Arienne Soares, Samara Gomes, Janiene Alves, Edilson Melo e a todos da sala pelos bons momentos, pelas brincadeiras e pela saudade boa que muitos vão deixar. Vai ser muito gostoso lembrar, de muitos de vocês.

Ao meu grande e admirável professor e orientador Wagner Junqueira, por ter acreditado em mim e ter aceitado me orientar mesmo com o tempo tão curto e com um tema ainda novo na área. Obrigada professor pelo seu profissionalismo e pela sua calma quando eu chegava nervosa e com medo de não dar certo. Obrigada por sua

À todos aqui citados e outros que deixei de citar os meus sinceros agradecimentos.

Dedico à minha maravilhosa mãe por ter educado seus filhos para a vida e por representar o meu conceito de amor e bondade. Não há palavras que expresse o tamanho do meu amor e admiração...

“A mente que se abre a uma nova idéia jamais volta ao seu estado original”

Albert Einstein

Resumo

As tecnologias da informação construíram uma nova forma de vida para a sociedade. A maneira de produzir informação mudou e o modo que essas informações são guardadas, também. Surgiu em meio a tantas inovações, a preocupação com a segurança dos dados produzidos, e os bancos de dados das empresas que são responsáveis por grande parte economia do país, ficaram vulneráveis as possíveis ameaças que existem no meio eletrônico. Assim é interessante pesquisar como a gestão empresarial lida com essa questão. Nesta pesquisa buscou identificar as vulnerabilidades nos procedimentos de gestão da informação em um escritório de advocacia sob a ótica da segurança da informação. Contudo, verificou-se a carência de publicações a respeito do assunto relacionado à área de biblioteconomia. Porém, com os métodos e técnicas de pesquisa aplicados adequadamente, conclui-se que a empresa pesquisada fez altos investimentos em tecnologias da informação, porém foram encontradas vulnerabilidades nos sistemas de segurança da informação, proveniente da falha na gestão por não dispor de uma política de segurança ao acesso de todos, não fazer uso de métodos de classificação da informação e não atualizar os procedimentos de segurança existentes periodicamente. Além dessas medidas de proteção da informação, a pesquisa também disponibilizou medidas para minimizar os impactos caudados por riscos identificados na análise de risco e no questionário aplicado.

Abstract

The information technologies have built a new way of life for society. The way to produce information has changed and how that information is stored, too. It appeared in the midst of so many innovations, concern for the security of the data produced, and the databases of companies that are responsible for much of the country's economy remained vulnerable to potential threats that exist in electronic form. So it is interesting to investigate how corporate governance deals with this issue. This research aimed to identify vulnerabilities in procedures for information management in a law firm from the perspective of information security. However, there was a lack of publications on the subject area related to librarianship. The methods and research techniques applied properly, it is concluded that the investigated company made significant investments in information technology, but were found vulnerabilities in the systems of information security, from the failure to manage not have a policy security access for all, not to use methods of classification of information and not update the existing safety procedures periodically. In addition to these measures of information protection, the survey also provided measures to minimize the impacts identified in the caudate for risk analysis and risk questionnaire.

Lista de Quadros

Lista de Gráficos

Lista de Tabelas

Lista de Siglas

ABNT	Associação Brasileira de Normas Técnicas
FRAP	*Facilitated Risk Analysis Process*
SERPRO	Serviço Federal de Processamento de Dados
TCU	Tribunal de Contas da União

SUMÁRIO

1 INTRODUÇÃO

Werthein (2000) fala a respeito da informação como um fator de transformação social. Desta forma podemos compreender que a mesma precisa ser tratada, armazenada e consequentemente, protegida de possíveis ameaças, sejam elas intencionais ou não, para garantir que seja usada para fins positivos. Veremos com detalhes como se dá esse processo, no decorrer deste trabalho.

Em 2010 foi notícia em quase todos os jornais nacionais e internacionais, o vazamento de documentos diplomáticos contendo informações secretas a respeito principalmente do governo americano. Tais informações foram divulgadas pelo Wikileaks, site especializado em divulgar documentos secretos.

Esse ato gerou uma crise de confiança entre nações, já que as revelações feitas no site tratavam de assuntos de grande importância entre os governos. Mas o que chamo a atenção para este assunto é que essas informações foram vazadas porque estavam vulneráveis às ameaças em algum momento e a mesma se concretizou gerando graves conseqüências. É interessante dizer que esse caso pode ser aplicado também em ambientes mais simples, como por exemplo, um escritório de advocacia.

A ausência da informação ou falha em sua integridade pode gerar danos irreparáveis numa empresa advocatícia já que lida com os problemas da sociedade, onde, por exemplo, a informação é responsável por definir o teor da sentença dado pelos tribunais, envolvendo questões éticas, devido à quebra do sigilo entre parte autora e parte ré. Este trabalho tem como campo, o cenário advocatício, onde o ambiente laboral necessita trabalhar com produções de informações fidedignas e íntegras para obter êxito em seus resultados, como por exemplo, a procedência julgada ao pedido processual.

Observa-se empiricamente que o alto investimento de um escritório de advocacia em tecnologia da informação, torna-se um ato arriscado se o mesmo não faz uso de uma política de segurança dessas informações que estão sobre meios tecnológicos de acesso.

Marciano e Marques (2006) em seu trabalho sobre segurança da informação diz que a tecnologia da informação pode proporcionar formas para ajudar a proteger a informação de ameaças no meio, mas não integralmente. É necessário o uso de políticas e sistemas de segurança.

> [...] este universo de conteúdos e continentes digitais está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem seriamente a segurança das pessoas e das informações a elas atinentes, bem como das transações que envolvem o complexo usuário-sistema-informação (MARCIANO E MARQUES, 2006, p.89)

Diante das citações supracitadas, justifica-se o interesse de se estudar a gestão da informação produzida em um escritório de advocacia.

2 OBJETIVOS

Gerais

- O trabalho busca identificar as vulnerabilidades nos procedimentos de gestão da informação em um escritório de advocacia sob a ótica da segurança da informação.

Específicos

Os objetivos específicos deste trabalho são:

- Verificar os processos de gestão do escritório;
- Identificar os procedimentos de segurança da informação implantados;
- Analisar os riscos provocados por possíveis ameaças e vulnerabilidades existentes;
- Avaliar os possíveis impactos provocados riscos a segurança da informação;
- Indicar medidas para minimizar os riscos;

3 FUNDAMENTAÇÃO TEÓRICA

Toda informação deve ser bem administrada, para garantir que ela esteja disponível em perfeito estado e em sua integridade. Essa idéia é teoricamente, o essencial. Mas com o avanço da tecnologia, as informações produzidas e armazenadas em redes tornaram-se frágeis.

Tal qual descreve o Tribunal de Contas da União em seu manual de boas práticas em segurança da informação:

> Na sociedade da informação, ao mesmo tempo que as informações são consideradas o principal patrimônio de uma organização, estão também sob constante risco, como nunca estiveram antes. Com isso, a segurança de informações tornou-se um ponto crucial para a sobrevivência das instituições. (BRASIL, 2003, p. 6)

De acordo com Araújo (2009), numa sociedade conectada em rede, as organizações tanto privadas quanto governamentais, precisam de processos que controlem esses fluxos de informações no objetivo de garantir e proteger sua informação das novas ameaças.

3.1 A informação como principal fator de competitividade na empresa

Nota-se que hoje as empresas estão dando mais atenção a questão da segurança da informação, pois é notável que a informação já é vista como um fator de valor e de competitividade. Mas é visível também que esse mesmo fator de competitividade tornou-se vulnerável e foi necessário que surgisse meios para protegê-la das ameaças, que num mundo totalmente conectado, fica ainda mais difícil reconhecer as intenções de quem as pretende acessar.

> As organizações estão modificando-se profundamente, invertendo suas pirâmides organizacionais, criando unidades de negócios autônomas, descentralizando decisões e constituindo parcerias. A garantia de sua integração e da manutenção de parâmetros comuns de atuação é dada pela informação, que flui entre suas várias partes (LAUREANO, 2005, p.7)

A informação tem o poder de transformar, seja ela onde for aplicada. Quando bem administrada gera bons frutos e desenvolvimento. A informação deve ser estudada

como fator essencial que permite o salto para a verdadeira transformação da sociedade (AMARAL, 1996). Se aplicarmos esta idéia numa empresa, iremos observar que aquela que tem sua informação bem armazenada, organizada e protegida, leva vantagem sobre aquelas que são contrárias a este pensamento.

> [...] a informação custa dinheiro para as empresas, mas os bons empresários logo percebem que esse investimento acaba garantindo melhor lucro, a partir do momento em que influi no crescimento da produção (...) quanto mais crescente o setor informativo, maior fica a capacidade de o país ou pessoa para agregar valor a seus próprios recursos (VITRO, 1988 apud AMARAL 1996).

Para um administrador de uma determinada empresa tomar a decisão sensata frente a um problema de urgência, ele precisa ter todas as informações a respeito do mesmo e de tudo aquilo que está ligado ao problema. Essa informação deve ter caráter verdadeiro, caso contrário ele tomará uma decisão baseada em falsas informações e terá grande probabilidade de equivocar-se, podendo dessa forma piorar ainda mais o problema que se tentava solucionar. É dessa forma que a informação se torna um fator de competitividade no mundo de hoje, não basta apenas uma estrutura empresarial de causar inveja as concorrentes, deve-se principalmente cuidar do conteúdo que é produzido interiormente e fazer um bom uso do mesmo.

> A informação e os processos de apoio, sistema, e redes são importantes ativos para os negócios. Confidencialidade, integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização no mercado (ABNT ISO/IEC 17799:2001)

Essa consciência de que a informação tornou-se vulnerável, fez as organizações repensarem na segurança da informação e a partir daí começa a surgir sistemas e políticas de segurança para minimizar os possíveis riscos que existem no meio empresarial e onde quer que exista informação.

Contudo nem toda informação produzida em uma organização possui o mesmo valor. Quando se propõe procedimentos de segurança da informação, o primeiro passo é saber quais são as informações realmente relevantes à organização. Tais informações serão objetos dos processos de segurança da informação, para tal é necessário que a

organização classifique suas informações, portanto deve-se conhecer métodos e técnicas para sua classificação.

3.2 Classificação da Informação

A classificação da informação é o processo que irá permitir a proteção diferenciada dos diversos suportes de dados, permitindo uma eficiente gestão dos recursos necessários para a proteção dos bens da Empresa (SILVA, CARVALHO E TORRES, 2003, p.234)

Agregar valores as informações produzidas dentro da empresa é essencial quando se pretende implantar um sistema de segurança da informação. Pois quanto maior o grau de sensibilidade da informação, maior será o investimento na segurança.

Tal como afirma Ferreira e Araújo (2008):

> A classificação da informação é o processo de estabelecer o grau de importância das informações mediante seu impacto no negócio, ou seja, quanto mais estratégica e decisiva para manutenção ou sucesso da organização, maior será sua importância. A classificação deve ser realizada a todo instante, em qualquer meio de armazenamento (FERREIRA e ARAÚJO, 2008, p.78)

A literatura consultada (FERREIRA e ARAÚJO, 2008; ARAÚJO, 2009; BRASIL, BRASIL, TCU) indica diferentes formas e níveis de se trabalhar a classificação da informação.

Laureano (2005) diz que é exposto, a necessidade de classificação da informação em níveis de prioridade, respeitando a necessidade de cada empresa assim como a importância da classe de informação para a manutenção das atividades da empresa (WADLOW, 2000; ABREU, 2001; BORAN 1996, apud LAUREANO 2005, p.08).

Uma informação pode ter vários níveis de organização, mas de acordo com Ferreira e Araújo (2008), três são essenciais para que se tenha uma boa classificação sem deixar a desejar, são eles:

• **Informação Pública**: São informações que não necessitam de cuidados especiais, em caso de acesso e divulgação, não ocasiona prejuízos para a organização.

• **Informação interna**: São informações onde o acesso não autorizado deve ser evitado, no entanto, se divulgadas as conseqüências não serão críticas.
• **Informação confidencial:** São informações bastante relevantes, onde o acesso não autorizado pode gerar grandes perdas financeiras e de competitividade.

Existem decretos que tratam da segurança da informação da sociedade e do Estado. São as informações de caráter sigiloso. De acordo com decreto presidencial n° 4553, a classificação de documentos segundo grau de sigilo é: ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos. O Art. 7, do Decreto 5301/2004, determina os prazos de validação da seguinte forma:

• Ultra-secreto: máximo de trinta anos;
• Secreto: máximo de vinte anos;
• Confidencial: máximo de dez anos; e
• Reservado: máximo de cinco anos.

Há ainda na área literária, outros níveis de classificação da informação, mas vamos usar o nível citado por Ferreira e Araújo, por suprir a necessidade deste trabalho, pela sua linguagem simples e pela fácil compreensão que oferece sobre o assunto. A classificação da informação é um processo fundamental para a implementação de processos de segurança da informação.

3.3 Segurança da informação

Quando classificamos a informação de maneira adequada pode-se partir para um segundo ponto que é a segurança. É preciso entender o que é a segurança da informação e o que ela envolve num setor organizacional.

> Segurança da informação é a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas (ABNT NBR ISO/IEC 7799:2005)

O Decreto n° 3505/2000 define segurança da informação como proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações (...). As definições a respeito do que é segurança da informação, são bem semelhantes, no entanto para este trabalho vamos considerar a definição dada pela ABNT NBR ISO/IEC 7799, já que satisfaz de forma concisa a idéia deste tópico.

Numa organização privada ou governamental existem vários tipos de pessoas que envolvem a segurança da informação, seja de forma direta ou indireta. Desde aqueles que firmaram contrato com a unidade até aqueles que são apenas estranhos, ou estão ali temporariamente. Essas pessoas são chamadas por alguns autores de Atores da Segurança. Ou seja, aqueles que estão vinculados a informação de alguma maneira.

> Os atores da segurança são infinitos, pelo menos potencialmente. De elementos internos à Empresa a perfeitos estranhos, de clientes a parceiros, passando obviamente pelos funcionários, todos podem ter um impacto positivo ou negativo sobre a segurança da mesma (SILVA; CARVALHO; TORRES, 2003, p. 26).

É notável que a questão da segurança da informação é muito mais complexa do se pensava. Nota-se diante das citações supracitadas, que esse tema abrange toda a organização e não apenas aqueles que trabalham diretamente com a produção da informação, como os diretores, gerente, entre outros, mas pode começar da pessoa responsável pelo serviço geral da empresa até os seus mais importantes clientes. Para melhor compreender quem são os atores da informação, segue abaixo uma tabela com os mais comuns e suas definições:

Tabela 01– Definição dos Atores da Segurança da Informação

Atores da Segurança	Definição	Fonte
Administração da Empresa	São os proprietários da informação usada pela Empresa na sua relação com os clientes e na produção e comercialização dos seus bens.	Silva, Carvalho e Torres (2003, p.27)
Informáticos	Os colaboradores da empresa envolvidos de alguma forma na gestão dos sistemas de informação	Silva, Carvalho e Torres (2003, p.29)
Clientes	Constituinte; aquele que compra; freguês	Aurélio Albuquerque de Holanda Ferreira (2001)
Parceiros	Entidades externas que participam de múltiplas formas nos processos de negócio, tanto ao nível dos	Silva, Carvalho e Torres (2003, p.32)

	canais de distribuição, como na produção	
Pessoal temporário	Similar ao restante dos atores, requer um cuidado cauteloso e que seja assinado um contrato de confidencialidade e de aceitação da política de segurança da empresa.	Silva, Carvalho e Torres (2003, p.33)

Quando conhecemos o processo de segurança da informação, podemos observar a preocupação de proteger a informação das ameaças que existem quando há vulnerabilidades no sistema. Para entendermos como funciona a segurança da informação, alguns conceitos devem ser expostos neste trabalho, como por exemplo, o conceito de ameaça e vulnerabilidade na visão de vários autores. Ter conhecimento desses conceitos ajuda acima de tudo, identificá-los.

3.3.1 Vulnerabilidade

A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc (LAUREANO, 2005, p.17).

> A vulnerabilidade é definida como uma falha nos procedimentos de segurança, software, controles internos do sistema, ou implementação de sistema que podem afetar a integridade, confidencialidade, responsabilidade, disponibilidade ou de dados ou serviços. Vulnerabilidades incluem falhas que podem ser deliberadamente explorado e aqueles que podem causar a falha devido às inadvertidas ações humanas ou desastres naturais (Peltier, 2005, p. 218, tradução nossa).

Segundo o SERPRO (Serviço Federal de Processamento de dados), “vulnerabilidade é uma fraqueza que pode ser explorada por uma ameaça”. Quando o usuário da informação é descuidado com a segurança da mesma, aumenta ainda mais o grau de vulnerabilidade. Não haver controle de acesso a informação, sistemas desprotegidos de antivírus, entre outros, são exemplos que permitem que a informação se torne vulnerável às ameaças.

> Os avanços nas telecomunicações e nos sistemas de informação ampliaram essas vulnerabilidades. Sistemas de informação em diferentes localidades podem ser interconectados por meio de redes de telecomunicações. Logo, o potencial para acesso não

> autorizado, abuso ou fraude não fica limitado a um único lugar, mas pode ocorrer em qualquer ponto de acesso à rede (LAUREANO, 2005, p.18).

Diante das definições de vulnerabilidades, podemos dizer que toda unidade de informação necessita de alertas e posicionamento para o bom funcionamento da empresa. É cabível tomar medidas para que as ameaças, e vulnerabilidades sejam enfrentadas com segurança e calma.

Uma dessas medidas é a prevenção, que procura reduzir a probabilidade de concretização dos riscos. No momento que esses riscos se concretizam é extinto o seu efeito preventivo e logo é necessário recorrer para outra medida. A proteção vai, através de sistemas de informação com capacidade de inspeção, detecção, reação e reflexo, buscando reduzir e limitar o impacto das ameaças quando concretizadas.

3.3.2 Ameaça

As ameaças é o resultado das vulnerabilidades, ou seja, precisa que haja um descuido e que diante desse descuido, seja a informação provida de algum valor, que em caso de ataque venha a ter algum tipo de prejuízo para a empresa.

Ameaça é a causa potencial de um indesejável incidente o qual pode resultar em um dano para um sistema ou organização (SERPRO, 2007).

> A ameaça pode ser definida como qualquer ação, acontecimento ou entidade que possa agir sobre um ativo, processo ou pessoa, através de uma vulnerabilidade e conseqüentemente gerando um determinado impacto. As ameaças apenas existem se houverem vulnerabilidades, sozinhas pouco fazem (LAUREANO, 2005, p. 15).

Existem vários tipos de ameaças ou threat (significado para ameaça em inglês). Tais quais:

> • **Ameaça Inteligente**: Circunstância onde um adversário tem a potencialidade técnica e operacional para detectar e explorar uma vulnerabilidade de um sistema;
> • **Ameaça**: Potencial violação de segurança. Existe quando houver uma circunstância, potencialidade, ação ou evento que poderia romper a segurança e causar o dano;

> • **Ameaça de Análise**: Uma análise da probabilidade das ocorrências e das conseqüências de ações prejudiciais a um sistema;
> • **Conseqüências de uma ameaça**: Uma violação de segurança resultado da ação de uma ameaça. Inclui: divulgação, usurpação, decepção e rompimento. (SHIREY, 2000 apud LAUREANO 2005).

De acordo com Sêmola (2003, apud Laureano 2005), as ameaças podem ser classificadas quanto a sua intencionalidade e ser divididas em grupos:

• **Naturais** – São as ameaças natural, ou seja, não há interferência do homem, como incêndios naturais, enchentes, terremotos, tempestades, poluição, etc.
• **Involuntárias** – São ameaças ocasionadas involuntariamente, sem a intenção de causar.
• **Voluntárias** – São ameaças causadas de maneira consciente, onde o agente tem intenção de causar, como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

De acordo com Peltier (2005, p. 18, tradução nossa) diz ainda que há três categorias principais de fontes da ameaça, as quais cita, as define abaixo e tomaremos como base:

Ameaças naturais – Ameaças provocadas por fenômenos da natureza como inundações, terremotos, furacões, corrimentos, avalanchas, tempestades elétricas, e outros tais eventos.

Ameaças humanas – São ameaças provocadas por ações humanos, sejam elas involuntárias ou não.

Ameaças ambientais – São ameaças causadas pelo meio, como falhas elétrica a longo prazo, poluição, derramamentos químicos, escapamento líquido.

Muitas empresas fazem grandes investimentos em segurança da informação. Portanto existem alguns princípios a serem seguidos quando se pretende desenvolver

um sistema de segurança da informação. Um bom programa de segurança conhece bem esses princípios.

3.4 Princípios dos programas de segurança

De acordo com Silva, Carvalho e Torres (2003) um programa de segurança bem desenvolvido deve minimizar as vulnerabilidades do programa de segurança, (...) baseado num conjunto de princípios garantindo o seu equilíbrio e eficiência. São eles: Relação custo/benefício; concentração; proteção em profundidade; consistência do plano e redundância.

> Os administradores de hoje devem saber como estruturar e coordenar as diversas tecnologias de informação e aplicações de sistemas empresariais para atender às necessidades de informação de cada nível da organização e às necessidades da organização como um todo (LAUREANO, 2005, p.06).

É imprescindível dizer que toda organização que tem controle da informação produzida ganha vantagem junto às concorrentes, pois está mais preparada para enfrentar os problemas e automaticamente nas tomadas de decisões.

Todas estas medidas, independentemente do seu objetivo, necessitam ser implementadas antes da concretização do risco, ou seja, antes do incidente ocorrer (SILVA; CARVALHO; TORRES, 2003, pag. 18). Logo as medidas de segurança devem ser tomadas visando possíveis riscos. Não se deve esperar a concretização da ameaça para pensar em um plano de minimização do impacto, mas é necessário considerar todos os possíveis acontecimentos e estar sempre atento aos ataques.

> A preservação da confidencialidade, integridade e disponibilidade da informação utilizada nos sistemas de informação requer medidas de segurança, que por vezes são também utilizadas como forma de garantir a autenticidade e o não repúdio (SILVA; CARVALHO; TORRES, 2003, pag. 17).

O tipo de sistema utilizado vai depender de cada organização e o tipo de informação que a mesma trabalha. Porém os princípios da segurança são importantes para guiar os passos para a criação do sistema de segurança.

3.4.1 Relação Custo/Benefício

A relação custo/benefício traduz a necessidade de garantir uma relação favorável entre os gastos associados à implementação de medidas de segurança e o retorno em matéria de prevenção e proteção (SILVA; CARVALHO; TORRES, 2003 p. 19). Assim sendo, esse princípio avalia se o retorno é condizente com o investimento. Esse ponto passa a ser um problema nas pequenas organizações, já que normalmente esse tipo de investimento tem um custo elevado não compatível muitas vezes com rendimento da empresa. Por isso o grupo responsável pela criação do sistema de segurança deve saber avaliar a necessidade real da empresa, para não causar gastos desnecessários. Quanto mais importante e sigilosa for a informação, maior será o investimento na segurança sobre ela. E essa caracterização é dada pela direção da organização, que deve estar a ciente de toda movimentação da empresa e acompanhar todo processo de criação do sistema de segurança da informação.

3.4.2 Concentração

Segundo Silva, Carvalho e Torres (2003, p. 19) a concentração “tem como objetivo melhorar a eficiência da gestão das medidas de proteção, reduzindo as duplicações necessárias quando se tem de proteger diferentes repositórios de informação sensível com requisitos de proteção idênticos”. Desse modo vemos que esse princípio não é aplicado a qualquer tipo de informação, mas é aplicado de acordo com seu grau de importância ou sensibilidade.

3.4.3 Proteção em profundidade

A aplicação deste princípio evita a existência de um conjunto de medidas de proteção distintas e avulsas, transformando-as numa sequência de obstáculos somados, adaptados aos fins a que se destinam (SILVA; CARVALHO; TORRES, 2003. p. 20). Observa-se que as medidas de segurança procuram ser simples, porém eficaz, evitando o uso de várias medidas desnecessárias.

3.4.4 Consistência

O princípio da consistência afirma que as medidas de proteção dos bens com grau de sensibilidade equivalente deverão ser também, equivalentes, ou seja, a proteção deverá ser homogênea face à sensibilidade dos bens protegidos (SILVA; CARVALHO; TORRES, 2003, p. 20). Esse princípio deve ser aplicado em todos os pontos de acesso em que a sensibilidade da informação possa ser atingida e não apenas em um ponto. Não deve apenas dar ênfase ao meio lógico, por exemplo, mas dependendo da informação e como ela está armazenada, deve-se aplicar a mesma importância no meio físico.

3.4.5 Redundância

O princípio da redundância dita a necessidade de empregar mais de uma forma de proteção para o mesmo fim, de modo a impedir que a proteção de um bem seja comprometida por uma única falha (SILVA; CARVALHO; TORRES, 2003, p. 20). Dessa maneira evita-se de um contratempo colocar em risco todo o sistema de segurança. Em caso de risco outra medida de preservação já deve estar em total e perfeita funcionalidade para não permitir a concretização da ameaça.

Contudo é necessário saber o que proteger contra o que, quais os custos envolvidos. Para isso é preciso implementar uma gestão de risco que administre toda a operação do sistema de segurança.

3.5 Gestão de Risco

A gestão de risco é um assunto extremamente abrangente, envolvendo vários fatores de diversa natureza, como por exemplo: financeiro, pessoas, informações, entre outros. No que se refere à informação, deve-se levar em consideração o seu valor mediante a uma ameaça. É essencial que se faça uma definição para seguir uma linha de pensamento facilitando a sua compreensão. Assim sendo, temos várias definições. “A gestão de risco pode ser definida como a identificação, a análise, o controle, a

minimização da perda que pode ser associada com eventos" (KRUTZ e VINES, 2001, p.18 apud ARAÚJO, 2009).

Segundo Peltier (2005, p. 10, tradução nossa) "A gestão de riscos é uma responsabilidade de gerência. Para ser bem sucedido, o processo da gestão de riscos deve ser suportado pela alta administração e o conceito da posse dos recursos estabelecidos". Observamos que a administração responsável por manter a informação sob segurança deve encarregar-se de promover essa gestão.

Gestão de risco são atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos (ABNT NBR ISO/IEC 27001). Vamos tomar como base esta definição por se tratar da definição dada pela norma quer rege a gestão dos sistemas de segurança da informação.

Compreendemos assim que o objetivo da gestão de risco é evitar perdas, mas especificamente para este trabalho, a perda da informação. Segundo Araújo (2009) "O objetivo preliminar da gestão de risco é reduzir o risco a um nível aceitável. O que esse nível é depende da organização, do valor de seus recursos e do tamanho de seu orçamento".

Araújo (2009) diz que "[...] uma parte preliminar do processo de gestão de risco está em atribuir valores às ameaças e estimar sua freqüência, ou a probabilidade dessa ameaça ocorrer".

No processo de gestão de risco existem alguns termos que, se bem definidos, ajudam na compreensão a gestão de risco. Araújo (2009) em seu trabalho "A Segurança do conhecimento nas práticas da gestão da segurança da informação e da gestão do conhecimento", apresenta a tabela abaixo que trata das definições dos principais termos, que confere-se abaixo:

Quadro 01- Termos relacionados à gestão de risco

Termo	**Descrição**	**Autor**
Ameaça	A presença de todo o evento potencial que causar um impacto indesejável na organização é chamada de ameaça. Pode ser provocada ou natural, ter um efeito pequeno ou grande na segurança ou na viabilidade de uma companhia.	Krutz e Vines (2001, p. 19-20)

Ativo	É um recurso, processo, produto, ou infra-estrutura, e assim por diante, que uma organização determinou que deve ser protegido. A perda deste recurso poderia afetar a confidencialidade, integridade ou disponibilidade. Pode ser tangível ou intangível, podendo afetar a continuidade do negócio de uma organização. O valor de um ativo é composto de todos os elementos que são relacionados a esse recurso: sua criação, desenvolvimento, sustentação, reposição, credibilidade, custos considerados e valor de aquisição.	Krutz e Vines (2001, p. 19-20)
Brecha	É quando um mecanismo da segurança pode ser contornado por uma ameaça. Quando uma brecha é combinada com um ataque, pode resultar em uma invasão.	Tittel et al. (2003, p. 181)
Exposição	Suscetibilidade para perda de um ativo devido a uma ameaça, há possibilidade que uma vulnerabilidade seja explorada por um agente ou por um evento da ameaça.A exposição não significa que um evento de perda esteja ocorrendo realmente. Significa que, se houver uma vulnerabilidade e uma ameaça que possam ser exploradas existe a possibilidade de ocorrer uma exposição.	Tittel et al. (2003, p. 180)
Invasão	É quando um agente da ameaça ganha o acesso à infra- estrutura de uma organização com a subversão dos controles de segurança e pode infringir danos diretamente aos ativos.	Tittel et al. (2003, p. 181)
Proteção	É um controle ou as contramedidas empregadas para reduzir o risco associado a uma ameaça específica, ou o grupo de ameaças.	Krutz e Vines (2001, p. 19-20)
Risco	É a possibilidade de que uma ameaça específica venha explorar uma vulnerabilidade específica e causar dano a um ativo.	Tittel et al. (2003, p. 180)
Vulnerabilidade	É a ausência ou a fraqueza de uma proteção. Uma ameaça mínima tem o potencial de transformar-se em grande ameaça, ou em ameaça mais freqüente, por causa de uma vulnerabilidade.	Krutz e Vines (2001, p. 19-20)

Quadro 8 - Termos relacionados à gestão de risco
Fonte: Araújo, 2009.

3.5.1 Identificação do Risco

O processo de identificação de risco deve ser feito observando todos os pontos fracos e críticos do sistema. Os procedimentos devem ser tomados baseados na identificação das vulnerabilidades, ou seja, encontrar dentro do meio observado, as falhas que poderiam levar a perdas do bem no qual se pretende proteger. Segundo Peltier (2005, p.8, tradução nossa) “O risco é uma ameaça que explora alguma vulnerabilidade que poderia causar o dano a um recurso”. Após identificar os riscos, é preciso que antes de se tomar qualquer atitude, analisá-lo e verificar seu impacto sobre o bem protegido.

3.5.2 Processo de Análise de Risco e seu Impacto

Segundo Peltier (2005, p.15, tradução nossa), “A análise de risco é uma técnica usada para identificar e avaliar os fatores que podem comprometer o sucesso de um projeto ou de conseguir um objetivo”. Na gestão de risco existem dois tipos de análise de risco: análise quantitativa e análise qualitativa (KRUTZ e VINES, 2001; TITTEL et al., 2003 apud ARAÚJO, 2009, p. 53).

> A diferença entre a análise de risco quantitativa e qualitativa é simples: a quantitativa tenta atribuir valores numéricos ou monetários objetivos aos componentes da avaliação de risco e à avaliação de perdas potenciais, e a qualitativa é mais direcionada para os valores intangíveis dos dados e de outros ativos, que simplesmente o valor puro (ARAÚJO, 2009)

A análise quantitativa não é por completa satisfatória, pois em algum momento ela vai ser substituída pela análise qualitativa, já que esta oferece a oportunidade de interpretação. o processo para implementação de uma análise qualitativa de risco envolve julgamento, intuição e experiência (TITTEL et al. 2003, p. 186 apud ARAÚJO, 2009, p.52).

Os procedimentos de análise de risco podem compor as normas de uma política de segurança.

3.6 Políticas de Segurança

A política de segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos da informação (FERREIRA; ARAÚJO, 2008, p. 36). Ativo, de acordo com a ABNT ISO/IEC 27001, é tudo aquilo que tem valor na organização. Essas normas, métodos e procedimentos devem ser simples para serem bem compreendidas e devem corresponder ao grau de sensibilidade da informação, por isso vale ressaltar a importante da classificação da informação para uma política de segurança.

A ABNT ISO/IEC 17799 diz que "... a direção estabeleça uma política clara e demonstre apoio e comprometimento com a segurança da informação através da emissão e manutenção de uma política de segurança da informação para toda a organização"

> Deve-se utilizar uma visão metódica, criteriosa e técnica em seu desenvolvimento e elaboração, de forma que possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologia, na definição de responsabilidades, e por fim, na elaboração das políticas com o perfil da empresa e dos negócios que ela pratica (FERREIRA; ARAÚJO, 2008, p. 36).

Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos (TCU, 2003, p.28). Deve ter a cooperação de todos da organização para seu bom funcionamento, mas para isso é necessário que os mesmos sejam conscientizados pela alta administração. A política varia de acordo com a organização, dependendo do teor da informação é que há necessidade de aplicar uma política mais rigorosa. É importante que a política estabeleça ainda as responsabilidades das funções relacionadas com a segurança e discrimine as principais ameaças, riscos e impactos envolvidos (DIAS, 2000 apud LAUREANO, 2005, p.56). Mas antes disso, é preciso que se tracem os propósitos da política, enxergar a real necessidade dela. A política de segurança vai procurar guiar os caminhos que serão seguidos por todos dentro da empresa nos se refere a trabalhar com a segurança da informação.

O TCU (2003) nos alerta a respeito das alterações após elaboração e funcionalidade da política quando diz não só pode ser alterada, mas também como deve. É importante que seja revisada até mesmo porque, dessa maneira se identifica seus pontos fracos e se a mesma ainda está condizente para aquele ano ou época e se será necessário uma nova política ou fazer apenas algumas atualizações. Para fins desta pesquisa as políticas de segurança da informação são instrumentos objetos da investigação, descrito na metodologia.

4 METODOLOGIA DA PESQUISA:

Nos procedimentos metodológicos foi definido o tipo de pesquisa, a amostra, os métodos para coleta de dados e análise dos resultados.

4.1 Tipo de Pesquisa

É essencial a escolha do tipo de pesquisa quando se investiga um problema, já que dessa forma, descreve a estrutura que será utilizada para atingir seus objetivos.
Esta pesquisa se caracteriza como descritiva-exploratória, transversal e de natureza quanti-qualitativa.

Os estudos exploratórios, de acordo com Gil (2002), têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito. Por sua vez os estudos descritivos podem complementar os exploratórios. Segundo Almeida:

> [...] um estudo descritivo observa , registra, analisa e ordenam dados, sem manipulá-los, isto é, sem interferência do pesquisador. Assim, para coletar tais dados, utiliza-se de técnicas específicas, tais como: entrevista, formulário, questionário e observação, leitura analítica (ALMEIDA 1996, p. 104).

É possível encontrar na literatura, outras definições, contudo para fins deste trabalho os conceitos apresentados só suficientes. Uma vez definido o estudo exploratório e o descritivo, faz necessária a compreensão da combinação dessas duas características para entendermos o motivo pelo qual a pesquisa é descritiva-exploratória. O estudo exploratório-descritivos combinados – são estudos exploratórios que têm por objetivo descrever completamente determinado fenômeno (MARCONI e LAKATOS, 2010, p. 171).

A pesquisa é transversal quando se refere a sua dimensão temporal, pois seus resultados podem variar de acordo com o tempo e as variáveis que influenciam. Como por exemplo: Um questionário a respeito da violência aplicado há 10 anos pode não ter o mesmo resultado se aplicado em tempos diferentes. Em um estudo do tipo transversal,

ao se descrever e explorar fenômenos específicos em determinado momento, não há comparação dos dados ao longo do tempo.

Segundo Malhotra (2001, p. 155), “a pesquisa quantitativa procura quantificar os dados e aplicar alguma forma de análise estatística”. Na maioria das vezes, esse tipo de pesquisa deve suceder a pesquisa qualitativa, já que esta última ajuda a contextualizar e a entender o fenômeno.

A pesquisa quanti-quali, como o próprio nome sugere, representa a combinação das duas citadas modalidades, utilizando em parte do trabalho a visão positivista, e em outra parte a visão fenomenológica, aproveitando-se o que há de melhor em cada uma delas (ARAÚJO; OLIVEIRA, 1997, p.45).

A pesquisa quali-quantitativa deste se deu com a aplicação do questionário, seguindo os critérios de inclusão e exclusão, e a análise de risco.

4.2 Princípios éticos e formais

É importante que o pesquisador seja consciente do limite de suas pesquisas. O pesquisador enquanto ciente de seus direitos e deveres deve procurar fazer o seu trabalho dentro dos limites estabelecidos. Por exemplo, não cabe ao investigador forçar uma pessoa, enquanto objeto de estudo, a responder um questionário ou dar entrevista. Deve-se explicar o motivo da pesquisa, sendo claro na importância e objetivo de se responder ao questionário e respeitar a decisão tomada pela pessoa.

Fortin (2003, p. 116), descreve um conjunto de “princípios ou direitos” tendo em conta o determinado pelos códigos de ética: “ …o direito à autodeterminação, o direito à intimidade, o direito ao anonimato e à confidencialidade, o direito à proteção contra o desconforto e o prejuízo e …o direito a um tratamento justo e leal …”. Após levado em consideração esses princípios, digeridos e seguidos, o pesquisador pode dar continuidade a suas pesquisas.

Diante o exposto, a pesquisa com a aplicação do questionário, utilizou de codinomes para se realizar, dando o direito do anonimato, confidencialidade além total conforto para responder o que pede a pesquisa, sem ocasionar danos de nenhum tipo.

4.3 Campo de Estudo

Este estudo foi realizado em um escritório de advocacia, situado na cidade de João Pessoa – PB. O local foi escolhido devido o exercício do cargo de assistente jurídica desta empresa, fato que possibilita a observação e acesso a mesma em todo horário de funcionamento.

A empresa foi fundada em 1992, mas a partir de 2002 avançou para os demais estados nordestinos, tais quais: Recife, Aracajú, Natal, além de todo território paraibano como Campina Grande, Patos, Sousa e Cajazeira. Fazendo-se presente também em Brasília. É notável que se trata de uma empresa de médio porte e que provoca a curiosidade a respeito de sua gestão e nesse caso, a gestão da segurança da informação ali contida, mais especificamente na sede situada na capital da Paraíba, João Pessoa.

O Escritório aqui pesquisado trabalha com a área cível, trabalhista, tendo alguns casos isolados como criminal e eleitoral. Faz uso de ferramentas como arquivo deslizante, não deslizante e digital. Salas climatizadas e automatizadas, ótima iluminação.

4.4 Critérios de inclusão e exclusão

Para realização desta pesquisa, foi utilizados os seguintes critérios de inclusão e exclusão.

Critérios de Inclusão

• 1 Diretor, 2 advogados, 1 gerente , 1 assistente jurídica, 1 arquivista, e 1 estagiário que trabalham na empresa que estavam presentes e concordaram em participar da pesquisa.

Critérios de Exclusão

• Diretores, advogados, secretária, auxiliar de limpeza e estagiários que trabalham na empresa que estavam ausentes ou não concordaram em participar da pesquisa.

4.5 Definição do Universo e da Amostra

Segundo Marconi e Lakatos (2001, p. 108)

> [...] população é o conjunto de seres animados ou inanimados que apresentam pelo menos uma característica em comum (...). A delimitação do universo consiste em explicitar que pessoas ou coisas, fenômenos etc. serão pesquisadas, enumerando suas características comuns [...] (MARCONI e LAKATOS, 2001, p. 108).

A população correspondeu aos profissionais que exercem as seguintes atividades na empresa: cumprimento dos prazos, processo de digitalização, consulta processual, empréstimo de documentos, cadastro de processo e seu acompanhamento eletrônico, protocolo eletrônico, integral, via sedex e via fax, agendamento de audiência, atendimento ao cliente (reuniões, informar a respeito de audiência, acompanhar o mesmo em audiências), atividades financeiras, tais como: pagamentos, transferências, prestação de contas, contratos de prestação de serviços (informática, telefonia e internet) e diligências como: xerografar processos nos fóruns e tribunais e analisar, enviar relatórios aos clientes.

Não há necessidade de se trabalhar com toda a população ou universo que envolve a pesquisa, mas a técnica utilizada é a de trabalhar com uma parcela dessa população, [...] que contém todas as características da população ou do universo. (PARRA FILHO e SANTOS, 1998, p. 196). Observa-se que a amostra é o número específico de indivíduo ou fator em que a pesquisa foi aplicada. Deve ser bem definida para que não tenha erros nos resultados. Para aplicação do questionário foi selecionada uma amostra de 7 (sete) integrantes da empresa que trabalham diretamente com acesso a informação, de um universo de 25. E na análise de risco, foi selecionada uma amostra de três atividades, tais quais: digitalização, tabelas de prazos, acompanhamento processual. Foram escolhidas essas três atividades por te sido observado empiricamente que são as que mais podem apresentar possíveis vulnerabilidades a ameaça e risco para a informação.

A amostra selecionada para este estudo foi do tipo não probabilística, já que não faz uso de seleção aleatória. A amostra foi escolhida intencionalmente. Segundo Carmo e Ferreira (1998, p. 197), esse tipo de amostra tem “[...] como base critérios de escolha intencional sistematicamente utilizados com a finalidade de determinar as unidades da população que fazem parte da amostra... para fazer estudos em profundidade”. Marconi e Lakatos (2001, p. 108) dizem que amostragem não-probabilista, “[...] não fazendo uso de uma forma aleatória de seleção, não pode ser objeto de certos tipos de tratamento

estatísticos, o que diminui a possibilidade de inferir os resultados obtidos para a amostra".

4.6 Técnicas de Instrumento e Coleta de Dados

Para Araújo:

> A coleta de dados, no estudo de caso, pode ser feita, principalmente, a partir de seis fontes de evidências: documentos, registros em arquivos, entrevistas, observação direta, observação participante e artefatos físicos; embora os autores não restrinjam a somente essas técnicas, o que permite a utilização de outras técnicas. (GODOY, 2006; YIN, 2005 apud ARAÚJO, 2009, p.116).

Para coleta de dados desta pesquisa, foi utilizada a aplicação de questionários para identificação do risco (Apêndice A) visto que SEVERINO (2007, p. 125) define questionário como sendo "conjunto de questões, sistematicamente articuladas, que se destinam a levantar informações escritas por parte dos sujeitos pesquisados...". Conhece-se assim a opinião dos mesmos a respeito do assunto que se pretende pesquisar. O questionário é a mais utilizada técnica de coleta de dados (CERVO e BERVIAN, 1996). Tecnicamente falando, o questionário constitui um meio de obter respostas sobre determinado assunto de maneira que o respondente forneça as informações de seu domínio e conhecimento.

Foi usada, também como método de pesquisa, a observação. Marconi e Lakatos (2010, p. 173) dizem que "a observação é uma técnica de coleta de dados para conseguir informações e utiliza dos sentidos na obtenção de determinados aspectos da realidade". Sendo assim, utilizamos a observação do tipo participante natural para a análise de risco. Nesse tipo de observação, o observador participa da mesma comunidade (MARCONI E LAKATOS, 2010, p. 26). Adotamos como exemplo de elaboração a tabela de análise de risco FRAAP. O FRAAP é uma metodologia formal para a avaliação de risco que é conduzida pelo proprietário (PELTIER, 2002, p. 134).

5 RESULTADOS E DISCUSSÃO

A amostra desde pesquisa foi de 7 profissionais, sendo 1 diretor, 2 advogados, 1 assistente jurídica, 1 arquivista, 1 gerente e 1 estagiário, que trabalham diretamente com a informação da empresa. A amostra representa vários setores da organização sendo essencial para atingir, através da aplicação do questionário, alguns dos nossos objetivos.

Quadro 02. Distribuição dos participantes segundo os identificadores utilizados na pesquisa, no período de novembro de 2011, em um escritório de advocacia na cidade de João Pessoa-PB.

Elemento A	**Elemento B**	**Elemento C**
Elemento D	Elemento E	Elemento F
Elemento G	-	-

Fonte: Dados da pesquisa (2011)

A pesquisa não tem a intenção de expor a imagem dos funcionários da organização, logo esses nomes foram sugeridos apenas como meio de manter a privacidade dos participantes do questionário, já que se trata de uma empresa privada e se fosse o contrário poderíamos não alcançar o objetivo desejado.

Gráfico 01. Distribuição dos participantes segundo o sexo, no período de novembro de 2011, em um escritório de advocacia na cidade de João Pessoa- PB.

Fonte: Dados da pesquisa (2011)

Referente aos 7 (sete) participantes que obedeceram aos critérios de inclusão, notou-se que a diferença é pequena entre os sexo, sendo o feminino predominante.

Gráfico 02. Distribuição dos participantes segundo a profissão, no período de novembro de 2011 em um escritório de advocacia, na cidade de João Pessoa-PB.

Fonte: Dados da pesquiso (2011)

Pode-se observar que a amostra que predomina são advogados. Os advogados trabalham tanto com o recebimento de informações quanto com a produção delas, além de ser, o seu conhecimento em termos de informação jurídica é significativamente maior, por tanto a opinião de pelo menos mais de um, foi tida importante. Apesar das outras funções serem também importantes na empresa, foi selecionado um, de cada uma das outras funções, por seu cotidiano ser muito semelhante aos outros e trabalharem com as mesmas informações. Esses profissionais estão ligados entre si por suas funções e pela informação abrangendo toda a organização. Por isso justifica-se o motivo pelo qual foram escolhidos

O questionário é composto de 15 questões, onde duas são complementares. Foi analisado e tirada algumas conclusões sobre três pontos que as perguntas foram baseadas, tais quais: Procedimento de segurança, gestão de segurança e política de segurança. Com a observação demonstrada através da análise de risco verificamos o processo de gestão da empresa. Sendo eles: Cumprimento dos prazos, processo de digitalização, consulta processual, empréstimo de documentos, cadastro de processo e seu acompanhamento eletrônico, protocolo eletrônico, integral, via sedex e via fax, agendamento de audiência, atendimento ao cliente (reuniões, informar a respeito de audiência, acompanhar o mesmo em audiências), atividades financeiras, tais como:

pagamentos, transferências, prestação de contas, contratos de prestação de serviços (informática, telefonia e internet) e diligências como: xerografar processos nos fóruns e tribunais e analisar, enviar relatórios aos clientes. Destes foram selecionados, para análise de risco, três atividades: Digitalização. Tabela de Prazos e Acompanhamento Processual. Com a observação destas atividades foi possível analisar os riscos provocados por possíveis ameaças e vulnerabilidades existentes, avaliar os possíveis impactos provocados à segurança da informação e identificar medidas para minimizar esses riscos. Satisfazendo os nossos objetivos. Abaixo segue o quadro dos dados coletados no questionário.

Quadro 03: Dados coletados através da aplicação do questionário a 7 (sete) funcionários de um escritório de advocacia, situado na cidade de João Pessoa – PB.

Meio Físico/ Lógico	**Perguntas**	**Fonte da Pergunta**	**Dados coletados**
Procedimentos de Segurança	1. A internet é aberta a todos os funcionários para acessar todo tipo de site?	TCU (2003, p. 11)	3 responderam “sim”
			1 respondeu “Não”
			3 responderam “Em alguns computadores o acesso é livre”
	2. Quais sites você costuma acessar diariamente?	TCU (2003, p. 11)	1 respondeu “sites de notícias em geral”
			1 respondeu “sites de redes sociais”
			1 respondeu “apenas referente ao trabalho”
			4 responderam “todo tipo de site”
	3. Seu acesso a rede da empresa é ilimitado?	TCU (2003, p. 11)	4 responderam “sim”
			3 responderam “não”
	4. Com que freqüência	Silva, Carvalho e	5 responderam “raramente”

	você baixa programas para uso pessoal?	Torres (2003, p.100)	2 responderam “nunca”
	5. Com que freqüência você baixa arquivos como música, vídeos entre outros?	Silva, Carvalho e torres (2003, p.100)	4 responderam “raramente”
			1 respondeu “sempre”
			2 respondeu “nunca”
	6. Existem meios para tentar minimizar os riscos à segurança da informação na sua empresa?	TCU (2003, p.35)	7 respostas positivas. As quais se referiram aos itens: • Antivírus • Backups
	7. Qual critério usado para estabelecer a criação de senha do seu login	TCU (2003, p. 15)	1 respondeu “A senha segue a política de segurança da empresa”
			6 responderam “a senha deve conter letras, números e símbolos”
	8. De quanto em quanto tempo sua senha é atualizada?	Laureano (2005, p.45)	1 respondeu “a cada um ano”
			4 respondeu “a cada um mês”
			1 respondeu “minha senha é a mesma desde que entrei na empresa”
			1 respondeu “só quando ela apresenta algum tipo de problema”
G e st ã	9. (...) Em que categoria	Araújo (2009,	3 responderam “interna”

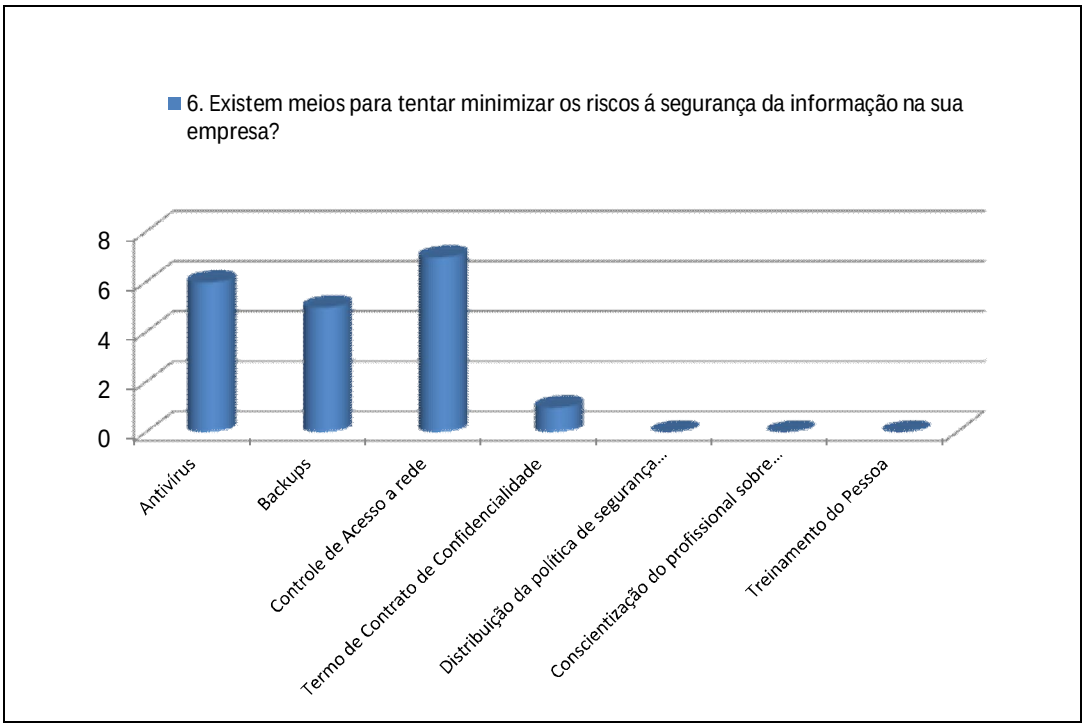
	você classifica as informações da sua empresa?	p. 230) Laureano (2005, p. 5)	4 responderam “confidencial”
	10. Essas informações se encontram em meio:	Silva, Carvalho e Torres (2003, p.80)	7 responderam que as informações se encontram tanto em meio físico como eletrônico.
	11. Com que freqüência você perde arquivos causado por vírus?	TCU (2003, p. 12)	4 responderam “raramente”
			3 responderam “nunca perdi arquivo causados por vírus”
Política de Segurança	12. Ao ser contratado (a), recebeu algum tipo de orientação a respeito dos procedimentos da segurança da informação na empresa?	Araújo (2009, p. 230)	6 responderam “ não” 1 responderam “sim”
	13. A empresa dispõe de uma política de segurança?	Araújo (2009, p. 230) Laureano (2005, p. 56)	4 responderam “sim, mas nunca tive acesso”
			1 respondeu “sim e tive acesso”
			2 responderam “não tenho conhecimento da existência”

Fonte: Dados da pesquisa (2011)

Selecionamos algumas perguntas consideradas importantes para representar graficamente seus resultados e com isso resumir os três pontos analisados, sendo estes procedimentos de segurança, política de segurança e gestão da informação.

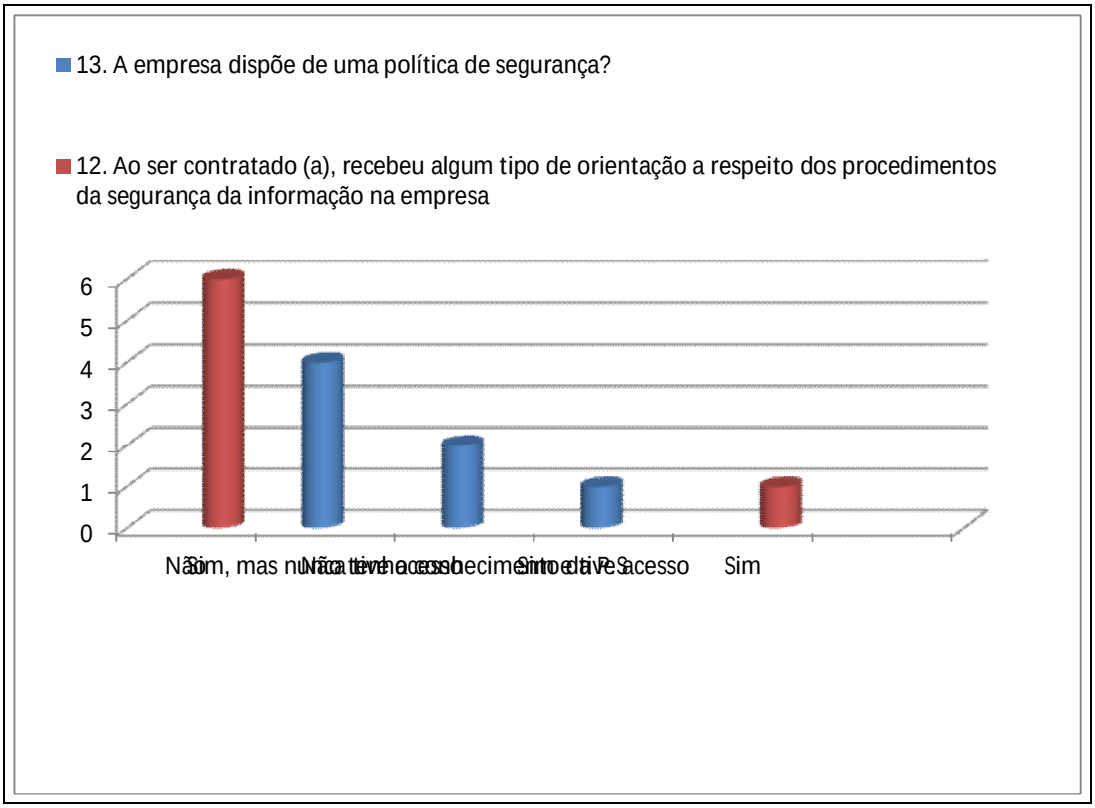
Nos procedimentos de segurança, observa-se que a administração aplica alguns métodos de segurança, mas esses métodos não são válidos para todos os usuários, pois foi identificado que em alguns computadores, o acesso a internet é ilimitado assim como na rede, colocando em risco as informações armazenadas nas pastas pertencentes à diretoria, onde deveria ser restrito. Como procedimentos de segurança foram identificados o uso principlamente de antivírus e backups.

Gráfico 03. Procedimento de Segurança segundo o questionário:



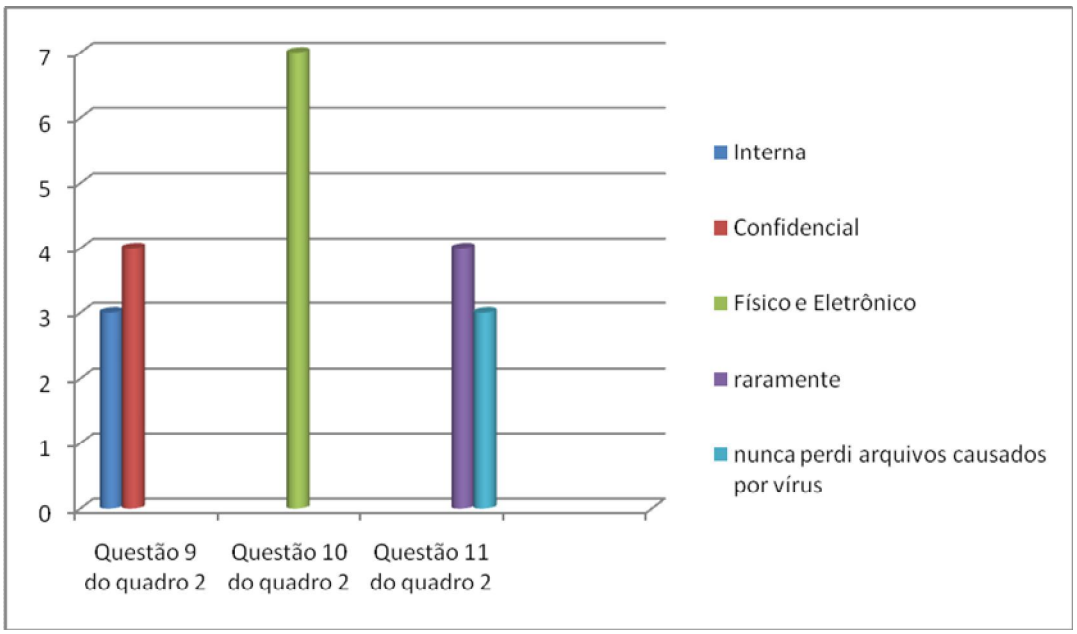
No que se refere à política de segurança observa-se que existe uma política de segurança, no entanto a maior parte dos funcionários não tem acesso ou desconhecem a existência da mesma. Desta forma, cabe a gestão da empresa disponibilizar essa política em meio físico ou eletrônico. As normas de segurança devem ser passadas para todos que estão entrando na empresa e é importante o contrato de confidencialidade, já que a empresa contrata os serviços de estagiários, sendo estes, considerados pessoal temporário.

Gráfico 04. Política de Segurança da Empresa:



Na gestão da informação, foi possível identificar que o tipo de informação produzida e armazenada na empresa é de caráter interno e confidencial. Desta forma requer cuidados e atenção para manter sua integridade, confidencialidade e disponibilidade. Ressalto que a informação de caráter confidencial, se não bem administrada, pode causar danos a organização levando a prejuízos. Apesar de a empresa fazer uso de antivírus e backups, houve casos perda de arquivos por ameaças de vírus. Isso leva a crer que existem portas vulneráveis para o ataque de vírus, provavelmente conseqüência do livre acesso à internet ou ainda proveniente da não atualização da política de segurança.

Gráfico 05. Processo de Gestão da Informação:



Nossa pesquisa também se deu pela análise de risco em três atividades através da verificação do processo de gestão do escritório. São elas: Digitalização, Tabela de Prazos, Acompanhamento Processual.

A análise de risco dessas três atividades se deu pelo método da observação, onde foi possível fazer um levantamento de suas ameaças, riscos, impacto e indicar medidas para a minimização o impacto do risco identificado. A elaboração da tabela de análise de risco foi baseada no modelo FRAP (Processo facilitado da análise e da avaliação de risco) de Peltier (2002, p. 129).

> Entre os diferentes métodos para análise de risco apresentados na literatura estudada, o FRAP foi selecionado devido aos seus resultados e forma de aplicação, por ser apontado como um dos mais populares e eficientes para implementação de análise de risco (FREIRE, 2003a apud ARAÚJO, 2009, p.127).

O FRAAP é uma metodologia formal desenvolvida com a compreensão dos processos qualitativos previamente desenvolvidos da avaliação de risco e a alteração deles para cumprir exigências atuais (PELTIER, 2002, p. 132, tradução nossa).

Observando cada uma das três atividades selecionadas, concluímos que:

• **Digitalização**: A justiça do trabalho permite fazer protocolo de petições apenas por meio eletrônico e para isso tanto a petição quanto a documentação devem está em meio

eletrônico e em formato PDF tornando possível apenas por meio de digitalização. É através da digitalização que se alimenta o arquivo digital, onde evita a consulta ao documento físico, livrando-o de perdas ou ameaça a sua integridade.

• **Tabela de prazos:** A tabela de prazo é acessada diariamente para a realização dos prazos publicados nos diários da justiça do trabalho, justiça comum e justiça federal. Essa tabela é alimentada e consultada pela rede da empresa. No caso de problemas na rede, os advogados responsáveis pelos prazos não terão acesso a essa tabela, podendo perder o prazo causando graves prejuízos para empresa.

• **Acompanhamento processual:** O acompanhamento é muitas vezes, feito por recebimento de e-mails com notificação, citação, intimação, etc, além das consultas aos diários da justiça. Nesse aspecto encontramos algumas vulnerabilidades, como problemas no e-mail. Essas notificações na maioria das vezes, refere-se a marcação de prazos e audiências. A perda de um prazo ou o não comparecimento em uma audiência pode resultar em revelia, desta forma não recebimento dessas informações pode gerar prejuízos de caráter financeiro para a empresa.

Foi consultado um advogado para que pudéssemos fazer a classificação do risco. O advogado tem maior conhecimento em termos das informações da empresa, porque é com essa informação que ele consegue concluir suas atividades e obter lucros para a organização. Portanto ele sabe o impacto que seria em cada ameaça detectada.

Tabela 02: Visão geral da análise de risco de três atividades selecionadas

Processo	Ameaça	Risco	Impacto	Medida
Digitalização	• Quebra de um equipamento	Baixo	• Não envio de documentos digitalizados • Indisponibilidade de acesso as pastas de Consulta processual	• Manter um contrato de manutenção X horas de atendimento. • Comprar um equipamento sobressalente
	• Livre acesso	Alto	• Perda total do arquivo digital	• Limitar o acesso, colocar senha em caso de tentativa de exclusão de arquivo

Tabela de Prazos	Queda de rede Acesso livre	Alto	• Perda de prazo • Não controle de prazos •Perda da causa por revelia • Prejuízo financeiro	• Manter em controle físico (agenda de prazos) • Salvar no computador diariamente • Solicitar o serviço de informática o bloqueio e acesso apenas para o computador responsável para o controle
Acompanhamento processual	Não recebimento de citação via e-mail, fax por problemas técnicos Não recebimento das intimações via e-mail, fax por problemas técnicos	Alto	• Perda de prazo • Perda da causa por revelia • Perda de cliente • Prejuízo financeiro	• Fazer uma limpeza no e-mail para evitar que não exceda o limite • Serviço de manutenção mensal do aparelho de fax

Os resultados apresentados revelaram que apesar da empresa investir em tecnologia da informação, não segue as normas de segurança como deveria. A administração afirma ter em meio eletrônico uma política de segurança, mas não permitiu o acesso, no entanto essa política precisa ser atualizada para encontrar os pontos francos. É interessante que a gestão faça cheque list para analisar o que precisa ser ajustado. A empresa é consciente do valor da informação e investe em meios para protegê-la, mas ressaltando o que foi dito antes, só precisa que a gestão analise se os métodos aplicados há 20 anos ainda se aplicam para os dias de hoje.

6 CONSIDERAÇÕES FINAIS

Em uma sociedade onde a tecnologia da informação ainda não foi bem adaptada no sentido de domínio das ferramentas oferecida pela TI, saem à frente aquelas empresas que disponibiliza maior segurança para o cliente. A informação ganhou nos últimos anos um valor inestimável em todos os sentidos. Desde o crescimento econômico financeiro de uma empresa até transformação de uma sociedade, quem a tem e a organiza de maneira segura e adequada, automaticamente adquire vantagens sobre as demais, encontrando-se mais preparado para qualquer tomada de decisão necessária.

Essa idéia favorece a ambos os lados, ou seja, tanto o cliente é beneficiado, quanto a empresa fornecedora do serviço. Desta forma, considera-se que os objetivos propostos neste trabalho foram alcançados, de maneira que tivemos conhecimento a respeito da gestão da segurança da informação no escritório de advocacia pesquisado, deixando a idéia para novas pesquisas.

Sintetizando o que foi apresentado neste trabalho, entende-se que:

a) Verificamos o processo de gestão da empresa. Considerando que o escritório investe em tecnologia da informação como, arquivo digital programa laserfiche de digitalização que pode ser acessado para consulta evitando o empréstimo de pastas desnecessário. Disponibiliza de um arquivo deslizante dividido em duas áreas, cível e trabalhista, onde apenas três pessoas têm acesso a chave deste arquivo, sendo estas uma arquivista e duas assistentes jurídicas correspondente ao setor cível e trabalhista.
b) Identificamos os procedimentos de segurança da informação implantados. Onde maior parte das informações produzidas pela organização é de caráter confidencial e interno, ou seja, algumas informações se acessadas sem autorização podem causar prejuízo a empresa. A maioria dos profissionais não tem acesso a política de segurança da informação, outros não tinham conhecimento, apesar da empresa ter em seus arquivos as normas e procedimentos de segurança.
c) Analisamos, através da análise de risco, os riscos provocados por possíveis ameaças e vulnerabilidades. Onde as três atividades analisadas apresentaram algum tipo de vulnerabilidade.

d) Avaliamos os possíveis impactos das ameaças identificadas. Tendo em vista que esses impactos gerariam perdas financeiras o que requer medidas urgentes de prevenção.
e) Indicamos medidas para minimizar o impacto das ameaças encontradas ou deixá-las a um nível aceitável. Trata-se basicamente de medidas simples, na maioria de baixo custo para a organização.

Diante dos objetivos alcançados, concluímos que a gestão precisa conscientizar-se da informação contida na empresa. Apesar dos funcionários classificarem as informações como interna e confidencial, não existe critérios para tal, nem métodos de classificação. Nota-se que os problemas apresentados são basicamente provenientes da má administração de segurança da informação. Com isso foram indicadas algumas medidas que podem ajudar a minimizar os riscos. Além das medidas de minimização dos riscos apresentadas no quadro 02 correspondente ao questionário e na tabela 02 correspondente a análise de risco, acrescentamos ainda a divulgação da política de segurança a todos os funcionários, sejam eles temporários ou não, a implementação de método de classificação das informações e contrato de confidencialidade.

Concluímos a pesquisa deixando em aberto para novos estudos, afins acrescentar à literatura novas perspectivas, e ás empresas, maior conscientização sobre o assunto aqui apresentado.

7 REFERÊNCIAS

ALMEIDA, M. L. P. Tipos de pesquisa. In: ALMEIDA, Maria Lúcia Pacheco de. **Como elaborar monografias.** 4. ed. rev. e atual. Belém: Cejup, 1996. Cap. 4, p. 101-110.

AMARAL, Sueli Angélica do. **Marketing e desafio profissional em unidades de informação**. Ci. Inf., Brasília, v. 5, n. 3, 1996.

ARAÚJO, Aneide Oliveira; OLIVEIRA, Marcelle Colares. **Tipos de pesquisa.** Trabalho de conclusão da disciplina Metodologia de Pesquisa Aplicada a Contabilidade - Departamento de Controladoria e Contabilidade da USP. São Paulo, 1997.

ARAÚJO, Wagner Junqueira de. **A Segurança do Conhecimento nas Práticas da Gestão de Segurança da Informação e da Gestão do Conhecimento.** Tese (Doutorado em Ciência da informação) – Universidade de Brasília, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB 17799**: Tecnologia da informação: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NRB 27001**: Tecnologia da informação, técnicas de segurança, sistemas de gestão de segurança da informação, requisitos. Rio de Janeiro, 2006.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. Institui a política de segurança da informação nos órgãos e entidades da Administração Pública Federal, e dá outras providências. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 14 jun. 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em 20 mar. 2008.

BRASIL. Tribunal de Contas da União. **Boas práticas em segurança da informação**. Brasília: TCU, Secretaria Adjunta de Fiscalização, 2003.

CARMO, H.; FERREIRA, M.M. **Metodologia da investigação. Guia para Auto-aprendizagem.** 1.ª ed., Lisboa: Universidade Aberta, 1998. ISBN 972- 674-231-5. 353p.

CERVO, A.L. BERVIAN, P. A. **Metodologia científica**. São Paulo: Makron Books, 1996.

FORTIN, M. **O Processo de Investigação: Da Concepção à Realização.** 3.ª ed. Loures, Lusociência: 2003.

GIL, ANTONIO CARLOS. **Como Elaborar Projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação.** 2005. 02. Disponível em: http://www.ppgia.pucpr.br/~laureano/guias/GuiaFirewallIptables.htm. Acessado em: 24/09/2004.

MALHOTRA, NARESH K**. Pesquisa de marketing: uma orientação aplicada.** 3. .ed. Porto Alegre: Bookman, 2001.

MARCONI, Marina de Andrade, LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica.** 7. ed. São Paulo: Atlas, 2010.

MARCIANO, João Luis; MARQUES, Mamede Lima. **O enfoque social da segurança da informação.** Ci. Inf., Brasília, v. 35, n. 3, p. 89-98. 2006.

PARRA FILHO, Domingos, SANTOS, João Almeida. **Metodologia Científica.** 2. Ed. São Paulo: Futura, 1998.

PELTIER, Thomas R. **Information security policies, procedures, and standards.** USA: CRC Press, 2002.

SERPRO. **Curso de Introdução à segurança da informação.** Ministério da Fazenda. 2007.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. **Segurança dos Sistemas de Informação: Gestão Estratégica da Segurança Empresarial.** Lisboa, 2003.

WERTHEIN, Jorge. **A sociedade da informação e seus desafios.** Ci. Inf., Brasília, v.29, n.2, p. 71-77. 2000.

APÊNDICES

APÊNDICE A

Instrumento para Coleta de Dados

QUESTIONÁRIO

Sexo:
Idade :
Função na empresa :
Tempo de trabalho :

• **Informação Pública**: São aquelas que não necessitam de sigilo algum, podendo ter livre acesso para os colaboradores. Não há necessidade de investimentos em recursos de proteção. São informações que, se forem divulgadas fora da organização, não trarão impactos para os negócios.

• **Informação interna**: O acesso às informações deve ser evitado. Entretanto, se esses dados tornarem-se públicos, as conseqüências não serão críticas. A integridade dos dados é vital.

• **Informação confidencial:** As informações desta classe devem ser confidenciais dentro da organização e protegidas do acesso externo. Se alguns desses dados forem acessados por pessoas não autorizadas, as operações podem ser comprometidas, causando perdas financeiras e de competitividade.

1. Baseado na classificação das informações no quadro acima, em que categoria você classifica as informações na sua empresa:

   ( ) Pública

   ( ) Interna

   ( ) Confidencial

2. Essas informações se encontram em meio:

   ( ) Eletrônico ( ) Físico ( ) Ambos

3. Ao ser contratado (a) recebeu algum tipo de orientação a respeito dos procedimentos da segurança da informação na empresa?

   ( ) Sim ( ) Não

4. A empresa dispõe de uma política de segurança?

   ( ) Sim, mas nunca tive acesso

( ) Sim e tive acesso

( ) Não tenho conhecimento da existência

( ) Não

5. Se você respondeu “sim e tive acesso”, em suporte se encontra essa política?

   ( ) papel ( ) meio eletrônico ( ) tanto em papel, quanto eletrônico

6. Existem meios para tentar minimizar os riscos á segurança da informação na sua empresa?

   ( ) Sim

      Qual?

      ( ) Antivírus

      ( ) Treinamento do pessoal

      ( ) Termo de contrato de confidencialidade

      ( ) Distribuição da política de segurança da empresa

      ( ) Conscientização do profissional sobre segurança da informação

      ( ) Os usuários têm acesso limitado a rede

      ( ) Backups

   ( ) Não tenho conhecimento de nenhum desse itens citados acima

7. A internet é aberta a todos os funcionários para acessar todo tipo de site?

   ( ) Sim ( ) Não ( ) Em alguns computadores o acesso é livre

8. Em caso negativo, você já observou se em alguns computadores o acesso é livre?

   ( ) Sim

   ( ) Não

9. Com que freqüência você baixa programa para uso pessoal?

   ( ) Sempre ( ) raramente ( ) quase nunca ( ) nunca

10. Com que freqüência você baixa arquivos como música, vídeos entre outros?

( ) Sempre ( ) raramente ( ) quase nunca ( ) nunca

11. Quais sites você costuma acessar diariamente?

( ) Sites de Notícias em geral

( ) Sites de redes sociais

( ) Apenas referente ao trabalho (TRT, TJ, JF, CORREIOS, ETC)

( ) Todo tipo de site

12. Seu acesso a rede da empresa é ilimitado?

( ) Sim

Por quê?

_____
_____
_____
___

( ) Não

Por quê?

_____
_____
_____
___

13. Qual critério usado para estabelecer a criação de senha do seu login?

( ) Não existem critérios

( ) Não tenho login

( ) A senha segue a política de segurança da empresa

( ) A senha deve conter letras, números e símbolos

14. De quanto em quanto tempo sua senha é mudada?

( ) a cada um 1 ano

( ) a cada mês

( ) Minha senha é a mesma desde que entrei na empresa

( ) Só quando ela apresenta algum tipo de problema

( ) Não tenho senha

15. Com que freqüência você perde arquivos causado por vírus?

( ) sempre

( ) quase sempre

( ) raramente

( ) Nunca perdi arquivo causado por vírus

ANEXOS

ANEXO A

UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE CIÊNCIA DA INFORMAÇÃO

TERMO DE CONSENTIMENTO

Ao Diretor do Escritório de Advocacia Nóbrega Farias e Trajano Advogados Associados
Dr. Carlos Frederico Nóbrega Farias,

Para efeito de capacitação universitária, em atividades de Estágio Supervisionado I, e tendo em vista o cumprimento dos critérios estabelecidos para atribuição de nota, peço a V.Sa. o consentimento para a realização da pesquisa intitulada **"GESTÃO DA SEGURANÇA DA INFORMAÇÃO: ESTUDO DE CASO APLICADO A UM ESCRITÓRIO DE ADVOCACIA"**, cujo objetivo é analisar a gestão de segurança da informação em um escritório de advocacia.Tal pesquisa fará parte do Projeto de Trabalho de Conclusão de Curso, da aluna Geniele Trajano da Silva, graduanda em Biblioteconomia pela Universidade Federal da Paraíba – UFPB, sob a orientação da Prof. Dr.Wagner Junqueira de Araújo.

Solicito ainda a permissão para divulgação desta pesquisa em eventos e revistas científicas com garantia do anonimato e o acesso livre a quaisquer informações relativas ao trabalho.

Atenciosamente,

Geniele Trajano da Silva

_____

João Pessoa ___ de _____ de 2011.

_____ _____
Wagner Junqueira de Araújo Geniele Trajano da Silva
PESQUISADOR RESPONSÁVEL PESQUISADORA PARTICIPANTE

Autorizo a realização da pesquisa

_____