UNIVERSIDADE FEDERAL DE MINAS GERAIS
ESCOLA DE CIÊNCIA DA INFORMAÇÃO

BERNARDO MARTINS HORTA

SEGURANÇA DA INFORMAÇÃO
VAZAMENTO DE INFORMAÇÕES - CONSCIENTIZAÇÃO OU PRIVAÇÃO?

Belo Horizonte
2014

BERNARDO MARTINS HORTA

SEGURANÇA DA INFORMAÇÃO
VAZAMENTO DE INFORMAÇÕES - CONSCIENTIZAÇÃO OU PRIVAÇÃO?

Monografia apresentada ao programa de Especialização do **Núcleo de Informação Tecnológica e Gerencial – NITEG**, no curso Gestão Estratégica da Informação, da **Escola de Ciência da Informação**, da Universidade Federal de Minas Gerais, como requisito para a obtenção do certificado de **Especialista em Gestão Estratégica da Informação**.

Orientador: **Prof. Dr. Jorge Tadeu de Ramos Neves**

BELO HORIZONTE

2014

Universidade Federal de Minas Gerais
Escola de Ciência da Informação
Programa de Pós-Graduação em Ciência da Informação

Trabalho de Conclusão de Curso de Especialização em Gestão Estratégica da Informação, intitulado **Segurança da Informação. Vazamento de Informações: Conscientização ou privação?** de autoria de **Bernardo Martins Horta**, aprovada pela banca examinadora constituída pelos seguintes professores:

_____
Prof. Dr. ***
instituição

_____
Prof. Dr. ***
instituição

_____
Prof. Dr. ***
instituição

_____
Prof. Dr. ***
instituição

_____
Prof. *** Nome do Coordenador(a) ***
Coordenador(a) do Núcleo de Informação Tecnológica e Gerencial – NITEG
ECI/UFMG

Data de aprovação: Belo Horizonte, de ..... de 20....

DEDICATÓRIA

A minha esposa e enteado que além de serem minha inspiração e combustível para continuar perseguindo os meus sonhos, tiveram a paciência e compreensão em aceitar a divisão do nosso tempo na consecução deste trabalho. A vocês todo o meu carinho e eterno agradecimento.

AGRADECIMENTOS

Ao meu orientador que forneceu o caminho para a realização deste trabalho.
Aos entrevistados que participaram deste estudo, sem os quais esse trabalho não teria sido possível.
A minha adorável esposa que ajudou ativamente na revisão deste trabalho.

A todos que, de alguma forma, contribuíram para esta construção.

“Segurança da informação se faz com tecnologia, processos e pessoas, e a formação destas exige mais que uma sequência de treinamentos. Porque você treina macacos, pessoas você educa!”

Roberto Cunha

RESUMO

O presente trabalho trata do tema o vazamento de informações corporativas e procura responder qual o principal motivador para a ocorrência de vazamento de informações sensíveis nas empresas, problema esse que tem se consolidado como uma das principais ameaças à segurança da informação nas organizações. Com isso se pretende discutir quais os principais desafios das empresas no combate ao vazamento de informações e traçar um plano de ação para efetiva conscientização dos usuários no tratamento das informações e criação de um comportamento seguro. Para esse desenvolvimento utilizou-se do levantamento bibliográfico, além da realização de estudos de campo que pautaram os resultados obtidos. Inicialmente a pesquisa aborda a contextualização do tema visando demonstrar a relação entre o desenvolvimento da sociedade da informação, a evolução da tecnologia, as implicações do cotidiano das empresas e mais especificamente dos fatores que mantêm relação com o vazamento de informações nas organizações. Por fim, o trabalho apresenta alternativas para mitigar o problema de vazamento de informações nas organizações, que foi respaldada por um questionário referente ao tema realizada com profissionais do mercado de trabalho que demonstrou como é visto o vazamento de informações em empresas brasileiras e por consequente buscou justificar as principais afirmações e conclusões apresentadas no decorrer do presente estudo. Em certos casos, evitar o vazamento de informações vem com a execução de um conjunto de ações que passam por melhorias nos processos, introdução de tecnologias de prevenção e mais do que nunca a implementação de programas de conscientização constantes, pois por mais automatizados que estejam os processos e tecnologias, sempre existirá o elemento humano, ou seja, pessoas usando, manipulando e até mesmo vazando as informações corporativas, de forma intencional ou não.

Palavras-chave: Segurança da Informação. Vazamento de Informações. Segurança da Informação.

ABSTRACT

This work deals with corporative information leakage, and was prepared to respond to the main motivator to combat the sensitive information leakage in companies, a problem that has been consolidating as one of the principal threats to the information security of organizations. With this we would like to discuss the main challenges companies face in combating information leakage and to create an action plan to make the users aware of how to treat the information, creating a secure behavior. To develop this, a bibliographic study was used, based on materials previously elaborated in the area, as well as surveys in the field which confirmed the obtained results. Initially the study addresses the contextualization of the theme aiming to demonstrate the relation between the information society development, the evolution of technology, the company's day to day implications and more specifically those factors that maintain a relation with the information leakage in the organizations. Lastly, this work presents alternatives to mitigate the organization's information leakage problems, which were backed up by a field survey that demonstrated how information leakage is viewed in Brazilian companies and, consequently, seeks justify the main affirmations and conclusions presented throughout this survey. In certain cases, avoiding information leakage is connected to a series of actions that include process improvements, introduction of prevention technologies and, more than ever, the implementation of constant awareness training programs. This is because, even with more automatic processes and technologies, the human element will always be a risk factor, that is to say, people will be using, manipulating and even leaking corporate information, be it intentionally or not.

Keywords: Information Security. Information Leakage. Information security policies.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

SUMÁRIO

1 Introdução

Nesta década de 2010, vive-se em um modelo de sociedade do conhecimento onde a informação é considerada um ativo de enorme valor, e nessa época realmente singular em termos de conhecimento e de avanços tecnológicos, a geração e o compartilhamento de informações tornaram parte integrante e indispensável em nossas vidas. Essa geração e compartilhamento de informações que pode ser considerada fator determinante para o sucesso de uma empresa, pode também levá-la ao fracasso caso medidas de proteções não sejam lembradas e implantadas (SILVA, 2012).

Para Ramos (2006) e SILVA (2012), não é de hoje que a informação é considerada um ativo de enorme valor para as empresas; contudo, no passado, quando a informação era em grande parte utilizada através de seu meio convencional, ou seja, em papel, era possível armazená-la e protegê-la de maneira mais eficiente, já que um simples envelope, gaveta, armário ou cofre eram utilizados para armazenar aquelas informações mais sensíveis contra acessos indevidos; entretanto essa prática não é mais aplicável nos dias de hoje visto que vive-se a fase da sociedade do conhecimento, na qual o conceito de “Big Data”, que são enormes quantidades de informações variadas, trafegando em alta velocidade em meio eletrônico, e armazenadas nos mais diferentes tipos de dispositivos, sejam eles computadores, laptops, HD externos*, pen drives*, bancos de dados locais ou na nuvem, *storages*, torna a tarefa de classificar a informação e protegê-la quase impossível.

Atualmente o número de negócios gerados, tendo como suporte o uso de ferramentas como a internet e os sistemas de TI vem aumentando de modo significativo, e com isso os riscos inerentes à utilização desse meio de suporte tornam-se mais evidentes e significativos. Violações ou falhas na segurança dos sistemas de informação podem causar diversos riscos à empresa, e consequentemente ao negócio, trazendo danos à reputação e imagem da organização causada por roubo de identidade, vazamento de informações confidenciais em função de falhas de sistemas e multas por questões regulatórias não atendidas.

As grandes transformações que aconteceram em meio ao surgimento e constante atualização da internet e da globalização, afetaram em cheio as organizações, quebrando diversos paradigmas e promovendo uma profunda reavaliação das prioridades daqueles que estão no comando.

Segundo Gomes e Braga (2006), numerosos problemas relacionados aos riscos as informações através de sua manipulação por meios tecnológicos se destacam, dentre eles:

a) Roubos de mídias de backup;

b) Processos litigiosos resultantes da produção e/ou preservação imprópria de registros eletrônicos;

c) Quebras de propriedades intelectuais;

d) Terrorismo;

e) Crimes eletrônicos;

f) Polêmicas em torno da legislação de direitos autorais e patentes;

g) Crescimento de programas maliciosos;

h) Fraudes financeiras;

i) Pirataria em geral;

j) Espionagem industrial;

k) Guerra cibernética.

Essas situações quando não previstas e tratadas como prioritárias, podem dar origem a uma série de problemas de segurança, acarretando grandes prejuízos financeiros às organizações.

Com o grande número de informações que são geradas em uma organização, o constante upgrade tecnológico e o vasto número de vulnerabilidades encontradas em seus sistemas de informação, podem ocorrer uma constante busca por métodos de proteção invioláveis, mesmo lembrando sempre que uma das premissas básicas da segurança da informação é o fato de que não existe segurança 100% (SÊMOLA, 2003a).

O que torna algo seguro está muito além da implantação de uma solução definitiva: na verdade, isso está relacionado com a gerência de uma série de fatores, como ativos, ameaças, vulnerabilidades, impactos, riscos e, principalmente, pessoas.

Na segurança da informação diversos domínios são considerados para a mitigação dos riscos, mas aquele que nos interessa neste momento para a solução de nosso problema é como tratar o vazamento de informações nas empresas, e principalmente em como preparar as pessoas para isso.

Resumidamente, Silva (2012) afirma que o vazamento de informações só ocorrerá se dois elementos estiverem presentes; o primeiro deles é o acesso à informação, pois um vazamento de informação intencional ou não só poderá ocorrer, se a pessoa que empreendeu essa ação tivesse acesso a ela. O segundo elemento é o meio ou recurso, pois uma informação só pode ser enviada para fora de seu local de origem e, consequentemente, acessada por uma pessoa não autorizada, se for utilizado um recurso, tecnológico ou não, para executar essa tarefa, seja um simples e-mail, um dispositivo de armazenamento móvel, ou então uma corriqueira conversa em local público. É importante destacar que esses

elementos não precisam estar presentes ao mesmo tempo para que o vazamento de informações aconteça, mas devem se fazer presentes em algum momento.

Conforme dito anteriormente, e segundo Silva (2012) e Dawel (2004), um vazamento de informações pode se dar de forma intencional ou não, podendo-se afirmar que na maioria das vezes ele é não intencional. Um vazamento intencional é caracterizado quando um determinado agente tem conhecimento de que uma determinada informação é restrita e mesmo assim ele tem a intenção de acessá-la, compartilhá-la e utilizá-la para outros fins. Em sua grande parte é realizada por funcionários, terceiros, prestadores de serviço ou parceiros de negócio. Já quando o vazamento ocorre de forma não intencional ele geralmente ocorre em decorrência de falha humana, falta de conscientização dos usuários, desconhecimento da classificação de uma informação, e/ou falha em um sistema de informação.

Dito isso, o que se pode constatar é que as empresas estão buscando implantar projetos de segurança da informação, mas quando uma empresa pensa em segurança da informação as primeiras ações que surgem são apenas para executar as diretrizes traçadas pela alta administração, através da implantação de mecanismos de proteção restritivos, em prazos cada vez mais curtos e buscando uma alta efetividade, porém esta estratégia afeta diretamente a forma de trabalhar dos usuários, reduzindo a colaboração, e consequentemente demanda uma mudança cultural repentina e na maioria das vezes bem dolorosa.

Dessa forma, o que se deve buscar é como chegar a um bom equilíbrio entre a conscientização dos usuários frente à Segurança da Informação e os mecanismos de proteção restritivos, o que será tema desse trabalho.

1.1 Justificativas

Na sociedade do conhecimento a informação é considerada um ativo de enorme valor e a geração e o compartilhamento de informações se tornou parte integrante e indispensável em nossas vidas. Essa geração e compartilhamento de informações, que podem ser considerados fatores determinantes para o sucesso de uma empresa, pode também levá-la ao fracasso caso medidas de proteções adequadas não sejam lembradas e implantadas.

Com esse trabalho busco identificar os motivos e encontrar os caminhos para combatê-lo e assim poder utilizar os resultados para tentar aplicar na empresa em que atuo. Além disso, esse trabalho irá ajudar a criar um argumento convincente que irá servir de apoio na replicação desse conhecimento.

1.2 Problema

Medidas de proteção à informação são caras e acima de tudo ineficientes se as pessoas não têm consciência de suas ações e tampouco do impacto que podem causar caso uma informação sigilosa seja tratada inadequadamente. O custo/beneficio envolvido na solução desse problema é alto e as empresas sempre esbarram no dilema da conscientização dos usuários em relação à segurança da informação e na aquisição e implantação de infinitas tecnologias de proteção baseadas em restrições que batem de frente com a colaboração da sociedade do conhecimento.

Dito isso, quais os principais motivadores e como eles se comportam para a ocorrência de vazamento de informações sensíveis nas empresas?

1.3 Objetivos

Este estudo propõe atender ao objetivo geral e aos objetivos específicos a seguir.

1.4 Objetivo geral

O presente trabalho pretende, através da identificação dos motivadores, analisar e discutir quais os principais desafios das empresas no combate ao vazamento de informações e traçar um plano de ação para efetiva conscientização dos usuários no tratamento das informações criando assim um comportamento seguro.

1.4.1 Objetivos específicos

- Contextualizar o tema da Segurança da Informação, através de levantamento teórico da área, dando ênfase ao tema ligado ao vazamento de informações.
- Identificar os principais motivadores dos problemas relacionados ao vazamento de informações nas empresas brasileiras.
- Promover uma pesquisa de campo, através de um questionário, visando compreender a visão dos usuários finais e das empresas em relação ao vazamento de informações.

- Analisar e traçar um plano de ação de como as organizações podem atuar frente a problemas de vazamento informacional envolvendo pessoas e como podem se prevenir em face de tais incidentes.

2 Revisão da literatura

5.1 A importância da Informação

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como resultado deste aumento da interconectvidade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (SILVA, 2012).

Para definir informação diversos autores buscam discernir os termos, dado, informação e conhecimento. Davenport e Prusak (1999) conceituam dados, informação e conhecimento (Figura 1); contudo, dão maior ênfase ao termo “informação” uma vez que é um termo que envolve todos os três, além de servir como conexão entre eles.

Dados	Informação	Conhecimento
Simples observações sobre o estado do mundo	Dados dotados de relevância e propósito	Informação valiosa da mente humana Inclui reflexão, síntese, contexto
Facilmente estruturado Facilmente obtido por máquinas Freqüentemente quantificado Facilmente transferível	Requer unidade de análise Exige consenso em relação ao significado Exige necessariamente a mediação humana	De difícil estruturação De difícil captura em máquinas Freqüentemente tácito De difícil transferência

Quadro 1 - Dados, informação e conhecimento.
Fonte: Davenport e Prusak (1999)

Observa-se que os conceitos apresentados convergem no sentido de caracterizar os dados como elemento bruto, que precisam da intervenção humana para transformar-se em informação. Ao contrário dos dados, apenas a informação e o conhecimento têm condições de interferir ou modificar o comportamento de uma organização.

É preciso entender as organizações como sistemas e a informação como um recurso útil que precisa ser administrado. A informação é um recurso que não se deteriora nem se deprecia e tem seu valor determinado exclusivamente pelo usuário sendo o único recurso que não se perde com o uso ou com a disseminação, apenas quando se torna obsoleta.

O propósito básico da informação é ser um facilitador para a tomada de decisão e levar a empresa a alcançar seus objetivos pelo uso eficiente dos recursos disponíveis, nos quais se inserem pessoas, processos, tecnologia, capital financeiro, além da própria informação.

Face aos desafios que as organizações enfrentam ao tratar suas informações sejam elas confidenciais ou não, torna-se fundamental não tão somente ao profissional da área de Tecnologia da Informação, mas também os demais usuários, que manipulam, armazenam ou a enviam, a serem orientados e conscientizados de forma a tratar as informações de maneira adequada e consequentemente segura.

Na época em que as informações eram armazenadas em papel, a segurança era relativamente simples. Com a utilização da internet e das tecnologias que sofrem mudanças a todo o momento, os aspectos de segurança atingiram tamanha complexidade, que há a necessidade do desenvolvimento de equipes cada vez mais especializadas, visando implementar e gerenciar estruturas de segurança cada vez mais sofisticadas e possuindo controles centralizados e integrados (SÊMOLA, 2003b).

5.2 Conceitos Gerais de Segurança da Informação

A informação pode ser obtida em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

> *Segundo NBR ISO/IEC 17799 (2005, p.9):*
>
> *Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio,*
>
> *e ainda complementa que:*
>
> *A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos,*

> *procedimentos, estruturas organizacionais e funções de software e hardware.*

Já Sêmola (2003a, p.43) 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.”

Segundo Ramos (2006), segurança é estar livre de perigos e incertezas. Dentro de uma organização, essa costuma se aplicar aos ativos, que é tudo aquilo que possui valor e consequentemente, demanda proteção.

Os ativos podem ser classificados e organizados através de diversas propriedades, como se pode observar nas Tabelas 1 e 2.

Categoria de Ativos	Exemplo
Tangíveis	Informações impressas ou digitais Impressoras Móveis de escritório
Intangíveis	Imagem de uma empresa Confiabilidade de um órgão federal Marca de um produto

Quadro 2 - Exemplo de classificação dos ativos.

Fonte: Ramos (2006)

Categoria de ativos	Exemplo
Lógicos	Dados armazenados em um servidor Sistema ERP Rede VoIP
Físicos	Estação de trabalho Sistema de ar-condicionado Data Center
Humano	Funcionários Terceiros

Quadro 3 - Exemplo de categorização dos ativos.
Fonte: Ramos (2006)

Esses ativos podem ser agrupados seguindo características semelhantes no que diz respeito às necessidades, estratégias e ferramentas de proteção. Diante dessa necessidade as organizações costumam possuir duas ou mais áreas que são responsáveis pela segurança, geralmente uma área de segurança física, responsável pela segurança patrimonial e outra área de segurança lógica, responsável pela segurança dos sistemas de Tecnologia da Informação.

Para assegurar que os ativos estejam em segurança, adotam-se medidas de proteção, que de acordo com Sêmola (2003a), são as práticas, procedimentos e mecanismos utilizados para a proteção da informação e seus ativos, que podem impedir a redução das vulnerabilidades, a limitação do impacto, o impedimento de que ameaças se concretizem ou a minimização do risco de qualquer outra forma.

As medidas de proteções também podem ser classificadas de acordo com suas características, como exemplo mostrado na Tabela 3.

Tipo de proteção	Exemplo
Lógica	Permissões em sistemas de arquivos Firewalls Perfis de usuários em aplicações
Física	Portas Fechaduras Guardas
Administrativa	Políticas Normas Procedimentos Treinamentos

Quadro 4 - Exemplo de classificação de proteções.
Fonte: Ramos (2006)

Outra maneira para se classificar as medidas de proteção é conforme sua ação. Essa medida de classificação se mostra bastante eficaz já que ela pode ser utilizada de

forma que as medidas se complementam, criando diversas camadas de proteção em cada ativo.

Tipo de Proteção	Descrição
Preventiva	Evita que incidentes ocorram
Desencorajadora	Desencoraja a prática de ações
Limitadora	Diminui danos causados
Monitoradora	Monitora o estado e funcionamento
Detectora	Detecta a ocorrência de incidentes
Reativa	Reage a determinados incidentes
Corretiva	Repara falhas existentes
Recuperadora	Repara danos causados por incidentes

Quadro 5 - Tipos de proteção

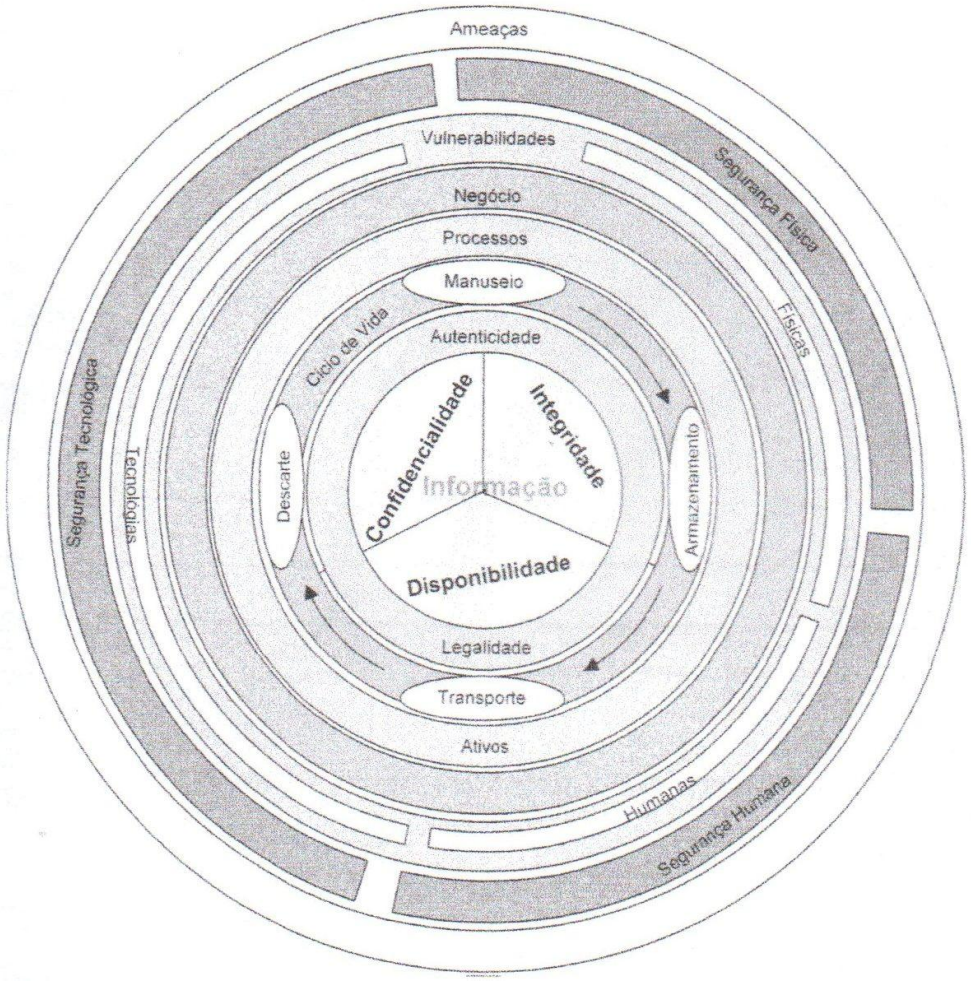
Fonte: Ramos (2006)

Certamente o grande segredo para obter o melhor retorno dos mecanismos de proteção está na segmentação inteligente dos ativos. Desta forma, é possível, aplicar os tipos de proteção adequados, em que cada um, oferecerá o nível dosado de proteção, sem que exceda os limites e não deixe de suprir às necessidades.

Segundo Sêmola (2003a), essa segmentação é conhecida como Teoria do Perímetro.

> *Além de um perímetro estar associado a compartimentalização de espaços físicos e lógicos, ele também cumpre um importante papel de alerta e de mecanismos de resistência distribuídos por áreas, a fim de permitir que tentativas de acessos indevidos e invasão gerem sinais de alerta e se deparem com a resistência que propiciará tempo para que medidas contingenciais sejam tomadas antes da ação avançar ainda mais em direção do alvo.*

Figura 1 - Visão condensada dos desafios (Teoria do Perímetro).



Fonte: Sêmola (2003a)

Diante dos conceitos apresentados pode-se entender melhor o que é segurança da informação e como ela pode ajudar a proteger os chamados ativos da informação, que geram, processam, manipulam, transmitem e armazenam informações.

Quando se fala de segurança da informação, devem-se considerar três pilares principais: confidencialidade, integridade e disponibilidade NBR ISO/IEC 17799 (2005).

A confidencialidade visa garantir que apenas as pessoas que devem ter conhecimento a respeito de uma informação possam acessá-la. Diferentes tipos de informação terão diferentes classificações em termos de confidencialidade, esse fator

depende do valor que esse ativo de informação traz a organização e ao impacto que ele pode causar se estiver acessível a pessoas não autorizadas.

Já a integridade visa manter a originalidade da informação, ou seja, proteger a informação contra alterações sejam elas intencionais ou acidentais.

A disponibilidade já visa manter uma informação acessível, para as pessoas que dela necessitem, no momento em que for necessário. A proteção da disponibilidade visa proteger a informação tanto em situações acidentais quanto intencionais.

Como já citado, uma premissa da segurança da informação é a de que não existe segurança 100%. Por mais medidas de proteção que utilizarmos e precauções que tomemos, jamais teremos como mitigar todas as possíveis situações de prejuízo. A razão para isso é muito simples, segurança tem um custo elevado e à medida que os investimentos vão crescendo, chegamos a um ponto onde o investimento realizado é maior que o valor do ativo protegido.

Dessa maneira, pode-se concluir que há uma série de fatores e componentes a serem gerenciados de forma a garantir que as seguranças dos ativos de informação se encontrem dentro de níveis adequados, e que os recursos gastos para atingir tais níveis sigam a premissa básica de relação custo/benefício.

A ISO/IEC GUIDE 73 (2002) define alguns componentes básicos que devem ser analisados para conseguir uma discrição financeira, são eles:

- Valor;
- Ameaça;
- Vulnerabilidade;
- Impacto;
- Risco.

Valor mostra a importância do ativo para a organização através de propriedades mensuráveis, como o seu valor financeiro, o lucro ou o custo de substituição, ou propriedades abstrata como o comprometimento da imagem de uma empresa.

Ameaça é todo evento potencial que possa comprometer os objetivos de uma organização.

Vulnerabilidade é a ausência de proteção ou a falha de uma proteção existente.

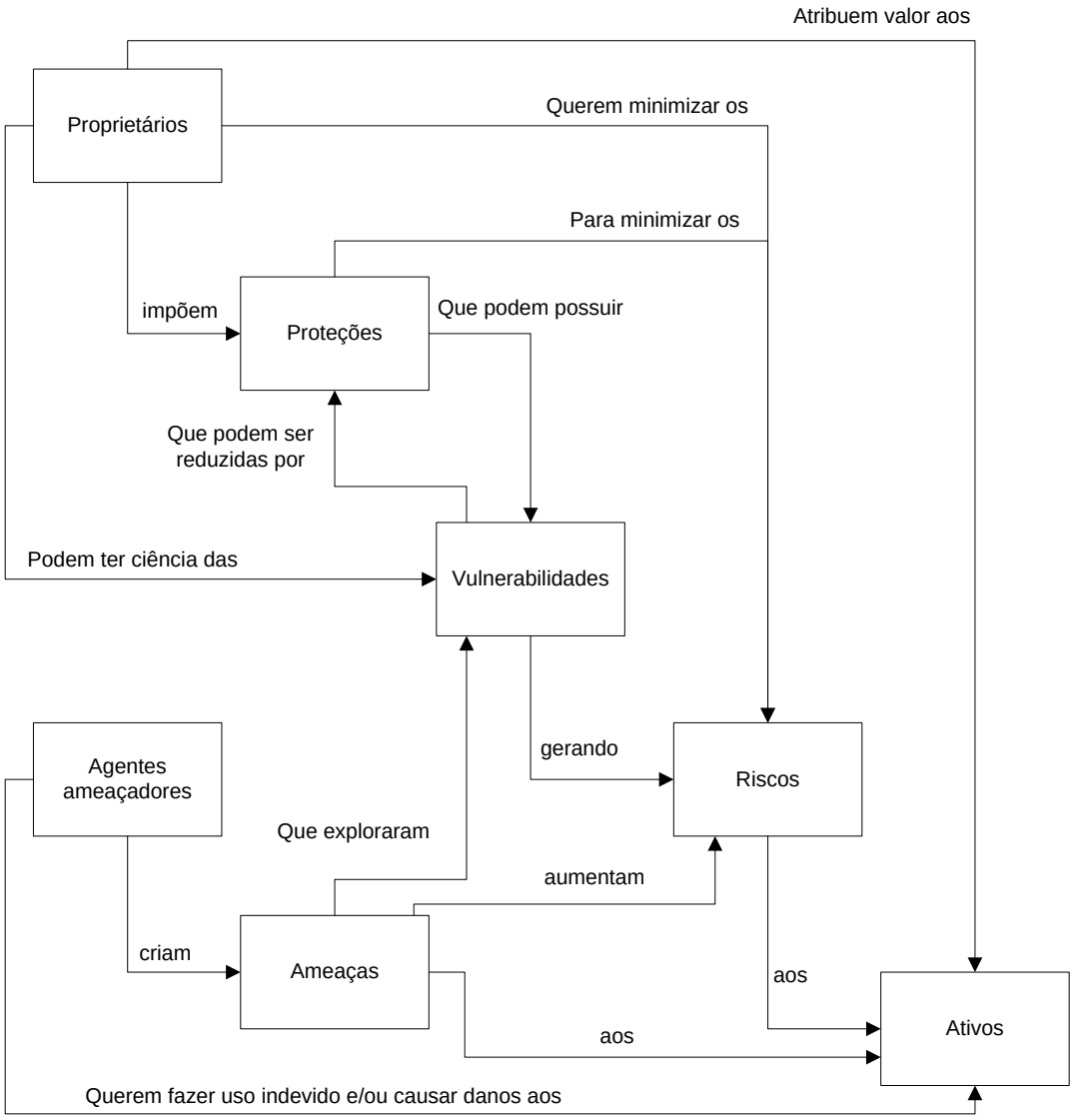
Impacto é a medida de prejuízo do ativo, seja ela tangível ou intangível.

Segundo Brasiliano (2003), quanto um risco pode causar de impacto financeiro em uma empresa é um dos problemas mais críticos que o gerenciador de riscos enfrenta.

Risco é a probabilidade de uma determinada ameaça se concretizar, combinada com o impacto que será causado, ou seja, quanto maior a probabilidade de uma ameaça ocorrer com um grande impacto, maior será o nível de risco.

Através de Ramos (2006), foi extraída uma Figura 2 que mostra como esses componentes interagem entre si.

Figura 2 - Interação entre os componentes básicos.



Fonte: Ramos (2006)

A proteção é desejada por uma razão, minimizar e evitar prejuízos. Porém, muitas vezes esses prejuízos não são bem quantificados. Dias (2000) mostra que a visibilidade de alguns problemas aumenta sua prioridade, dessa maneira a proteção contra um furto de uma estação de trabalho, por exemplo, acaba sendo mais prioritário do que uma

contaminação por vírus e pode deixar diversas estações inoperantes, ou seja, o prejuízo por deixa-las sem operar pode ser bem maior do que o furto de uma estação.

Os incidentes podem ser classificados em três grupos, natural, acidental ou intencional, como podemos ver na Tabela 5.

Origem do evento	Exemplo
Natural	Fenômenos meteorológicos
Acidental	Erros de usuário Falhas nos sistemas Falta de energia elétrica
Intencional	Invasões Terrorismo Espionagem industrial

Quadro 6 - Exemplo de classificação de eventos.
Fonte: Ramos (2006)

Ramos (2006) aponta que um dos grandes problemas com que as organizações têm que lidar atualmente é que os incidentes vêm aumentando gradativamente, mas junto com ele também aumenta a qualidade desses incidentes, proporcionando prejuízos cada vez maiores.

Algumas estratégias de proteção são utilizadas para implementação da segurança visando guiar o seu desenvolvimento, dentre elas pode-se citar a estratégia do privilégio mínimo, que define que não devemos nos expor a situações de riscos desnecessárias, ou seja, que somente deve ser liberado àquele usuário o necessário para que ele possa exercer suas funções.

Outra estratégia é a defesa em profundidade. Não adianta investir um número exorbitante em uma única proteção impenetrável. Dessa forma queremos dizer que para um determinado ativo sendo protegido, diversos canais de comunicação entre o ativo e o ambiente externo podem existir, e de nada adianta proteger incansavelmente um dessas canais se um outro está indefeso. Com certeza o canal pouco protegido ou desprotegido será utilizado como porta de entrada.

São muito aplicadas nesses casos às proteções em camadas, que além de garantir que os controles se complementem, garante que um será redundância do outro em caso de falha ou violação, e assim evita que a violação de um controle de proteção possa se tornar a violação de um sistema como um todo.

Mas essa estratégia só funciona caso os controles aplicados sejam diferentes uns dos outros, por exemplo, se em uma topologia existir 3 *firewalls* e todos eles forem do mesmo fabricante, e configurado da mesma maneira. Caso um atacante viole uma das proteções provavelmente ele irá violar o outro com facilidade.

Outra estratégia comumente usada é do elo mais fraco, de nada adianta você tratar diversas vulnerabilidades e deixar uma vulnerabilidade sem tratamento. O nível de segurança será sempre o mesmo da proteção mais frágil.

A estratégia do ponto de estrangulamento traz a idéia de se manter apenas um ponto de entrada e saída, dessa maneira além de reduzir os custos em medidas de proteção, já que o custo para tratar uma vulnerabilidade é menor do que tratar 10, reduz-se o número de vulnerabilidades.

Outra estratégia é a segurança através da obscuridade, o que muitas vezes pode ser uma ótima estratégia, se combinada com outros controles, já que a melhor forma de se proteger algo é evitar que alguém tenha conhecimento que ele exista.

A simplicidade talvez seja o mais importante conceito de todos, já que quanto mais simples for um sistema mais fácil será protegê-lo, menores serão as ameaças, as vulnerabilidades e consequentemente os riscos.

5.3 Gestão de Risco

Dentre as varias disciplinas ou domínios de conhecimento necessários para o processo de gestão de segurança da informação, provavelmente a gestão de riscos é um dos mais importantes.

Para Sêmola (2003b), no passado os riscos associados à informação estavam limitados aos aspectos como segurança e continuidade dos negócios. Hoje, o conceito sobre riscos evoluiu e tornou-se clara a visão de que os riscos não são unidimensionais. Um completo programa de gestão de riscos avalia os riscos relativos à segurança, disponibilidade, confiabilidade, integridade dos dados e a conformidade com exigências regulatórias ou legais.

Gomes e Braga (2006) afirma que a gestão de risco torna possível a identificação e a correta avaliação dos riscos associados aos ativos, ou seja, uma correta quantificação do impacto nos negócios das organizações. Com um processo sistemático de identificação, análise, avaliação, tratamento, comunicação e revisão dos riscos é possível traçar a evolução do nível dos riscos nos ativos, priorizando, dessa forma, os investimentos e iniciativas para a redução dos riscos.

O processo de gestão de risco envolve a escolha de um escopo que é, necessariamente, um conjunto de ativos que será coberto pelo processo. Esse processo de escolha de um escopo como passo-chave para o sucesso na implementação de um Sistema de Gestão de Risco. É importante lembrar que escopos muito grandes, podem gerar projetos muito longos, e assim dificultar a evolução e a apresentação de resultados.

De acordo com AS/NZS 4360 (2004), pode-se definir o Sistema de Gestão de Risco como sendo as práticas e procedimento a serem seguidos para suportar a gerência dos riscos.

Como já citado, vários componentes são definidos para realizar a discrição do impacto em um ativo, todos eles devem ser levados em consideração no processo de gestão dos riscos. Os ativos, o escopo, a ameaça, as vulnerabilidades, proteção, risco já foram definidos. Nesse momento vamos definir mais detalhadamente alguns desses temos.

A parte envolvida ou interessada é considerada como o individuo ou grupo que são afetados diretamente pelo risco, alguns exemplos dessa definição são os clientes, colaboradores, fornecedores entre outros.

A ameaça que é tudo que pode explorar uma vulnerabilidade a fim de causar algum impacto nos ativos, quando concretizados são conhecidos como incidentes. Quando um incidente ocorre pode trazer um dano direto, como por exemplo, um sistema de notas fiscais que fica inativo, e/ou um dano indireto como afetar a imagem de uma empresa.

Conforme Ramos (2006), as ameaças podem ser classificadas em duas categorias:

Ambiental, que são causadas por fenômenos naturais como, por exemplo, enxurradas, tornados, terremotos, também através da interrupção de serviços como o fornecimento de água, energia elétrica, ou ainda incêndios e desastres aéreos.

Humana, é definido quando uma ameaça se concretiza através de uma ação direta de uma pessoa, seja ela intencional ou não, como por exemplo, erros operacionais de um sistema, criação e envio de vírus, roubo de informações.

Conforme definido anteriormente, as vulnerabilidades por si só não causam prejuízos, e sim, a exploração de uma vulnerabilidade por uma ameaça. No processo de Gestão de Riscos é necessário identificar essas vulnerabilidades, ou seja, levantar as falhas ou ausências de proteções, e após desta identificação é necessária à avaliação das vulnerabilidades que é realizado combinado as vulnerabilidades encontradas com as ameaças existentes, a fim de avaliar a probabilidade que elas podem ocorrer.

No processo de gestão do risco, o risco de um ativo é dado através de uma escala, que é a combinação de dois fatores. A probabilidade de uma ameaça ocorrer aliada ao impacto causado por um incidente.

Quando se lida com risco geralmente se analisa, avalia, trata e comunica. Durante esse processo pode acontecer que no risco identificado, o seu tratamento tenha um custo maior do que o próprio valor do ativo, e dessa maneira, inicia-se o processo de aceitação do risco, que é reconhecer que o risco existe, e aceitá-lo, entendendo que ele poderá ser explorado futuramente.

Esse processo de tratamento também se torna muito caro e, às vezes, muito trabalhoso tratar todos os risco encontrados, dessa forma, sempre acaba existindo um risco residual. O principal objetivo da Gestão de Risco é trazer esse risco residual para níveis aceitáveis. Ao medirmos os riscos dos ativos de uma organização alcançamos índices individuais de risco por ativo, assim sendo, nesse processo de aceitação a organização define uma linha ou um critério de risco, que é o nível de risco definido como tolerável.

A gestão de risco contempla uma série de atividades, desde o processo de identificação até o processo de comunicação as parte interessadas. Podemos destacar as atividades de Análise, Avaliação, Tratamento, Aceitação e Comunicação dos riscos.

A análise dos riscos consiste em identificar as ameaças e estimar os riscos. A identificação das ameaças é feita através de buscas em bases de informação que possam servir como fonte sobre os diversos tipos de ameaças existentes sobre os ativos que estamos analisando. Alguns exemplos de bases utilizadas são as listas de discussão, boletins especializados, sites de fornecedores, entre outros. A estimativa dos riscos irá trazer os índices de risco sobre os componentes do ativo, sendo eles estimados através dos impactos, e probabilidades que é calculada a partir da combinação da ameaça com uma ou mais vulnerabilidades.

A fase seguinte é a de Avaliação de Riscos, e esse é o processo em que se comparam os níveis de risco identificados, com o nível de risco definido como tolerável pela organização. A partir desse ponto definimos se tratamos ou aceitamos o risco em questão.

Segundo Gomes e Braga (2006), uma vez definido quais os riscos que vão ser tratados e quais os riscos serão aceitos, dar-se inicio ao processo de tratamento. O tratamento do risco consiste em selecionar e implementar medidas de proteção que possam reduzir o risco encontrado, ou seja, aumentar o índice de segurança para níveis considerados aceitos de acordo o patamar definido.

Conforme apontado por NBR ISO 31000 (2009), durante um processo de tratamento de risco existem algumas medidas que podemos considerar, entre elas:

- Evitar o risco – Adotar medidas que não exponham o ativo a uma situação de risco;

- Transferir o risco – Às vezes pode ser mais barato, fazer um seguro do ativo, assim caso o risco se transforme em um incidente, o impacto será bem menor, se tornando um prejuízo calculado;
- Reter o risco – Caso a probabilidade de um risco se transformar em um incidente seja muito remota, talvez seja interessante fazer um auto seguro, ou seja, reter um valor mensal de forma que se houver um impacto a própria organização já esteja preparada para assumir os custos;
- Reduzir o risco – Como falado anteriormente são as medidas de proteção que implementamos para reduzir o nível do risco;
- Mitigar o risco - Seria a adoção de medidas que minimizem o impacto do risco sobre o ativo, ou seja, diminuam os prejuízos.

Durante a aplicação dessas medidas pode ocorrer que o custo de proteção sobre um determinado risco seja maior que o valor do ativo, ou até mesmo o impacto que ele pode trazer. Nesse momento ocorre uma aceitação do risco. Outro momento em que o risco é aceito, acontece quando o risco encontrado já se encontra dentro dos patamares definidos pela organização. A norma NBR ISO/IEC 17799 (2005) afirma que a definição desses patamares deve levar em consideração alguns fatores.

- Os requisitos e restrições de legislação e regulamentações nacionais e internacionais;
- Os objetivos organizacionais;
- Os requisitos e restrições operacionais;
- Custo de implementação e a operação em relação aos riscos que estão sendo reduzidos e que permanecem proporcionais as restrições e requisitos da organização;
- A necessidade de balancear o investimento na implementação e operação de controles contra a probabilidade de danos que resultem em falhas de segurança da informação.

Ramos (2006) identifica o último componente do processo de Gestão de Riscos. A comunicação do risco tem o propósito de fechar o ciclo por meio de divulgação de informações sobre os riscos que foram identificados, tenham eles sido tratados ou não, às partes interessadas, visando atingir alguns objetivos, como destacar o fornecimento de um cenário claro dos riscos existente e o compartilhamento de responsabilidades. Ao comunicarmos os riscos, as partes interessadas, estamos compartilhando a

responsabilidade, ou seja, estamos fazendo com que essas pessoas tenham ciência dos riscos, e assim tornando essa parte interessada responsável pelo risco.

A melhor maneira de comunicarmos um risco é através da criação de campanhas de conscientização de segurança.

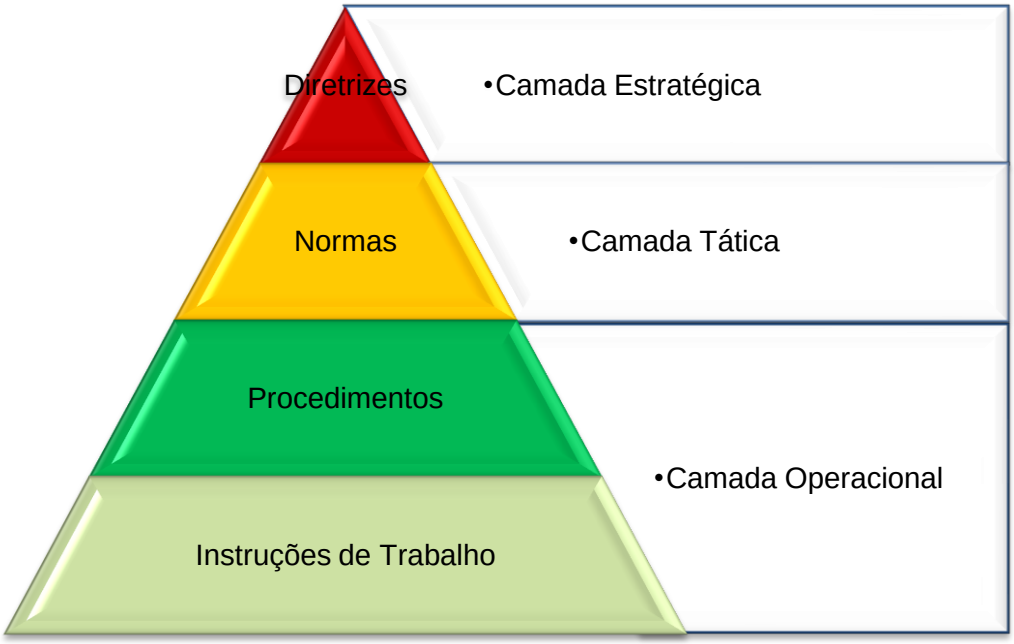
Resumidamente, pode-se afirmar que o ponto fundamental de um processo de gestão de risco é justamente a possibilidade de identificar quais são as maiores vulnerabilidades e as ameaças correspondentes e, a partir disto, realizar o planejamento dos controles e medidas de proteção necessárias para redução dos riscos.

5.4 Política de Segurança da informação

Numa Gestão de Segurança da Informação efetiva, sem dúvida a definição e implantação de uma Política de Segurança da Informação é o primeiro passo a ser dado. A política de segurança servirá não só para definir as regras e responsabilidades a serem seguidas por todos na organização, mas servirá como um guia, um norte para que a área responsável saiba para onde ir e o que executar.

Segundo Sêmola (2003) a política de segurança da informação tem um papel fundamental e muito se assemelha a constituição federal, uma vez que a política é quem descreve as regras fundamentais de Segurança da Informação nas empresas. O autor ainda comenta que por sua grande abrangência, uma vez que ela define regras e responsabilidades nas camadas estratégicas, táticas (gestão) e operacional, ela se divide em quatro categorias. São elas, diretrizes, normas, procedimentos e instruções de trabalho.

Figura 3 - Estrutura da Política de Segurança da Informação.



Fonte: Fontes (2012)

As Diretrizes (o que é esperado) são escritas em mais alto nível e geralmente definem o que alta diretoria espera que seja tratado pela área de Segurança e demais áreas. Já as Normas (o que deve ser feito) são escritas de forma a detalhar cada uma das diretrizes traçadas pela Alta diretoria, descrevendo diversas regras a serem seguidas pelos usuários para cada um dos requisitos esperados. Já os procedimentos (como fazer) e as instruções de trabalho (detalhamento do como fazer) são escritos de maneira a ensinar aos usuários e ajudá-los em caso de duvidas em como operacionalizar e seguir as regras existentes.

Como descrito anteriormente, a Política de Segurança da Informação nasce da alta administração, da camada estratégica, e para que tenha êxito no processo de implantação é imprescindível contar com o apoio da diretoria e, sobretudo, com o exemplo desse grupo no cumprimento das regras estabelecidas, levando a uma credibilidade das Políticas.

Fontes (2006) afirma que nas organizações o processo de segurança envolve aspectos técnicos, humanos e organizacionais e ainda que deva considerar as características operacionais, culturais e o relacionamento existente entre as pessoas na empresa, para que tenha êxito.

Já Pinheiro (2009) se manifesta sobre o tema afirmando que as Políticas de Segurança da Informação têm um viés jurídico, uma vez que ela define que todos os colaboradores são responsáveis pelo cumprimento de suas regras e ainda as punições caso

contrário, portanto, se faz necessário a formalização de ciência e aceite dos documentos. A autora ainda complementa que deve existir a etapa de divulgação e conscientização dos usuários com base na Política de Segurança da Informação, evitando assim a ocorrência de incidentes e a garantia de que os usuários sabem o seu papel perante o uso correto das informações na empresa.

Complementando a afirmativa acima, o Código Penal Brasileiro (artigos 153 e 154) já considera crimes referentes ao vazamento de informações, de tal forma que aqueles que o praticam podem responder a processo, obviamente se for comprovado. Diante disso cabe as empresas considerar a inclusão de uma cláusula de confidencialidade nos contratos de trabalho ou a geração de um termo de confidencialidade, onde é definido o termo vazamento de informação assim como as regras a serem seguidas e as punições cabíveis, incluindo nesse caso a possibilidade de processo baseado nos artigos do código penal brasileiro.

Assim sendo, é possível afirmar que a definição, implantação, divulgação e conscientização da Política de Segurança da Informação a todos os seus usuários, devem ser consideradas uma ferramenta indispensável para uma empresa que quer tratar o vazamento de informações corporativo, sendo um meio de inibição e prevenção desse problema recorrente e cada vez mais impactante nas organizações.

5.5 Vazamento e classificação de Informações

Buscando uma definição formal para o termo “vazamento de informações” o Código Penal Brasileiro através de seu artigo 153 define como crime que:

> *Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem...*
>
> *e complementa que:*
>
> *Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública.*

Já o Código Penal Brasileiro, através de seu artigo 154, define que vazamento de informação é:

> *Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem...*

> *e complementa que:*
>
> *Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.*

Resumidamente entende-se como vazamento de informação aquela informação sigilosa que chega ao conhecimento de pessoas não autorizadas, intencionalmente ou não, independente de seu formato e meio de transmissão e que gera algum dano ao seu proprietário.

Já a informação sensível ou sigilosa é aquela que possui algum valor, e que se de conhecimento de pessoas não autorizadas podem gerar danos financeiros, operacionais, legais ou a imagem de seu proprietário.

Pesquisas realizadas por diversas empresas brasileiras apontam o problema de vazamento de informações uma realidade que vem aumentando a cada ano e se tornando cada vez mais, uma das maiores preocupações e ameaças no ambiente corporativo. Considerando as ultimas 3 pesquisas nacionais de Segurança da Informação realizadas pela empresa Módulo Security Solutions, (8ª, 9ª e 10ª), é notório o avanço da preocupação das empresas com o vazamento da informação.

A 8ª pesquisa, divulgada em setembro de 2002, destaca que 48% dos entrevistados considerada o vazamento de informações como uma das principais ameaças e 20% (primeiro lugar) considerando-a como o fator mais critico. Já a 9ª pesquisa divulgada em outubro de 2003 o vazamento de informação é apontado por 47% dos entrevistados e novamente como fator mais critico. Na 10ª pesquisa divulgada em Novembro de 2007 a métrica foi alterada, mas a ameaça com o vazamento de informações é apontado novamente como o fator mais critico e ainda destaca que o fator chave para isso, a falta de conscientização dos executivos e usuários. Para a maioria dos entrevistados, 55%, considera a falta de conscientização dos executivos e usuários o principal obstáculo para a implementação de segurança da informação na empresa, seguido pela falta de orçamento (28%). E o maior motivador para a tomada de decisões visando a segurança é o nível de consciência dos executivos e usuários (31%).

Outras pesquisas mais recentes, como a Pesquisa Global de Segurança da Informação, realizada pela empresa PWC (2012) aponta à preocupação relacionada ao risco de vazamento de informações confidenciais, como na edição de 2011, como o maior problema considerado pelos executivos do Brasil. 70% dos entrevistados consideram esse

um problema estratégico e de grande importância, principalmente num cenário altamente competitivo, que por si só, já é motivo de sobra para explicar as preocupações.

Mas a diferença significativa para os números globais provavelmente se justifica pela insuficiência de controles efetivos nas empresas. Esta constatação é evidente quando observamos, por exemplo, que muitas organizações de médio e grande porte no Brasil ainda se encontram em estágios iniciais de implantação de soluções de DLP (*Data Loss Prevention*).

Nesta mesma pesquisa outro indicador chama bastante atenção quando concluiu-se que 54% das empresas brasileiras informaram que os incidentes tiveram origem de dentro da própria organização, ou seja, o inimigo está mais próximo do que podemos imaginar.

Dentro deste contexto não podemos deixar de destacar que além do vazamento de informações intencional, ou seja, aquele praticado com um propósito específico existe também o não intencional, geralmente cometido por desconhecimento, negligência ou fruto de falha humana.

Para garantir a segurança e o tratamento adequado da informação de qualquer empresa é necessário que, no mínimo, haja normas e procedimentos claros, que devem ser seguidos por todos os usuários, conforme falado no item anterior. E quando o assunto é vazamento de informações, a definição e divulgação de uma norma de Classificação da Informação são imprescindíveis, pois somente através de uma informação classificada é possível definir o seu valor, as medidas de proteção necessárias e consequentemente seu impacto caso sejam utilizadas por pessoas ou para fins indevidos.

Um processo de classificação da informação é imprescindível para o sucesso da proteção e tratamento adequado das informações, pois ninguém melhor do que o dono, para dizer o quão sensível é a informação.

O processo de classificação da informação consiste em definir quais são os níveis de proteção que as informações demandam, estabelecendo os rótulos para identificá-las e dessa forma determinar os controles de proteção necessários a cada uma delas.

A classificação da informação se dá de acordo com o seu grau de sigilo. Geralmente são definidos no mínimo, três níveis de classificação da informação: Pública, Interna e Confidencial. Esses níveis buscam evitar cenários indesejáveis como o de informações sensíveis sem níveis de proteção adequada e o de informações que não precisam de proteção, sendo protegidas de forma excessiva.

Este processo, para ser bem implementado, depende quase que exclusivamente das pessoas.

A Classificação da Informação obriga que todos os usuários da empresa passem a pensar e incorporar a classificação no seu dia a dia, despertando coletivamente a atenção dos usuários para a necessidade de protegerem as informações que estão sob sua custodia ou responsabilidade, trazendo diversos benefícios para a empresa. Vinícius (2010), aponta como benefícios mais tangíveis e mensuráveis:

- Conscientização – Esse processo requer o envolvimento de praticamente todas as pessoas, fazendo com que as pessoas tenham uma dimensão maior da criticidade das informações;
- Responsabilidades – A definição de papeis e responsabilidade distribui o peso da proteção entre os colaboradores da empresa, fazendo com que todos fiquem responsáveis por ela.
- Níveis de proteção – A atribuição de responsabilidades e melhora da consciência dos colaboradores faz com que eles mesmos tragam situações que demandam proteção e que, muitas vezes, fogem aos olhos daqueles que devem se responsabilizar pela proteção. Ninguém conhece melhor o fluxo das informações que as pessoas que fazem uso delas
- Tomadas de decisões – Quando as informações são bem categorizados no ponto de vista da segurança, o processo de tomada de decisões é extremamente beneficiado.

Aliada a esse processo devem ser utilizadas tecnologias, como o do DLP, filtros de conteúdos, ferramentas criptográficas, soluções de gestão documental e etc., que irão apoiar no controle, identificação de incidentes e realização de auditorias que possibilitarão a manutenção e melhoria continua desse processo.

5.6 Pessoas e a Engenharia Social

Mitnick (2003) diz que, ao pensar sobre como as pessoas interferem na segurança da informação, é notório o quanto são vulneráveis e o elo mais fraco dessa corrente.

Os usuários devem, idealmente, ter consciência sobre o que é, e como ter a atitude correta em relação à segurança da informação, fazendo-se necessário assim, criar a transparência, gestão e comunicação eficaz no que diz respeito às diretrizes de segurança da informação que uma empresa adota.

Kraemer, Carayon e Clem (2009) contribuem observando que os usuários não são, necessariamente, contrários à segurança, mas muitas vezes são incapazes de determinar as implicações de suas ações na segurança. A partir desta afirmação, podemos

refletir que a falta de conhecimento gera condutas inapropriadas, uma vez que para agir corretamente é necessário que as pessoas saibam como agir.

Elas deverão ser encaradas como um ponto chave, sendo essencial proporcionar-lhes condições de desenvolvimento e motivação para que exerçam seus papeis e responsabilidades de forma adequada, pois considerando que as políticas de segurança criam uma mudança cultural muito grande na empresa e alteram a forma como os usuários trabalham, ter as pessoas resistentes ao seu processo resultará em uma menor aderência e consequentemente em um menor ganho de segurança.

Por isso é importante que as empresas dediquem especial atenção ao programa de conscientização dos usuários, pois assim o usuário será capaz de construir o comportamento seguro a partir das informações apresentadas, passando da incerteza e da indefinição para a clareza e a confiança do que e como fazer.

Visando a construção desse comportamento seguro, sugere-se proporcionar esclarecimentos adequados acerca do que vem a ser um comportamento seguro, o que é segurança da informação, formas através das quais se consegue minimizar os riscos, como salvaguardar os ativos informacionais corporativos e como se posicionar para se preservar de ataques.

A chamada engenharia social vai além dos hackers e vírus; o funcionário insatisfeito, negligente ou ingênuo aliado ao vazamento de informações, passam a fazer parte do rol de preocupações, e se tornam um dos desafios mais complexos no âmbito das vulnerabilidades encontradas na gestão da Segurança da Informação.

O sucesso no ataque de engenharia social ocorre geralmente quando os alvos são as pessoas ingênuas ou que desconhecem as melhores práticas de segurança, daí a importância do programa de conscientização dos usuários.

De acordo com Ramos (2006), a engenharia social é

> *"um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações".*

Ou, segundo um dos maiores especialistas na arte da engenharia social, Kevin Mitnick em Mitnick (2003, p. 5) a engenharia social

> *"usa a influencia e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia".*

Geralmente o engenheiro social é um tipo de pessoa agradável. Ou seja, uma pessoa educada, simpática, carismática. Mas, sobretudo criativa, flexível e dinâmica.

Possuindo uma conversa bastante envolvente que geralmente ocasiona o vazamento de informações sensíveis.

Entre as principais técnicas utilizadas pelos engenheiros sócias para alcançar seus objetivos, pode-se destacar as realizadas por telefone quando se passam por alguém, conhecendo informações básicas que podem ser adquiridas pela internet através da coleta de informações pessoais e itens de autenticação, como por exemplo, sites que fornecem id e passwords padrões, sites clonados, envio de e-mails falsos, ou mesmo pessoalmente, persuadindo os seus alvos, utilizando-se de tecnologias espiãs para monitorar de modo oculto as atividades do computador. Também é bem plausível a avaliação do lixo, físico ou lógico, onde muita das vezes contém informações essenciais ao suposto engenheiro social.

É importante conscientizar as pessoas sobre o valor da informação que elas dispõem e manipulam, e como elas podem ser influenciadas através das ações de um engenheiro social.

O seu risco não diminui com o simples fato de publicar uma política ou de fornecer uma cartilha sobre a política de segurança. As empresas devem não apenas definir por escrito as regras das políticas, mas também devem se esforçar ao máximo para orientar todos os que trabalham com as informações corporativas ou com os recursos de tecnologia da informação para que eles entendam o motivo de sua existência, aprendam e sigam as regras. Caso contrário, a ignorância sempre será a melhor desculpa do empregado, e é exatamente essa vulnerabilidade que os engenheiros sociais vão explorar.

O objetivo central de um programa de conscientização sobre segurança da informação é influenciar as pessoas para que elas mudem seu comportamento e suas atitudes motivando cada empregado a querer entrar no programa e fazer a sua parte para proteger os ativos de informações da organização.

Um programa de conscientização deve ser focado nas pessoas que tem acesso a informações confidenciais ou a recursos de tecnologia da informação, deve ser contínuo e ser sempre revisado, visando manter atualizar os usuários sobre as novas ameaças e vulnerabilidades que vem com as novas tecnologias, a todo o momento implementado.

3 Metodologia

O presente trabalho foi realizado por meio de uma pesquisa descritiva. Segundo Gil (2002), a pesquisa descritiva visa à descrição das características de determinadas populações ou fenômenos e a descrever características de grupos, como também a descrição de um processo numa organização.

A metodologia adotada neste estudo utilizou-se do levantamento bibliográfico e análise de exemplos da literatura com base em materiais já elaborados da área, principalmente publicado em livros, normas e artigos científicos, além da realização de estudos de campo para pautar os resultados obtidos.

Com isso a pesquisa pretende apontar os principais aspectos relacionados ao vazamento de informações nas empresas. Como referência de fontes, foram escolhidos autores referidos em projetos similares e os títulos mais significativos relacionados com a área envolvida com o tema. O tema principal dessa pesquisa, vazamento de informações, ainda não foi muito explorado por pesquisadores, fazendo-se necessária assim, a realização de uma pesquisa bibliográfica de temas co-relacionados e aplicar o conhecimento prático e estudos de campo na área para auxiliar na conclusão da pesquisa, com a criação de um checklist, a ser utilizada como roteiro ou ferramenta de consulta para criação de um modelo eficaz contra o vazamento de informações corporativas.

4 Apresentação e análise dos Resultados

Foi realizado um estudo de campo, com a aplicação de um questionário, para a coleta e obtenção de dados baseado em uma amostra. Nesta pesquisa foi feita a distribuição de questionários presenciais bem como enviados por e-mail, para um universo de amostra, com profissionais diversos e consultores da área que atuam em empresas brasileiras, principalmente no estado de Minas Gerais. Foram distribuídos ao todos 74 questionários dos quais 41 foram respondidos entre os meses de Junho e Julho de 2014.

A composição da amostra está constituída por profissionais da área de Tecnologia da Informação, Segurança da Informação, Auditoria, Financeiro, Comércio e Educação, conforme dados constantes da tabela 1.

Ramos de atividade	Distribuição	%
Comercial	4	10%
Industrial	18	44%
Educacional	3	7%
Financeira	4	10%
Prestação de Serviços	10	24%
Governamental	2	5%
Outros	0	0%

Tabela 1 – Ramos de atividades envolvidos na pesquisa.

Fonte: Autor

A estrutura do questionário foi propositalmente dividida em duas partes, onde na primeira foram apresentadas perguntas sobre a percepção da segurança da informação em geral e os possíveis fatores que elevam a ocorrência do problema de vazamento de informações nas empresas, e que tinha como propósito comprovar as afirmações levantadas no estudo bibliográfico, apontado por outros autores. Já a segunda parte do questionário, por sua vez, foi composta de perguntas que buscavam identificar possíveis planos de ação para reduzir o risco de ocorrência do vazamento de informações nas empresas. Nesta segunda parte do questionário o objetivo era identificar quais são as ações e quais devem ser priorizadas pelas empresas brasileiras, visando a mitigação do risco de vazamento de informações corporativas.

Com a aplicação desse questionário, apresentado no apêndice A, buscou-se validar se as sugestões apresentadas no próximo capítulo seriam ou não medidas viáveis para serem utilizadas para aplicação e conseqüente redução deste risco.

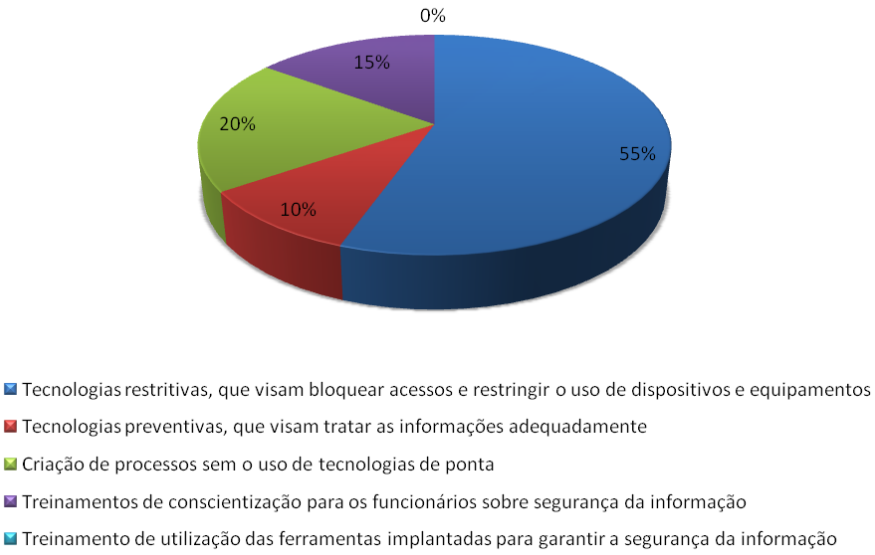
Com a aplicação do questionário foi possível concluir que as afirmações dos autores, de que em Segurança da Informação nada é 100% seguro, é verdadeiro já que grande parte dos entrevistados, 61%, afirmaram terem conhecimento ou que já foram alvos de incidentes de segurança informações em suas empresas, além de 83%, afirmarem que não acreditam que seja possível proteger a empresa por completo.

Com a aplicação do questionário também foi possível constatar que a eliminação total do risco de ocorrência de vazamento de informações nas empresas é praticamente impossível de se conseguir, uma vez que, dentre as razões para que o problema exista estão às ações de má fé, condutas ilícitas, acidentais ou por falta de conhecimento de regras e processos, que em nosso modo de pensar são, a priori, impossíveis de se prever ou evitar, destaque-se que a própria pesquisa comprovou isto.

Os entrevistados apontaram que o maior agente de vazamento de informações das empresas atualmente, ocorrendo de forma não intencional por desconhecimento das regras, seguido pelas ações acidentais. Isso demonstra o quanto um treinamento efetivo pode reduzir os riscos de vazamento de informação na empresa, já que educar as pessoas para que entendam o processo e criar treinamento para automatiza sua execução de forma correta, tratará de forma consistente esses riscos. A pesquisa demonstrou que o menor risco associado ao vazamento vem de forma intencional e realizado por pessoas externas, ou seja, isso demonstra que investir nas tecnologias é necessário, porém não deve ser o foco do investimento.

Seguindo essa linha os entrevistados deram sua opinião sobre onde os investimentos de segurança estão concentrados e, como era esperado, a maioria, 55%, percebe que os investimentos estão sendo concentrados em tecnologias restritivas, que como podemos observar anteriormente não é o grande causador do vazamento de informações na empresa.

Figura 4 – Foco de investimento em Segurança da Informação.



Fonte: Elaborado pelo Autor.

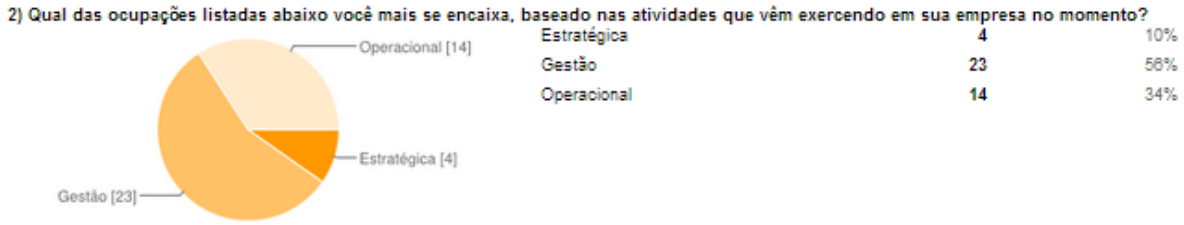
Em contrapartida, os entrevistados apontaram que as empresas deveriam mudar seu foco de investimento para a realização de treinamentos de conscientização, o que para surpresa demonstra que os usuários têm a visão de que as pessoas são os maiores causadores de vazamento de informação, e demonstrando também que os treinamentos que vêm sendo realizados não estão sendo efetivos, cabendo a empresa mudar sua atuação buscando empresas cada vez mais especializadas neste tipo de atividade. Outro ponto importante foi que os usuários apontam que o uso de tecnologias preventivas ao invés das restritivas também irá auxiliar no tratamento desse risco tão iminente, já que com o uso de ferramentas preventivas, além de reduzir a quase zero o numero de exceções, ela prevê a atuação direta do usuário final, servindo assim como uma ferramenta de conscientização constante aos usuários.

Durante a pesquisa foi comprovado que grande parte dos usuários, 80%, enxerga em sua organização alguma iniciativa de segurança da informação, e afirma que ela possui regras definidas, porém a falta de transparência e a pouca qualidade dos treinamentos não cria nos usuários o comportamento seguro tão desejado e que necessita ser proativo. Isso foi demonstrado pelo pouco apoio que a alta administração tem dado a essas iniciativas e que apesar de 71% terem afirmado que têm um programa de conscientização em Segurança da Informação em suas empresas, apenas 56% afirmam terem sido treinados. E como premissa nessa área, um elo fraco da corrente pode quebrá-la, ou seja, uma pessoa que na organização que não possui um comportamento seguro pode vazar informações sigilosas e trazer grandes impactos para a organização.

E confirmando a expectativa de todos e que justifica esse estudo, é que 80% dos entrevistados afirmam que informações sensíveis vazam em suas empresas e 20% delas dizem que isso ocorre a todo o momento. Além disso, 76% dos entrevistados não se sentem seguros em suas empresas, quando o assunto é manipulação e compartilhamento informações, porém como uma luz no fim do túnel essa pesquisa também demonstra que a solução para esse problema está dentro de casa, já que 85% afirmam que se sentem parte responsável pela segurança da informação praticada na organização, o que mais uma vez ressalta a necessidade de demonstrar a esses usuários como fazer o certo, para que essa sensação de responsabilidade se torne uma medida de proteção eficaz e eficiente.

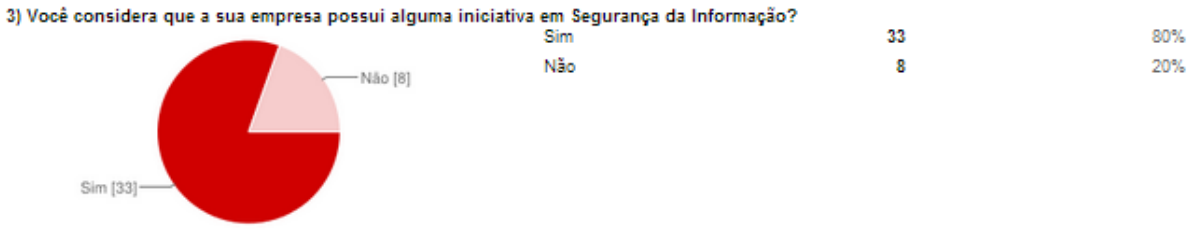
Abaixo seguem algumas figuras representando as respostas dos entrevistados.

Figura 5 – Questão 2 da pesquisa de campo.



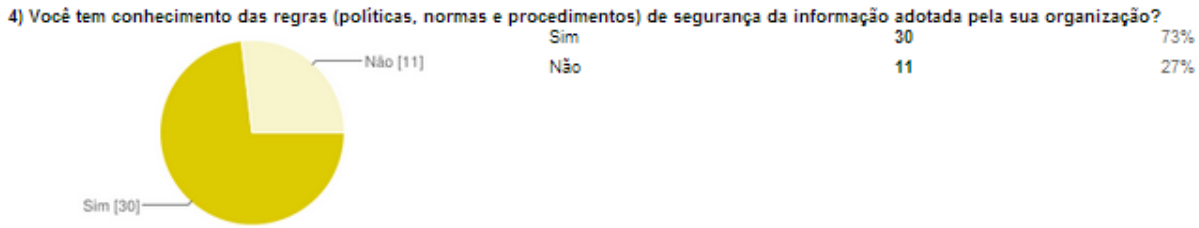
Fonte: Elaborado pelo autor.

Figura 6 – Questão 3 da pesquisa de campo.



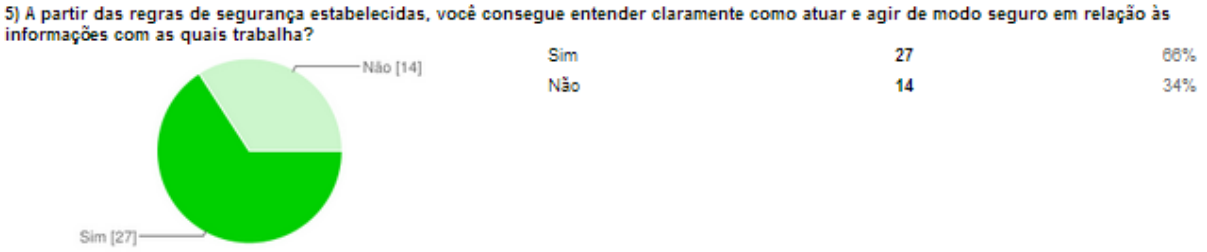
Fonte: Elaborado pelo autor.

Figura 7 – Questão 4 da pesquisa de campo.



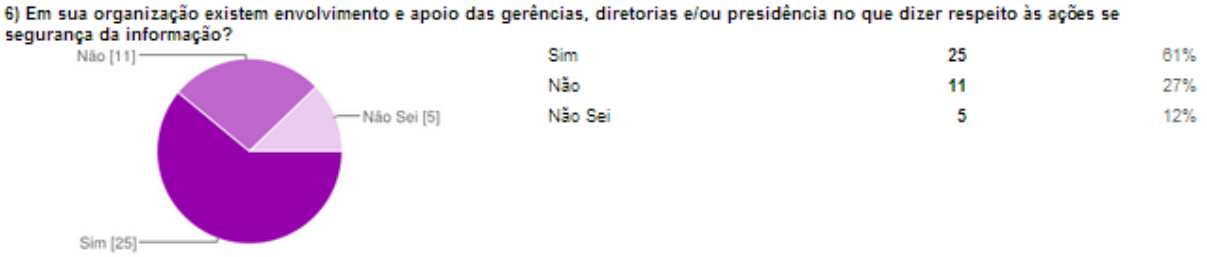
Fonte: Elaborado pelo autor.

Figura 8 – Questão 5 da pesquisa de campo.



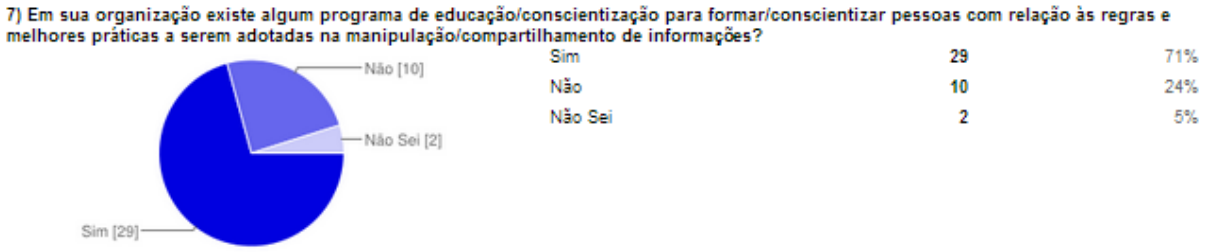
Fonte: Elaborado pelo autor.

Figura 9 – Questão 6 da pesquisa de campo.



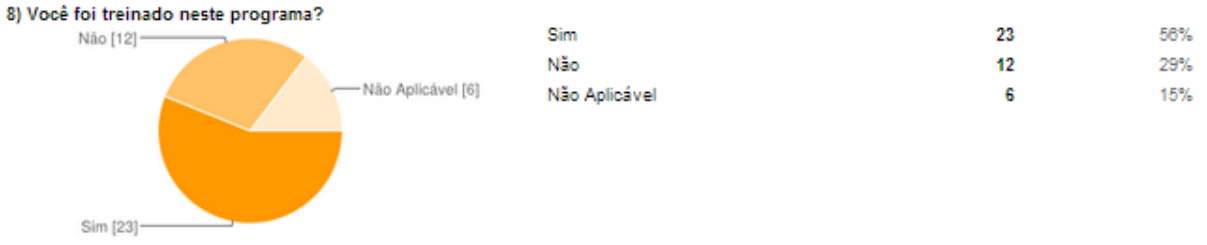
Fonte: Elaborado pelo autor.

Figura 10 – Questão 7 da pesquisa de campo.



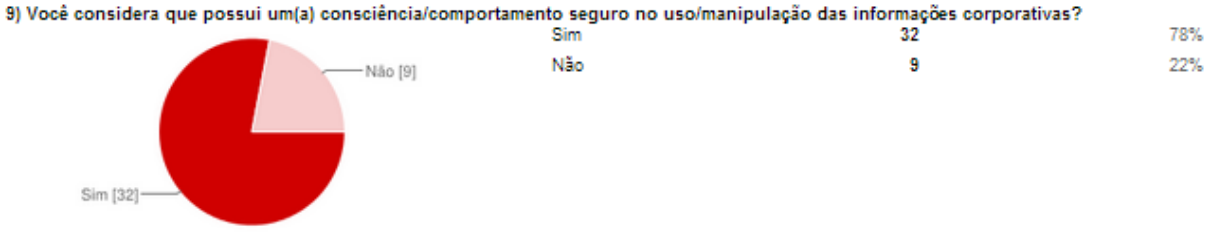
Fonte: Elaborado pelo autor.

Figura 11 – Questão 8 da pesquisa de campo.



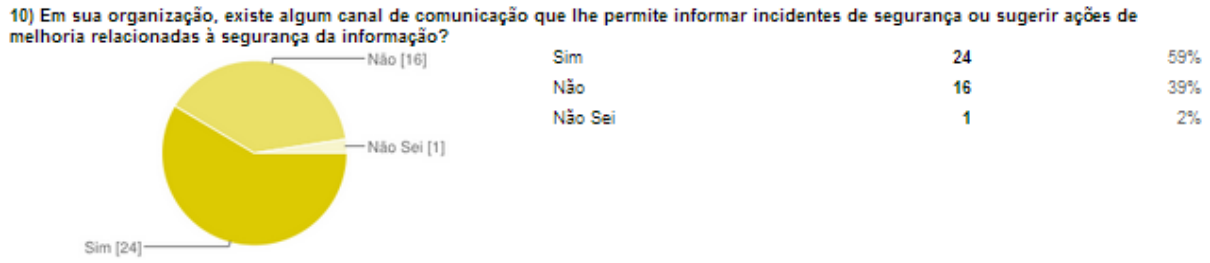
Fonte: Elaborado pelo autor.

Figura 12 – Questão 8 da pesquisa de campo.



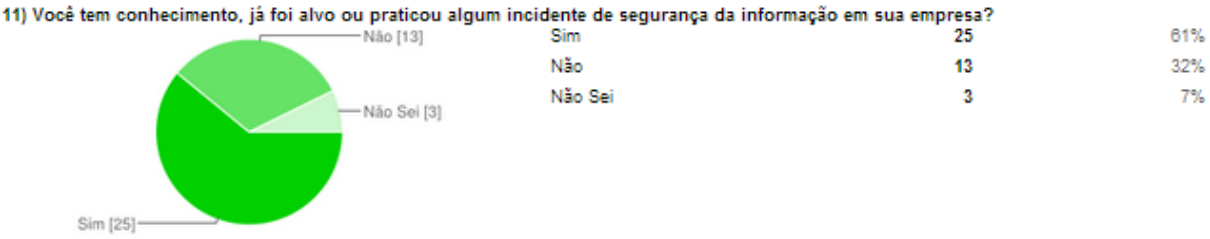
Fonte: Elaborado pelo autor.

Figura 13 – Questão 10 da pesquisa de campo.



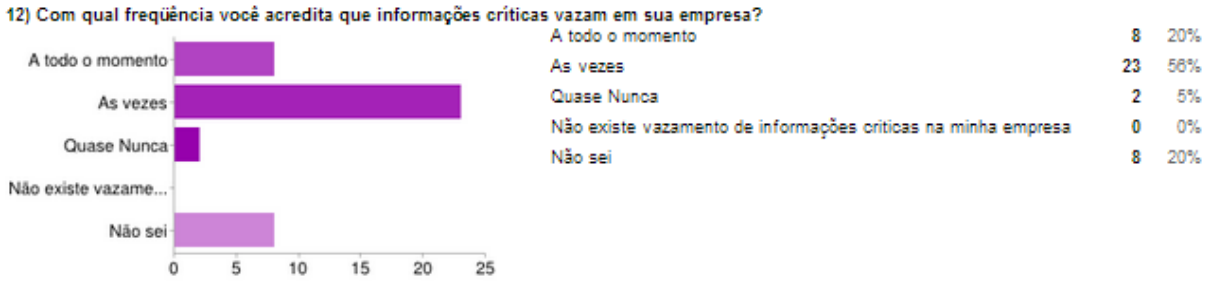
Fonte: Elaborado pelo autor.

Figura 14 – Questão 11 da pesquisa de campo.



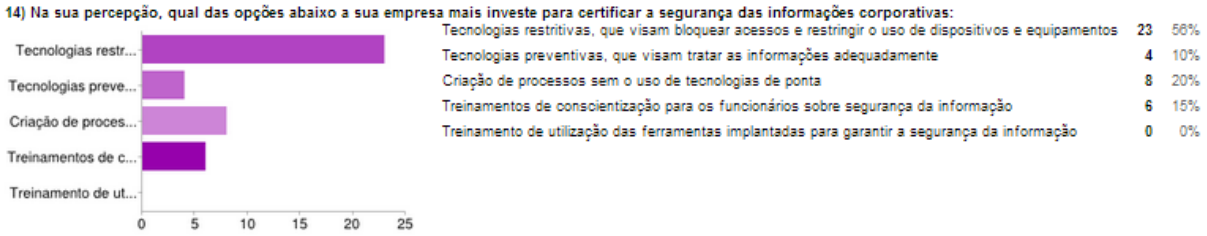
Fonte: Elaborado pelo autor.

Figura 15 – Questão 12 da pesquisa de campo.



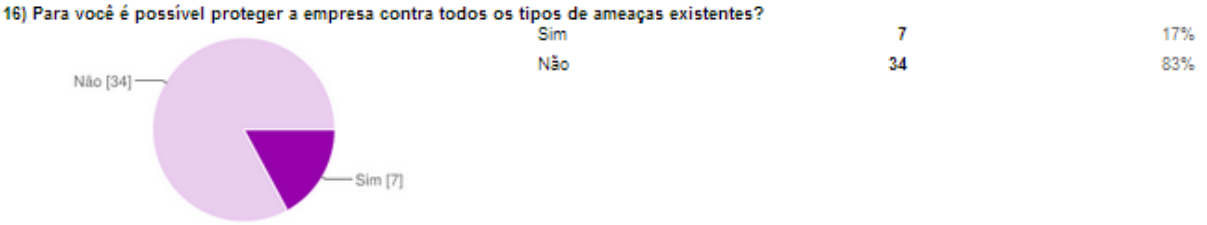
Fonte: Elaborado pelo autor.

Figura 16 – Questão 14 da pesquisa de campo.



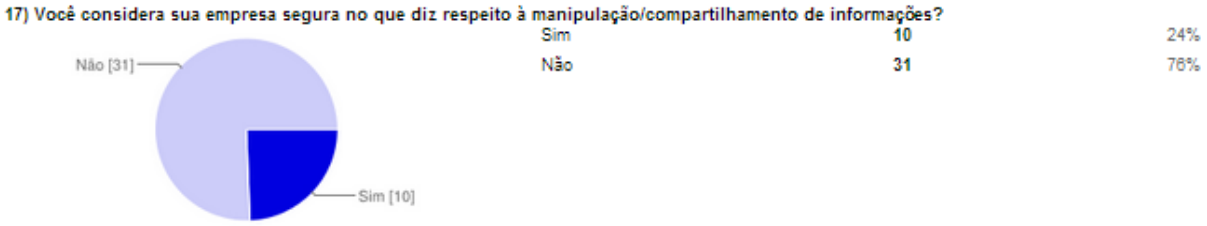
Fonte: Elaborado pelo autor.

Figura 17 – Questão 16 da pesquisa de campo.



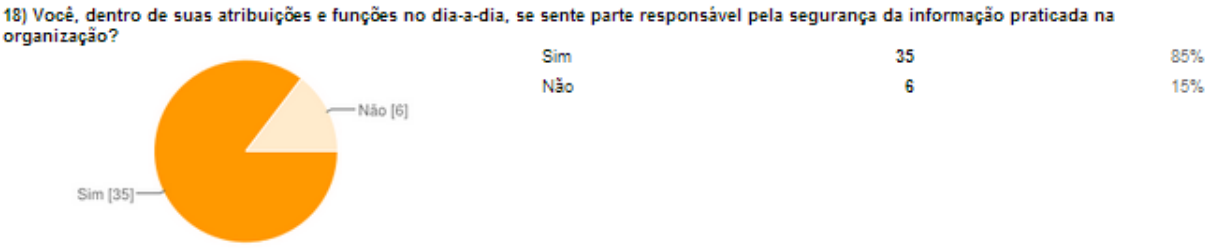
Fonte: Elaborado pelo autor.

Figura 18 – Questão 17 da pesquisa de campo.



Fonte: Elaborado pelo autor.

Figura 19 – Questão 18 da pesquisa de campo.



5 Conclusões

É importante questionar o porquê do fato de que mesmo os executivos conhecendo todos esses problemas, citados na pesquisa, as falhas de segurança continuam a ocorrer de maneira tão constante.

Com o apoio de César e Onaga (2007), pode se dizer que isso ocorre, basicamente, devido a quatro motivos:

- É impossível cobrir todos os aspectos para garantir a proteção de todas as informações;
- Ao mesmo tempo em que as tecnologias de proteção evoluem, as ferramentas utilizadas para causar danos, invasões e roubo de informações também;
- O alto custo de investimento necessário para implementar os mecanismos de proteções;
- A constante atuação provisória, sem atacar a causa raiz dos incidentes de segurança.

Ainda pode-se complementar dando destaque a outros dois motivos:

- Equilibrar a implementação de mecanismos de segurança e a privação de colaboração entre os usuários, ou seja, tornar a empresa mais segura sem engessar os seus processos de negócio;
- Pessoas.

Considerando os elementos básicos que compõe e fazem o sistema de Segurança da Informação operar corretamente (processos, tecnologias e pessoas), com certeza o elemento mais frágil e que tende a mudanças constantes são as pessoas. Levando em consideração que a tecnologia (produtos, soluções e sistemas) e os processos (diretrizes, normas e procedimentos) são manipulados e utilizados pelas pessoas, logo, as pessoas se tornam o elemento mais importante e frágil, que faz todo esse sistema funcionar.

E ai vem as seguintes questões: as pessoas são tratadas como o elemento mais importante? Os investimentos estão sendo direcionados para a conscientização constante das pessoas? Os diretores estão preocupados com esse tema? As pessoas sabem que são o ponto chave para o sucesso de um programa de segurança da informação?

Com base na pesquisa realizada por esse trabalho e a sua comparação com pesquisas de mercado se constatou que a seqüência de prioridades dentro de uma organização são, primeira a tecnologia, seguido pelos processos e só depois as pessoas. A falta de conscientização dos usuários tem contribuído bastante para o problema de

vazamento de informações corporativas, uma vez que esse assunto não vem sendo discutido de maneira profissional e assim crendo que esse problema nunca ocorrerá na sua empresa.

Dessa maneira chega-se à conclusão que é muito importante que sejam desenvolvidos e implantados processos e ações voltados para a conscientização dos usuários, sobretudo a sensibilização da alta administração, pois sem o apoio e o exemplo dos diretores, o sucesso de uma tarefa já difícil, se torna praticamente impossível.

Embora seja difícil de medir a evolução e justificar o investimento, foi constatado pela pesquisa que cada vez mais as empresas, através de seus próprios funcionários, estão se dando conta de que é necessário dar importância a conscientização das pessoas. Segurança 100% não existe; acabar com o vazamento de informações em uma sociedade onde o que a fomenta é a criação e o compartilhamento de informações, além de impossível é estar em desencontro com as estratégias de criatividade e inovação propostas pelas grades empresas de sucesso, porém mitigá-las e reduzir as causas de vazamento apenas às praticadas de forma intencionais, é possível através da conscientização das pessoas.

O objetivo central de um programa de conscientização sobre segurança é influenciar as pessoas para que elas mudem seu comportamento e suas atitudes motivando cada empregado a querer entrar no programa e fazer a sua parte para proteger os ativos de informações da organização.

Assim, abaixo são sugeridas algumas iniciativas que podem ser seguidas para o sucesso de uma campanha de conscientização em segurança da informação:

Momento	Objetivo	Ações destaque	Exemplo/Considerações
Pré-Lançamento	Planejamento das ações a serem realizadas antes do lançamento oficial da Campanha.	• Identificar os objetivos a serem tratados na campanha; • Ordenar os temas que serão tratados levando em consideração sua criticidade; • Selecionar os recursos de comunicação a serem utilizados na campanha; • Selecionar e produzir	• Definir um Slogan, um mascote, uma logomarca, onde e como será realizada a palestra presencial, a definição e criação de um treinamento on-line, e-mail marketing, jogos educacionais, peças de teatro e etc.

Momento	Objetivo	Ações destaque	Exemplo/Considerações
		peças de divulgação; • Criar página web especifica sobre o assunto; • Definir quem serão os multiplicadores; • Definir os procedimentos e ferramentas de medição de efetividade; • Desenvolver o treinamento envolvendo á área de comunicação e recursos humanos da empresa.	• Utilziar cartazes, banners e plotters, banners eletrônicos na intranet, protetores de tela, brindes, cartilhas e folhetos.
Lançamento	Lançar a campanha de forma efetiva, através de um evento imponente, para que todas as pessoas da empresa, funcionários e terceiros, saibam do inicio da campanha.	**Ações antes do lançamento:** • Com uma antecedência, de aproximadamente 15 (quinze) dias da data definida para o lançamento da campanha, fixar cartazes, banners e plotters em locais estratégicos, enviar informações sobre o lançamento da campanha via e-mail, intranet e outras mídias de comunicação eletrônica. • 05 (cinco) dias antes o lançamento da campanha, enviar convite (eletrônico) para todos os	Utilizar-se do tema segurança no dia a dia, onde devem ser observados: • Ser realizados presencialmente, utilizando-se de bons interlocutores e materiais interativos, como por exemplo, uso de peças de teatros, dramatização e entrega de brindes em rodadas de perguntas e respostas. Para funcionários que não podem participar do

Momento	Objetivo	Ações destaque	Exemplo/Considerações
		usuários. Além disso, fixar cartazes, banners e plotters em locais estratégicos e disponibilizar na intranet banner no formato do convite, informando o tema, o motivo da palestra, palestrante, local, data e hora. **Ações durante o lançamento:** • Divulgar o objetivo, a logomarca, o slogan e mascote (se houver) da campanha na página da Segurança da Informação na Intranet, nos painéis, informativos e outras mídias habitualmente usadas; • Disponibilizar na Intranet, papel de parede sobre a campanha de divulgação para download; • Distribuir a cartilha de Segurança da Informação; • Distribuir os materiais de divulgação ao final da palestra; • Distribuir questionário de avaliação do evento;	encontro é importante que sejam desenvolvidos treinamento on-line, com a utilização, por exemplo, de vídeos, animações e conteúdo didático claro; • É importante que sejam criados treinamentos que prendam a atenção e que sejam curtas o suficiente para que a mensagem a ser transmitida seja entregue, compreendida e lembrada ao longo da rotina de trabalho. Como exemplo pode ser apresentado problemas reais que acontecem na corporação e soluções que podem ser adotadas para sua correção; • O conteúdo deve dar ênfase à segurança no dia a dia e ao mal que um incidente de

Momento	Objetivo	Ações destaque	Exemplo/Considerações
			segurança pode trazer para a empresa e para os empregados a menos que todos assumam um comportamento seguro, afinal o elo mais franco de uma corrente é que a compromete toda a segurança;
Pós Lançamento	Garantir a fixação e a conscientização dos usuários de forma continua	• Divulgar toda a campanha realizada na Intranet e/ou em áreas de acesso a documentos para os usuários; • Orientar, divulgar e treinar os usuários nos temas considerados críticos. Durante essa divulgação, alguns temas exigirão ações específicas voltadas para o usuário final e outros focados nos administradores técnicos; • Deve ser considerada a realização obrigatória de treinamento para todos os novos usuários; • Ter apoio dos gerentes deixando claro que os	• Realizar sessões mais longas com o intuito de educar os empregados sobre temas mais específicos, entrando em seu detalhe. Realizando referencias a políticas, normas e procedimentos de Segurança da Informação e claro utilizando-se de exemplos reais da empresa; • Executar treinamentos de renovação pelo menos uma vez por ano;

Momento	Objetivo	Ações destaque	Exemplo/Considerações
		subordinados devem investir o tempo de trabalho na execução desses treinamentos.	• Verificar necessidade de realizar novos treinamentos em casos de mudança de posição dentro da organização, já que esses usuários podem ter acesso a informações mais sigilosas. • Os empregados novos devem realizar os treinamentos antes de receber um acesso a um computador.
Medição e melhoria continua	Garantir que os treinamentos estejam sendo efetivos	• Criar treinamentos adicionais sobre os temas que se mostraram mais vulneráveis. • Identificar possíveis alvos de treinamentos através da ocorrência repetida de incidentes do mesmo tipo; • Identificar melhorias através de pesquisas e resultados de testes; • Capacitar agentes multiplicadores	• Realizar teste de engenharia social através de ligação telefônica fingindo ser quem não é e tentado resetar a senha de outro colaborador; • Enviar as mesmas mensagens escritas de forma diferente em meios diferentes, já que a mudança na redação das mensagens evita

Momento	Objetivo	Ações destaque	Exemplo/Considerações
			que elas se tornem familiar demais para serem ignoradas.

Tabela 2 – Recomendações programa de conscientização.
Fonte: Autor

Ressalte-se sempre que as mudanças são diárias, as tecnologias se aprimoram, os processos são alterados, novas pessoas chegam à empresa e outras saem, fazendo-se necessário assim, que todo esse processo se torne um ciclo continuo e bastante criativo para que se alcance o êxito.

Referências

10ª PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO, Módulo Security Solutions, Rio de Janeiro, 2007

8ª PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO, Módulo Security Solutions, Rio de Janeiro, 2002

9ª PESQUISA NACIONAL DE SEGURANÇA DA INFORMAÇÃO, Módulo Security Solutions, Rio de Janeiro, 2003

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000:2009**. Gestão de Risco - Princípios e Diretrizes. Rio de Janeiro, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:2005.** Tecnologia da Informação, Técnicas de Segurança, código de prática para gestão da Segurança da Informação. Rio de Janeiro, 2005.

AUSTRALIAN E STANDARDS NEW ZEALAND, Série Risk Management. **AS/NZS 4360**. Gestão de riscos. São Paulo: Editora Risk Tecnologia, 2004.

BRASILIANO, Antônio Celso Ribeiro. **Manual de Análise de Risco para a Segurança Empresarial**. São Paulo: Editora Sicurezza, 2003.

CÉSAR. Ricardo; ONAGA, Marcelo. Cercada por hackers. Portal Exame, 2007. Disponível em: http://exame.abril.com.br/revista-exame/edicoes/0897/noticias/cercadas-por-hackers-m0133377. Acesso em: 5 de abr 2014.

CÓDIGO PENAL BRASILEIRO, Art. 153 do Código Penal - Decreto Lei 2848/40. Disponível em: http://www.jusbrasil.com.br/topicos/10620036/artigo-153-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940 Acesso em: 14 de mar 2014.

CÓDIGO PENAL BRASILEIRO, Art. 154 do Código Penal - Decreto Lei 2848/40. Disponível em: http://www.jusbrasil.com.br/topicos/10619917/artigo-154-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940 Acesso em: 14 de mar 2014.

DAVENPORT, T., PRUSAK, L. **Conhecimento empresarial**. Rio de Janeiro: Campus, 1999. 237p

DAWEL, George. **A segurança da informação nas empresas: as informações de sua empresa estão seguras?** 1. ed. Ciência Moderna, 2004.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Editora Axcel Books do Brasil, 2000.

FONTES, Edison Luiz Gonçalves. **Políticas e Normas para a Segurança da Informação**. 1. Ed. São Paulo: Brasport, 2012.

FONTES, Edison Luiz Gonçalves. **Segurança da Informação: O usuário faz a diferença.** 1. Ed. São Paulo: Saraiva, 2006.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GOMES, Elisabeth; BRAGA, Fabiane. **Gestão de riscos para tomar decisões mais precisas é o nome do novo jogo empresarial**. 2006. Disponível em http://www.gomesebraga.com.br//artigo06.htm. Acesso em 14 de Fev 2014.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC GUIDE 73:2002** – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

KRAEMER, S.; CARAYON, P.; CLEM, J. ***Human and organizational factors in computer and information security***. Computer & Security. 2009. v.28, p. 509-520

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar.** 1. ed. Makron Books, 2003.

PESQUISA GLOBAL DE SEGURANÇA DA INFORMAÇÃO, PriceWaterHouseCoopers, São Paulo, 2012

PINHEIRO, Patricia Peck. **Direito Digital.** 3. Ed. São Paulo: Saraiva, 2009.

RAMOS, Anderson (org.) **Security Officer – 1: guia oficial para formação de gestores em segurança da informação**. Porto Alegre: Editora Zouk, 2006.

SÊMOLA, Marcos. **É preciso ter uma visão integrada dos riscos**. Jornal O Globo, 20 de janeiro de 2003b. Disponível em <http://www.semola.com.br/disco/Coluna_IDGNow_E1.pdf>. Acesso em 16 de Mar 2014.

SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma Visão executiva.** Rio de Janeiro: Editora Campus, 2003a.

SILVA, Antônio Everaldo. **Segurança da Informação. Vazamento de Informações - As Informações Estão Realmente Seguras em sua Empresa?** Rio de Janeiro: Editora Ciência Moderna, 2012.

VINÍCIUS, Elger. Classificação da Informação. Security Hacker, 2010. Disponível em: http://www.securityhacker.org/artigos/2010/12/05/classificacao-da-informacao. Acesso em: 15 de mar 2014.

APÊNDICE A

Questionário aplicado visando à compreensão e comparação dos resultados.

QUESTIONARIO PARA ANÁLISE E AVALIAÇÃO DE PROFISSIONAIS SOB A PERSPECTIVA DA SEGURANÇA DAS INFORMAÇÕES NO TRATAMENTO AS INFORMAÇÕES CORPORATIVAS

Olá,

Este questionário foi criado para ser utilizado como ferramenta de pesquisa para elaboração de monografia referente ao curso de **especialização em Gestão Estratégica da Informação da UFMG**. O objetivo deste questionário é servir como base para aferir o estudo bibliográfico realizado sobre o tema **Vazamento de Informações Corporativas**.

Caso tenha interesse em receber o resultado deste trabalho, favor informar seu e-mail no campo a seguir:

e-mail:_____

Instruções para resposta ao questionário:

O questionário nas páginas a seguir é formado por 18 perguntas objetivas que **não possuem respostas certas e erradas**. Seu propósito é avaliar como os profissionais que atuam em empresas brasileiras lidam com as informações corporativas no seu dia a dia.

Você levará de 7 a 10 minutos para respondê-lo completamente.

---

1) **Qual o ramo de atividade da empresa em que você atua?**
   a) Comercial
   b) Industrial
   c) Educacional
   d) Financeiro
   e) Prestação de Serviços
   f) Governamental
   g) Outros. Qual:_____

2) **Qual das ocupações listadas abaixo você mais se encaixa, baseado nas atividades que vêm exercendo em sua empresa no momento?**
   a) Estratégica
   b) Gestão
   c) Operacional

3) **Você considera que a sua empresa possui alguma iniciativa em Segurança da Informação?**
   a) Sim
   b) Não

4) **Você tem conhecimento das regras (políticas, normas e procedimentos) de segurança da informação adotada pela sua organização?**
   a) Sim
   b) Não

5) **A partir das regras de segurança estabelecidas, você consegue entender claramente como atuar e agir de modo seguro em relação às informações com as quais trabalha?**
   a) Sim
   b) Não

6) **Em sua organização existem envolvimento e apoio das gerências, diretorias e/ou presidência no que dizer respeito às ações se segurança da informação?**
   a) Sim
   b) Não
   c) Não sei

7) **Em sua organização existe algum programa de educação/conscientização para formar/conscientizar pessoas com relação às regras e melhores práticas a serem adotadas na manipulação/compartilhamento de informações?**
   a) Sim
   b) Não
   c) Não sei

8) **Você foi treinado neste programa?**
   a) Sim
   b) Não
   c) Não aplicável

9) **Você considera que possui um(a) consciência/comportamento seguro no uso/manipulação das informações corporativas?**
   a) Sim
   b) Não

10) **Em sua organização, existe algum canal de comunicação que lhe permite informar incidentes de segurança ou sugerir ações de melhoria relacionadas à segurança da informação?**
   a) Sim
   b) Não
   c) Não sei

11) **Você tem conhecimento, já foi alvo ou praticou algum incidente de segurança da informação em sua empresa?**
   a) Sim
   b) Não
   c) Não sei

12) **Com qual freqüência você acredita que informações críticas vazem em sua empresa?**
   a) A todo o momento
   b) Às vezes
   c) Quase nunca
   d) Não existe vazamento de informações criticas na minha empresa
   e) Não sei

13) **Indique nas opções abaixo os tipos de vazamento de informações que você acredita que ocorra com maior freqüência em sua empresa, seguindo uma escala de 1º(primeiro) ao 5º (quinto), onde 1º é o que mais ocorre e o 5º é o que menos acontece:**
   a) Relacione:

   ( ) Intencional, através de um funcionário, com o objetivo de trazer prejuízos para a empresa

   ( ) Intencional, através de uma pessoa fora da empresa, com o objetivo de trazer prejuízos para a empresa

   ( ) Intencional, sem o objetivo de prejudicar a empresa

( ) Não intencional, por falta de conhecimento das regras

( ) Não intencional, acidental

b) Não aplicável

14) Na sua percepção, qual das opções abaixo a sua empresa <u>mais</u> investe para certificar a segurança das informações corporativas:

a) Tecnologias restritivas, que visam bloquear acessos e restringir o uso de dispositivos e equipamentos
b) Tecnologias preventivas, que visam tratar as informações adequadamente
c) Criação de processos sem o uso de tecnologias de ponta
d) Treinamentos de conscientização para os funcionários sobre segurança da informação
e) Treinamento de utilização das ferramentas implantadas para garantir a segurança da informação

15) Em sua opinião, relacione nas opções abaixo as ações que você acredita que a sua empresa deveria <u>mais</u> investir para certificar que as informações corporativas estejam mais seguras, numa escala de 1º(primeiro) ao 5º (quinto), onde 1º é o que mais deveria existir investimento e o 5º é o que menos deveria:

( ) Tecnologias restritivas, que visam bloquear acessos e restringir o uso de dispositivos e equipamentos

( ) Tecnologias preventivas, que visam tratar as informações adequadamente

( ) Criação de processos sem o uso de tecnologias de ponta

( ) Treinamentos de conscientização para os funcionários sobre segurança da informação

( ) Treinamento de utilização das ferramentas implantadas para garantir a segurança da informação

16) Para você é possível proteger a empresa contra todos os tipos de ameaças existentes?

a) Sim
b) Não

17) Você considera sua empresa segura no que diz respeito à manipulação/compartilhamento de informações?

a) Sim
b) Não

18) Você, dentro de suas atribuições e funções no dia-a-dia, se sente parte responsável pela segurança da informação praticada na organização?

a) Sim

b) Não