UMA ANÁLISE SOBRE OS RECURSOS HUMANOS COMO ORIGEM DE INCIDENTES À SEGURANÇA DA INFORMAÇÃO

Eriany da Cruz Matos[1]

Douglas Farias Cordeiro[1]

Resumo:

A informação é considerada um dos elementos chave para o desenvolvimento das organizações, e a garantia de sua segurança passa ser um requisito necessário e primordial. Entretanto, o conhecimento sobre as principais origens de violações à segurança da informação, assim como os mecanismos de proteção a serem adotados, ainda são considerados desafios, nos seus mais diversos aspectos. Em grande parte das organizações se mantém a ideia de que as principais fontes de ataques provêm de meios externos, fato este que não condiz com levantamentos realizados na área. Neste sentido, este artigo apresenta um estudo analítico sobre a representatividade dos recursos humanos como ameaça à segurança da informação, comparando resultados com outras possíveis fontes, e destacando a importância da implantação de políticas de segurança e controles específicos voltados a este propósito.

Palavras-chave: segurança da informação, recursos humanos, análise.

Abstract: Information is a key element for the organization development, and the guarantee of their security passes to be a necessary and fundamental requirement. However, knowledge of the main sources of violations of information security as well as protection mechanisms to be adopted, are still considered challenges in its various aspects. In most organizations remains the idea that the main sources of attacks come from external means, a fact that is not consistent with surveys conducted in the area. Thus, this paper presents an analytical study of the representation of human resources as a threat to information security, comparing results with other possible sources, and highlighting the importance of implementing security and specific controls aimed at this purpose policies.

Keywords: information security, human resources, analysis.

1. Introdução

A informação pode ser descrita como um conteúdo passível de armazenamento ou que possa ser transferido e utilizável pelo homem. Além disso, a informação possibilita adquirir conhecimento e auxiliar nas tomadas de decisão. Esses fatores levaram a informação a se tornar um elemento de grande relevância para as organizações. Entretanto, à medida que a manipulação das informações podem convergir no surgimento de vulnerabilidades, suscetíveis a diversos tipos de ataques, o que leva a uma necessidade iminente de proteção da informação. Proteger a informação implica em analisar os causadores de incidentes, analisar os valores de cada informação, para então especificar quais as medidas que podem ser tomadas.

[1] Faculdade de Informação e Comunicação - Universidade Federal de Goiás

Em virtude disso este artigo apresenta estudos realizados em conformidade com a proteção da informação, visando identificar o principal causador de incidentes contra a informação em ambientes corporativos, e quais os principais obstáculos que as empresas identificam para melhorar a proteção da informação. Neste sentido, é apresentada uma pesquisa voltada à identificação de falhas nos recursos humanos, o que os caracterizam como fonte principal de danos à informação.

2. A Informação

A informação é um elemento fundamental no processo da comunicação. Esse processo de comunicação não acontece somente no processo social, mas também no mundo tecnológico. A informação pode ser descrita como um conjunto de dados organizados que referenciam um acontecimento, fato ou fenômeno com a finalidade de adquirir conhecimento, e auxiliar nas tomadas de decisão (Choo, 2003).

O desenvolvimento tecnológico associado à evolução cientifica culminou no surgimento da Era da Informação, onde a informação se tornou um elemento motriz para os negócios e novos empreendimentos. Uma boa informação abre verdadeiras oportunidades, gera competitividade entre as empresas, porém a ausência da Informação ou a Informação de má qualidade pode constitui uma grande ameaça à continuidade de negócios.

Uma informação passa por um ciclo vida que pode ser classificado em seis etapas: identificação das necessidades e dos requisitos, obtenção, tratamento, distribuição, uso, armazenamento e descarte (Beal, 2005). Além deste ciclo de vida, a informação possui elementos que a compõem como dado, conhecimento, a informação propriamente dita, e inteligência, os quais são descritos como:

- **Dado**: informações soltas sem tratamento, pode-se dizer que são informações que não transmite uma mensagem específica.
- **Informação**: conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenômeno ou evento. A informação permite resolver problemas e tomar decisões, tendo em conta que o seu uso racional é a base do conhecimento..
- **Conhecimento**: informação com relevância, cuja importância e confiabilidade foram avaliadas.
- **Inteligência**: informação como oportunidade, é a parte de da informação que se utiliza para tomadas de decisões.

A informação pode ser classificada também como tácita, onde o conhecimento em geral é definido como o conhecimento pessoal, contextual e, portanto difícil de formalizar, ou como informação implícita, em que o conhecimento é passível de ser transmitido formalmente e sistematicamente através da linguagem. Sendo assim é possível que o usuário descubra novas formas de identificar e tornar viável o uso dessa informação.

O grande fluxo de informação que uma empresa possui se transformou em um fator de preocupação nas organizações, pois quanto maior o número de informação mais vulnerável ela se encontra. Diante disso, é importante que a informação receba um

tratamento para garantir sua disponibilidade e integridade àqueles que necessitam utilizá-la. Cuidar da disponibilidade e integridade da informação é um fator que se remete à proteção da informação em sua forma impressa, armazenada em nuvens, manipulada em dispositivos móveis, entre outros. Neste contexto, os maiores esforços em segurança da informação são voltados ao seu compartilhamento e armazenamento com referência à aspectos externos, e não à questões que estão diretamente relacionadas aos recursos humanos, como é descrito neste artigo.

3. Segurança da Informação

Segundo Dias (2000), segurança da informação trata da utilização de ferramentas para a proteção de informações, sistemas, recursos e serviços, contra erros, manipulação não autorizada e desastres. Esses mecanismos visam garantir a redução do impacto e a diminuição da probabilidade de incidentes de segurança.

A segurança da informação surge como resposta às necessidades de proteção da informação, nos seus mais diversos aspectos, os quais podem ir desde ameaças puramente tecnológicas, eventos climatológicos, até questões relacionadas aos recursos humanos de uma organização (BEAL, 2005). Diante disso a segurança da informação trata do processo de proteção dos ativos pertencentes a uma organização ou a um indivíduo. Este processo de proteção da informação visa, principalmente, diminuir as vulnerabilidades existentes e prevenir de possíveis ataques.

De acordo com a norma ISO/IEC 27002 (2013), a segurança da informação é a proteção da informação contra diferentes tipos de ameaças, com o intuito de garantir a continuidade do serviço, minimizar os riscos, maximizar o retorno sobre os investimentos e as oportunidades. Conforme a norma, a segurança da informação possui três principais conceitos:

- **Ativo**: tudo que possua valor para organização.
- **Vulnerabilidade**: possibilidade de que a informação esteja suscetível a ameaças.
- **Ameaça**: possibilidade de ocorrer algum evento que impacte negativamente nas organizações.

Além dos principais conceitos descritos, convém dizer que a segurança da informação é composta por elementos que auxiliam na identificação e proteção dos ativos de uma organização. Essas características devem ser consideradas desde o início do ciclo de vida da informação até o processo de criação de uma política de segurança. As características mais identificadas na busca pela proteção da informação podem ser classificadas como:

- **Integridade**: garantia de que a informação mantenha suas propriedades originais, as quais são definidas pelo proprietário da informação;
- **Disponibilidade**: garantia de que a informação sempre esteja disponível ao uso por aqueles que foram autorizados pelo proprietário da informação;
- **Confidencialidade**: garantia de que o acesso à informação seja limitado apenas àqueles autorizados pelo proprietário da informação.

Outros fatores também podem ser inclusos no processo de proteção a informação, que se destacam os seguintes aspectos:

- **Autenticidade**: garantia de que a informação não foi alterada.
- **Confiabilidade**: garantia que a informação é confiável.
- **Não repudio**: garantia de que o autor não negue ter criado e assinado o documento.
- **Responsabilidade**: É a coparticipação de responsabilidades por todos os que produzem,manuseiam,transportam e descartam a informação, seus sistemas e redes de trabalho.

Quando não apresentadas as propriedades citadas acima pode ocorrer um fator de risco extra no que tange a vulnerabilidade da informação, esses fatores são divididos em três grandes áreas, catástrofes naturais, involuntárias ou intencionais que podem ser conferidas no quadro (1). A exploração destas vulnerabilidades, denominada de ameaça, pode acabar acarretando em danos e perdas, sendo necessária uma análise concisa sobre quais são as vulnerabilidades existentes, e como estas podem ser tratadas a fim de minimizar ou eliminar os possíveis prejuízos.

Quadro 1. Resumo das áreas de vulnerabilidades.

Áreas	O que caracteriza	Exemplos
Catástrofes Naturais	Eventos naturais	Terremotos
		Tempestade
Ações Involuntárias	Quando não há intenção de prejudicar	Derramamento de líquido documentos
		Indisponibilidade de energia
Ações intencionais	Quando há intenção de prejudicar	Extravio de documento
		Acesso não autorizado

Dentro das três áreas mencionadas acima, a única que não se pode ter total controle é a de catástrofes naturais, pois o controle dos eventos da natureza extrapolam as possibilidades de tratamento viabilizadas pela segurança da informação. Por outro lado, as outras duas áreas permitem controle de execução, uma vez que é possível identificar seus responsáveis. Sendo assim, as responsabilidades pelas informações podem ser visas de forma individual.

A responsabilidade da segurança da informação em cada organização depende principalmente do manuseio de cada usuário. É importante que os usuários tenham consciência que um ativo informacional necessita de proteção para que não esteja vulnerável a ameaças e possíveis riscos. Diante disso, existem métricas que podem ser utilizadas para prevenir a probabilidade de sinistros em uma organização,

4. A segurança da informação em recursos humanos de acordo com a norma 27002

A fim de orientar sobre os cuidados que as instituições devem ter em relação aos funcionários e partes externas, a norma ISO 27002 (2013) disponibiliza um documento com diretrizes que podem ser adotadas em um ambiente organizacional. O primeiro tópico a ser destacado pela norma se concentra na contratação dos funcionários por parte das empresas. Sempre que uma empresa busca um novo colaborador no mercado, primeiramente precisa levantar dados e características que adéquam o tipo de funcionário às atividades a serem desenvolvidas. Ao realizar esse tipo pesquisa, a empresa busca identificar se o candidato possui algum histórico de incidente que pode se tornar um diferencial na hora de selecioná-lo, para então permitir acesso do mesmo ao ambiente da empresa. Assim que selecionado o empregador explicitará ao empregado quais as normativas vigentes na instituição, e se a instituição já possuir uma política de segurança é importante que seja apresentada ao empregado quais as diretrizes necessárias para garantir que a informação não se encontre vulnerável. Diante disso, é importante que o empregado tenha ciência, e se possível, assine o termo de compromisso que comprove que ele possui total conhecimento dessas diretrizes, pois se identificado algum tipo de violação o mesmo poderá ser responsabilizado também.

Quando se trata da contratação de um serviço ou fornecedor, é importante seguir os mesmos passos da contratação de um funcionário, acrescentando que sempre que um terceiro necessite de acesso à parte interna da instituição, seja realizada uma triagem para identificação e justificação sobre a real necessidade de acesso ao ambiente. Neste cenário, embora a identificação por crachá seja caracterizada trivial, ainda é uma das melhores formas de identificar um elemento estranho na estrutura física do ambiente. Atualmente as empresas já possuem novos métodos de identificação, os quais permitem que os usuários sejam cadastrados imediatamente, através da utilização de uma digital ou até mesmo uma foto tirada na hora. Esse tipo de identificação facilita o controle de acesso à parte interna da empresa, contribuindo também para garantir a segurança física do ambiente.

O conteúdo da política de segurança da informação pode ser elaborado pela equipe de TI, em conformidade com os regimentos internos e as leis vigentes, sendo necessário que a direção da empresa tenha conhecimento de todas as métricas estabelecidas para a criação dessa política. O princípio da criação de uma política se dá a partir do levantamento de requisitos que se classifica em três principais etapas, que segue a seguir:

1. Análise de riscos da organização - a partir dessa análise é possível avaliar quais ativos estão mais vulneráveis a determinadas ameaças.
2. Analisar a legislação - verificar se o que está descrito na legislação está de acordo com as necessidades do ambiente.
3. Princípio de objetivos e requisitos - identificar objetivos e requisitos que a organização necessita para desenvolver suas atividades.

Diante disso, é importante ressaltar que uma política só entra em vigor a partir do momento em que estiver em conformidade com todos os critérios pré-estabelecidos com a gerência da organização e de acordo com os requisitos listados. Quando este documento se torna vigente, passa a ser de responsabilidade de cada elemento o sigilo e

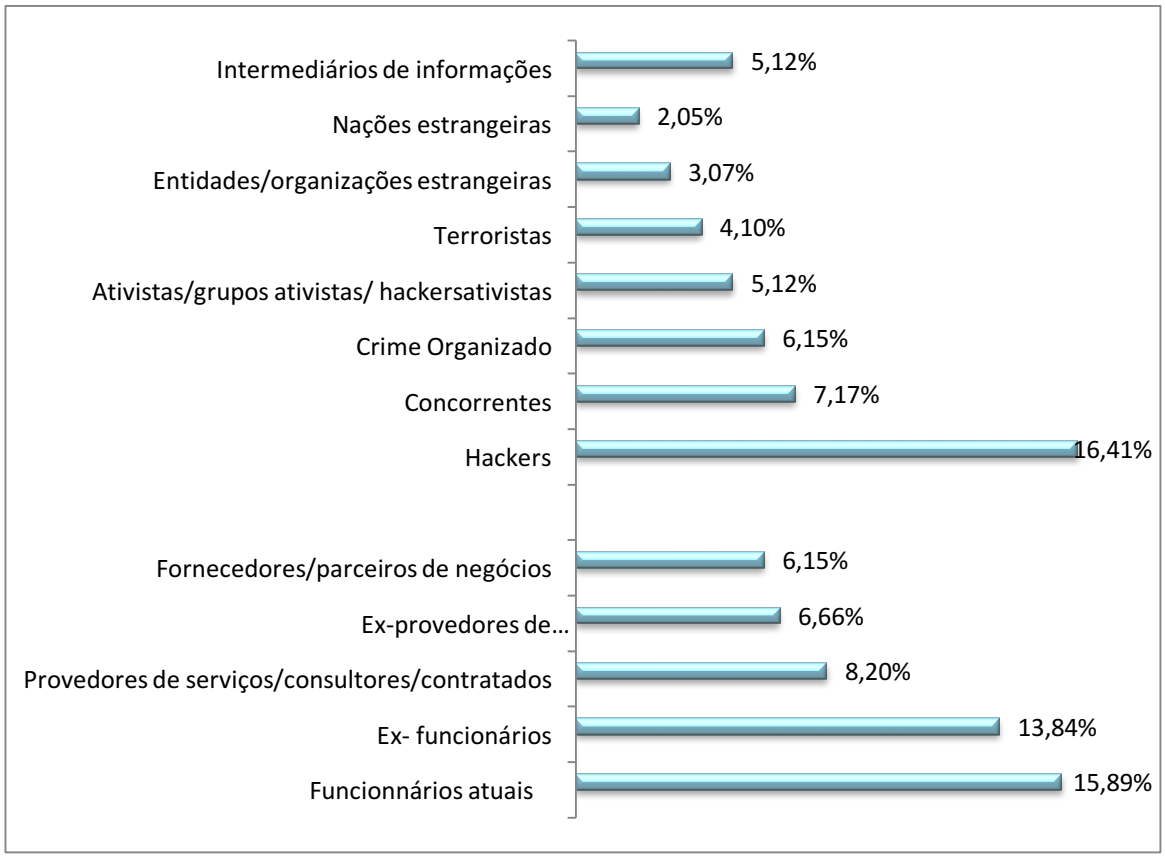
proteção da informação que lhe é confiada. A empresa será responsável por colher assinaturas de todos os funcionários expondo a existência do documento oficial que permite que cada usuário ao utilizar da informação para benefício próprio ou para malefício da instituição poderá ser punido de acordo com o regimento interno.

É importante que funcionários e terceiros sejam monitorados quando permitido o acesso a parte interna ou ao uso de informação privilegiada, e se for verificado que existe algum item previsto na política de segurança que não esteja sendo cumprido pelos empregados ou colaboradores, a empresa possui total autonomia para romper o contrato entre empresas e funcionário ou empresa e fornecedor. Além disso, é fundamental destacar que mesmo após o encerramento de contrato a responsabilidades pela segurança da informação obtida durante o tempo de contrato continuam validas.

4. Análise da segurança da informação

Tradicionalmente, o foco em segurança da informação é voltado ao tratamento de informações compartilhadas, essencialmente sob o contexto externo, entretanto, levantamentos estatísticos revelam que os principais ataques ocorrem por fontes ligadas aos recursos humanos das organizações, conforme é visto na Figura 1. É comum os cenários onde as organizações não aplicam, ou aplicam de forma restrita, controles de segurança da informação com foco em seus recursos humanos.

Figura 1. Pesquisa sobre incidentes na área de segurança da informação, realizada pela PWC no ano de 2014.

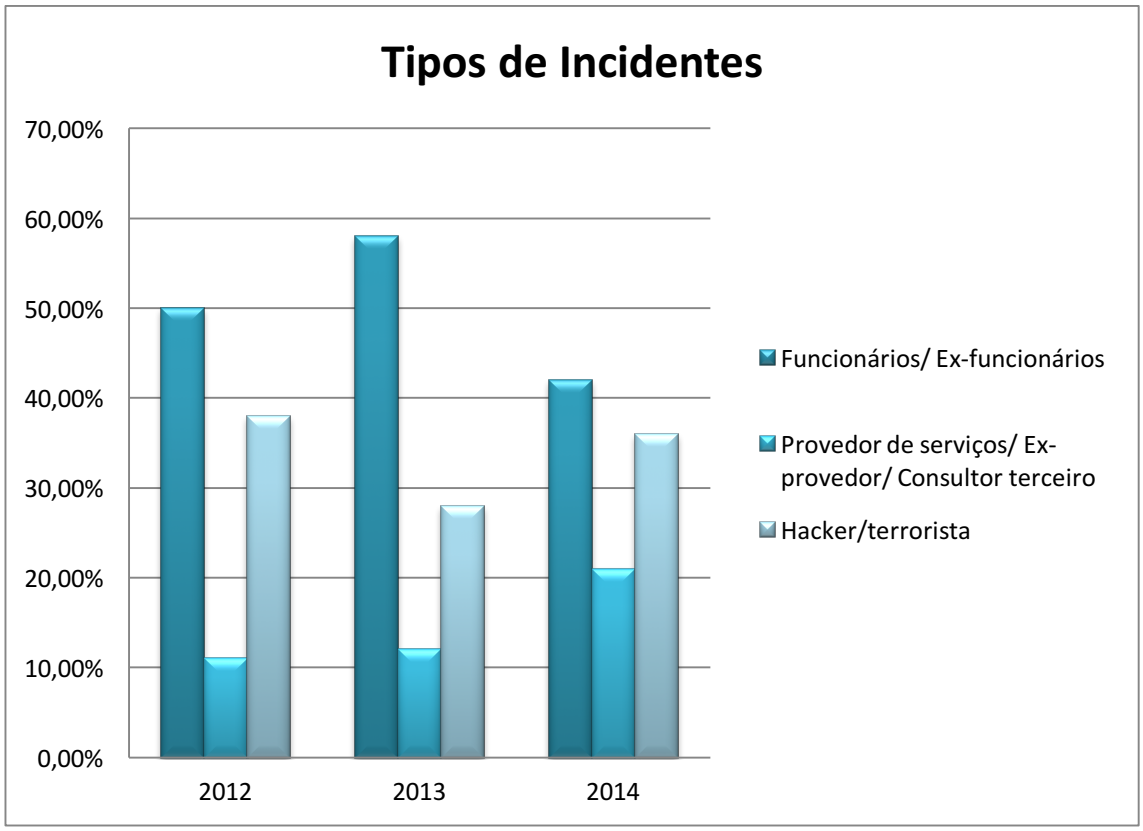


Fonte: PWC (2014)

A segurança da informação não se restringe somente a sistemas de computadores, uma vez que mesmo na utilização destes sistemas torna-se necessária a intervenção humana. Neste contexto, existem indivíduos que manuseiam sistemas a fim de trazer benefícios às empresas, mas também existem aqueles, que motivos diversos, acabam explorando as vulnerabilidades dos sistemas para prejudicar a empresa.

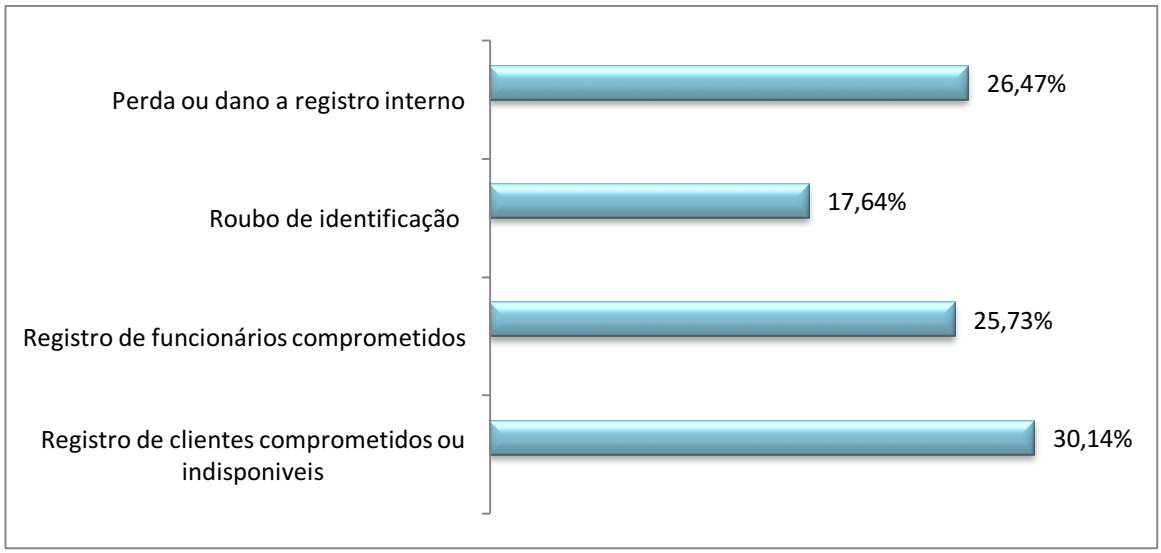
Diante do anteriormente exposto, foi desenvolvido um levantamento comparativo de pesquisas realizadas nos últimos anos sobre a origem das ameaças à segurança da informação. A Figura 2 revela os tipos de incidentes que as empresas vêm sofrendo ao longo dos anos. É possível notar que o maior índice ocorra justamente com funcionários e ex-funcionários. Além disso, também é importante mencionar que terceirizados estão tendo um leve aumento nos índices de incidentes, que de alguma forma acarretam prejuízo a organização. Tais fatores revelam a necessidade de elaboração e implantação de políticas de segurança concisas, a fim de garantir a integridade, confidencialidade e disponibilidade da informação, e consequentemente, amenizar os prejuízos acarretados.

Figura 2 – Comparação temporal dos incidentes de segurança da informação.



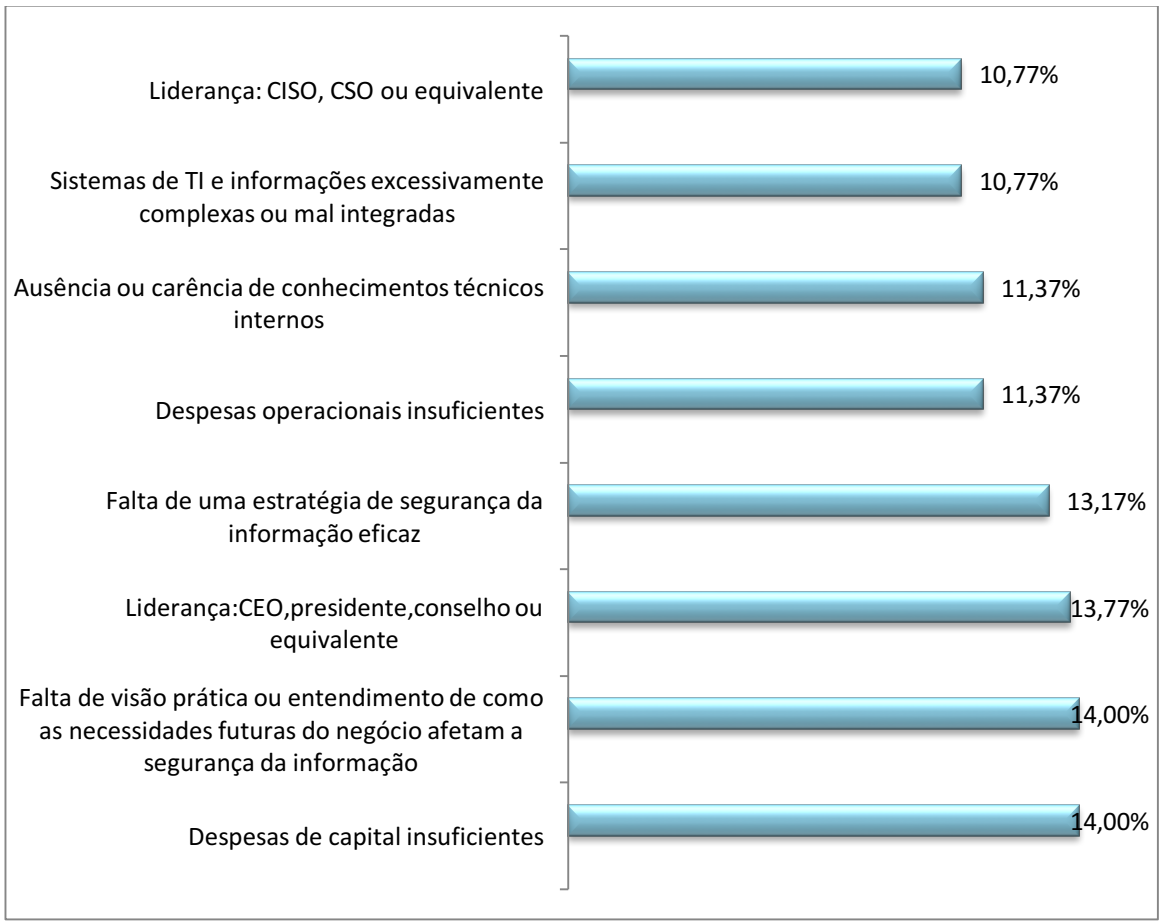
É possível notar uma clara relação entre os dados apresentados na Figura 1 e na Figura 2, onde ambos revelam os altos índices de incidentes provenientes dos recursos humanos. Para tentar diminuir esses incidentes, as empresas buscam investir em estratégias que auxiliem na proteção dos ativos, entretanto é comum que estas encontrem obstáculos, conforme pode ser observado na Figura 4. Esses obstáculos podem acarretar em prejuízos à organização, tanto financeiramente, quanto através de interferências diretas à imagem que a organização possui junto ao mercado, provocando perda de credibilidade e de clientes, tanto os fixos como os que ainda podem ser conquistados. A Figura 3, por outro lado, ressalta os impactos que os incidentes a segurança acarretam em uma organização, confirmando a fragilidade por parte dos recursos humanos na proteção da informação.

Figura 3. Pesquisa sobre impactos de incidentes de segurança de informação, realizada pela PWC no ano de 2014.



Fonte: PWC(2014).

Figura 4. Pesquisa sobre obstáculos para melhorar a segurança da informação nas organizações, realizada pela PWC no ano de 2014.



Fonte: PWC(2014).

Como dito anteriormente, os obstáculos que as empresas encontram equivalem principalmente à falta de estratégia organizacional. Uma organização precisa orientar sua estratégia em comunhão com a proteção da informação, pois só desta maneira será possível que a cultura organizacional da empresa seja modificada de modo a favorecer a proteção da informação e de dados relevantes a organização.

5. Conclusão

A sociedade vive em prol da busca excessiva por informação, ou seja, quanto maior a quantidade de informação que uma organização possua, mais benefícios poderá encontrar. Entretanto, é importante destacar que as informações alcançadas por um indivíduo ou organização necessitam de um levantamento e análise criteriosos, destacando sua relevância e aplicabilidade. Além disso, a segurança da informação surge como um mecanismo adicional, responsável por imputar garantias específicas à informação: disponibilidade, confidencialidade, integridade, confiabilidade, entre outras. Porém, as organizações necessitam estar cientes e dispostas à proteger seus dados e suas informações para que não estejam vulneráveis ao perigo. A segurança da informação deve ser usada de forma estratégica, seguindo as diretrizes que a norma disponibiliza, pois assim é possível manter as informações relativamente seguras, reduzindo os possíveis riscos, como extravio de informação, perda ou roubo de dados importantes, degradação da imagem, perda financeira e entre outros.

Neste contexto, este artigo demonstrou quais os principais fatores de prejuízo à segurança da informação, assim como a origem destes. A partir deste estudo realizado, é possível identificar que as fragilidades existentes nas organizações com relação aos recursos humanos demandam a necessidade de criação de controles específicos, além de conscientização de funcionários. Além disso, é essencial que mecanismos de prevenção sejam implementados para prevenir possíveis danos à organização. Organizações que ainda não possuem política de segurança devam estar atentas ao desenvolvimento e implantação destas, buscando formas de minimizar os incidentes causados a informação. A diminuição e minimização das consequências relativas aos incidentes de segurança da informação só ocorrerá a partir do momento em que as empresas destinarem a atenção para proteção dos ativos.

Referências

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

CHOO, C. W. **A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões**. São Paulo: Editora Senac, 2003.

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

ISO 27002. **NBR ISO/IEC 27002 – Tecnologia da Informação. Código de Prática para Gestão da Segurança da Informação**. Associação Brasileira de Normas Técnicas. Rio de Janeiro, 2013.

PWC. **Uma defesa ultrapassada – principais resultados da Pesquisa Global de Segurança da Informação 2012**. PricewaterhouseCoopers Serviços Profissionais, 2012.

PWC. **Uma defesa ultrapassada – principais resultados da Pesquisa Global de Segurança da Informação 2013**. PricewaterhouseCoopers Serviços Profissionais, 2013.

PWC. **Uma defesa ultrapassada – principais resultados da Pesquisa Global de Segurança da Informação 2014**. PricewaterhouseCoopers Serviços Profissionais, 2014.

SILVA, Denise; STEIN, Lilian. **Segurança da informação: uma reflexão sobre o componente humano**.Ciências & Cognição, 2007.