SEGURANÇA DA INFORMAÇÃO: A PROTEÇÃO CONTRA O VAZAMENTO DE DADOS E SUA IMPORTÂNCIA PARA AS EMPRESAS PRIVADAS

Guilherme Augusto Ruani Barbosa[1], Profa. Me. Maria Helena Barriviera e Silva[2]

[1]Faculdade de Tecnologia de Garça (FATEC) – Egresso do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

[2]Faculdade de Tecnologia de Garça (FATEC) – Docente do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

guilhermeruani@hotmail.com, mhelena@fatecgarca.edu.br

Abstract: *Currently the information is the most important asset for organizations. digital crimes are increasingly sophisticated. They are routinely reported in the news media companies that had their cast intellectual heritage irretrievably. This is because there is usually little concern for information security. Information security is primarily engaged in the development of actions aimed confidentiality, availability, integrity and authenticity of information. The aim of this study is to highlight the value of information, the information security policies, social engineering factor and the combination of technologies such as Data Loss Prevention (DLP) for the security of enterprise information. The methodology relies on literature and field research in a large food company, to describe the view of professionals who are responsible for the security of enterprise information.*

Keywords: *Data Loss Prevention. Prevention. Information security.*

Resumo: Atualmente a informação é o patrimônio mais importante para as organizações. Crimes digitais estão cada vez mais sofisticados. Rotineiramente são divulgadas na mídia notícias de empresas que tiveram seu patrimônio intelectual vazados de forma irrecuperável. Isso ocorre porque normalmente existe pouca preocupação com a segurança da informação. A segurança da informação tem por objetivo principal o desenvolvimento de ações que objetivam a confidencialidade, disponibilidade, integridade e autenticidade das informações. O objetivo deste trabalho é salientar o valor da informação, das políticas de segurança da informação, o fator Engenharia Social e a associação de tecnologias como *Data Loss Prevention* (DLP) para a segurança das informações empresariais. A metodologia utilizada apoia-se na pesquisa bibliográfica e na pesquisa de campo em uma empresa de grande porte do ramo alimentício, no sentido de descrever a visão de profissionais que são responsáveis pela segurança da informação da empresa.

Palavras-chave: *Data Loss Prevention.* Prevenção. Segurança da Informação.

1 INTRODUÇÃO

A evolução do conhecimento é percebida ao longo do tempo e acontece através de inúmeros esforços e experimentos que culminam com o desenvolvimento de novas ciências, tecnologias e controle das informações, bem como sua proteção, o que foi crucial para a ascensão de antigas e atuais organizações. Informações devem ser tratadas de forma correta, pois possuem papel de suma importância para o crescimento de uma organização e para a tomada da boa decisão, essencial para o sucesso dos negócios.

A ampliação dos investimentos em segurança da informação e o desenvolvimento de tecnologias e ferramentas capazes de identificar, classificar e proteger a informação são medidas presentes nas organizações devido ao aumento dos crimes cibernéticos.

O objetivo deste trabalho é salientar o valor da informação, das políticas de segurança da informação, o fator Engenharia Social e a associação de tecnologias como *Data Loss Prevention* (DLP[1]) para a segurança das informações empresariais.

Para o levantamento das informações e análise apresentada ao longo do trabalho foi adotado o procedimento técnico de pesquisa bibliográfica e documental, tendo como base materiais previamente publicados em livros, trabalhos acadêmicos, revistas e na *Internet*. Também foram utilizados para a análise descritiva, entrevistas e aplicação de questionário com profissionais que atuam na área de Tecnologia da Informação (TI).

2 SEGURANÇA DA INFORMAÇÃO

De acordo com Fontes (2006), segurança da informação trata-se de um conjunto de procedimentos, políticas e ações para a proteção das informações, permitindo que o negócio da organização seja contínuo e sua missão alcançada.

O principal objetivo da segurança da informação é minimizar ao máximo qualquer tipo de risco referente ao vazamento de dados, tendo em vista que na maioria dos casos o maior inimigo pode estar dentro da própria organização. Desta forma, é necessário um conjunto de temas, procedimentos e ferramentas para garantir a melhor proteção possível para a informação.

2.1 CLASSIFICAÇÃO DA INFORMAÇÃO

A identificação das informações e a classificação de sua criticidade dentro de uma organização são importantes para estabelecer as melhores práticas e critérios para a sua proteção. A informação gerada por uma organização deve ser criteriosamente classificada e organizada, e desta forma protegida para que haja a continuidade dos negócios.

De acordo com Lyra (2008), a segurança da informação possui várias características importantes, dentre as quais pode-se citar:

- **Confidencialidade:** é a capacidade de um sistema permitir ou restringir o acesso de usuários específicos;
- **Integridade:** consiste em a informação manter-se com suas características originais;
- **Disponibilidade:** significa que a informação deve estar sempre disponível para o acesso;

[1]DLP: o termo DLP, ou *Data Loss Prevention* refere-se a sistemas que identificam, monitoram e protegem dados em uso, em movimento e em repouso, com o objetivo de detectar e prevenir o uso e a transmissão não autorizada de dados que sejam confidenciais (ROEBUCK, 2011).

- **Autenticação:** é a confirmação de autoria do usuário;
- **Não repúdio:** é a capacidade do sistema de provar que um usuário realizou uma tarefa específica;
- **Legalidade:** objetiva garantir que o sistema esteja aderente à legislação pertinente;
- **Privacidade:** é a capacidade de um sistema em garantir o sigilo das informações e ações de um usuário; e
- **Auditoria:** caracteriza-se como a capacidade do sistema em registrar e identificar tudo o que um usuário realiza.

Ainda segundo Lyra (2008), a classificação do ativo da informação deve estar centrada em quatro eixos: confidencialidade, disponibilidade, integridade e autenticidade.

A classificação quanto à confidencialidade possui quatro níveis com relação à informação:

- **Nível 1 - Informação pública:** são informações que não possuem impacto direto para a organização mesmo se forem divulgadas externamente. Exemplo: catálogo de produtos;
- **Nível 2 - Informação interna:** são informações que possuem características relacionadas à empresa, mas que se divulgadas as consequências não serão críticas. Exemplo: lista de ramais;
- **Nível 3 - Informação confidencial:** as informações neste grupo devem ser categorizadas como restritas e protegidas, tendo em vista o potencial risco de perdas financeiras. Exemplos: senhas de acesso, dados de clientes etc; e
- **Nível 4 - Informação secreta:** são informações de grande importância para os negócios da empresa, por isso seu acesso deve ser restrito a pessoas de confiança e deve-se estabelecer regras para o seu uso e aplicação. Exemplos: contratos confidenciais, informações militares etc.

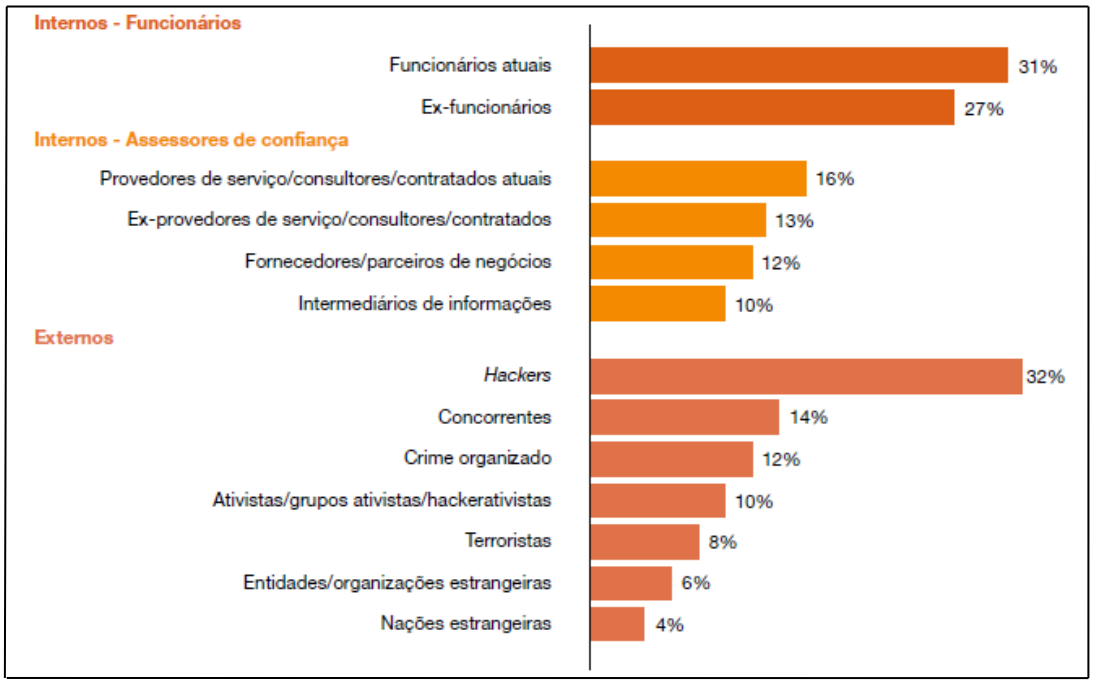
2.2 SEGURANÇA NO ATUAL CENÁRIO GLOBAL

Segundo Ernest & Young (2013), em apenas 17% das organizações a segurança da informação é eficaz. A ineficácia na área de segurança atinge 83% das organizações. Neste mesmo cenário, 93% estão mantendo ou aumentando seus investimentos em segurança para combater a crescente ameaça dos ataques cibernéticos.

Uma pesquisa realizada pela PWC com executivos de negócios, de segurança e de TI, apontou que 71% afirmam contar com um executivo sênior que faz a comunicação sobre a importância da segurança para a corporação. A comunicação interna corporativa é essencial para o sucesso das demais iniciativas, salientado por PWC (2014).

Viviane Oliveira, diretora da PWC, afirma que "não é possível combater as ameaças de hoje com as estratégias de ontem" e salienta que "é necessário um novo modelo de segurança da informação, que leve em consideração o conhecimento das ameaças do ciberespaço, dos ativos de informação e dos motivos e alvos dos potenciais atacantes" (PWC, 2014, p. 6).

Figura 1 - Origem provável estimada dos incidentes



Fonte: PWC (2014)

De acordo com Edgar D´Andrea, sócio da PWC, "os incidentes estão crescendo não só porque existem ameaças, mas também porque algumas empresas investiram em novas tecnologias para detectá-los melhor". O mesmo considera também que, "nesse sentido, a maior detecção de incidentes dever ser vista como acontecimento positivo" (PWC, 2014, p. 11).

Abordando a pesquisa realizada, onde foi questionada a origem provável estimada dos incidentes (Figura 1), na qual os entrevistados apontaram para o ano de 2013, um percentual considerável em relação aos *Hackers*[2], 32% considerou uma provável ameaça em relação aos incidentes pelo ambiente externo, já no ambiente interno da organização os funcionários atuais e ex-funcionários, são indicados como origem provável das ameaças, além de outros fatores como provedores de serviços/consultores/contratados atuais que podem realizar potenciais ataques já que em teoria possuem um conhecimento prévio da organização. É importante destacar o percentual de 31% e 27%, apresentado pelos funcionários atuais e ex-funcionários, respectivamente.

2.3 ENGENHARIA SOCIAL (ES)

Segundo Ulbrich & Valle (2007), as técnicas de ES exigem uma preparação psicológica profunda e contínua. A pessoa que irá aplicar as técnicas de ES deverá estar pronta para estudar o comportamento do seu alvo e entender melhor seu modo de operação, incluindo até o monitoramento de horários. O engenheiro social alvejará a boa vontade, a cortesia, a ingenuidade das pessoas e até mesmo as normas da empresa para enganar as vítimas.

A interpretação com base nos aspectos legais classifica a ES em muitos casos como falsidade ideológica, sendo considerados crimes passíveis de punição. Atualmente novas técnicas e

[2] *Hacker:* é um indivíduo que se dedica, com intensidade incomum, a conhecer e modificar os aspectos mais internos de dispositivos, programas e redes de computadores.

ferramentas de segurança foram desenvolvidas, no entanto, a utilização da ES em uma empresa privada pode se tornar um vetor principal de invasão, onde o ataque pode ser inevitável.

2.3.1 Ataque Indireto

O ataque indireto corresponde à utilização de ferramentas de obtenção de dados, como por exemplo, cavalos de Tróia e *sites*[3] com código malicioso, ou a utilização de impostura, a partir de *e-mails*[4] e *sites* falsos.

2.3.2 Ataque Direto

São caraterizados pelo contato pessoal, normalmente através de telefone ou até mesmo pessoalmente. Exige um planejamento e análise do alvo para passar confiança por parte do engenheiro social.

2.3.3 Metodologias Utilizadas por Engenheiros Sociais

Inicialmente, a pesquisa a ser realizada utilizando a ES pode ser compreendida como a aquisição de materiais, sejam eles, relatórios anuais ou listas de pagamentos. Nestes casos podem permitir uma visão financeira da empresa. Posteriormente, o meio pelo qual os Engenheiros Sociais tentam identificar onde está a informação e quais delas são importantes e relevantes para a realização de um ataque.

2.4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

De acordo com a definição de Mitnick e Simon (2003), as políticas de segurança são entendidas como instruções claras que fornecem as orientações de comportamento do empregado para guardar as informações, e são um elemento fundamental no desenvolvimento de controles efetivos para contra-atacar as possíveis ameaças à segurança das informações.

As políticas de segurança essencialmente devem expressar os anseios dos proprietários ou acionistas, responsáveis pela decisão do destino dos recursos da organização em relação ao uso das informações. É necessário, para sua elaboração, utilizar uma visão metódica, criteriosa e técnica, para que exista uma flexibilidade em relação aos equipamentos, tecnologias e na definição das responsabilidades fundamentais para a sua aplicação com o objetivo de elaborar políticas com o perfil adequado aos negócios da empresa.

2.4.1 Definição e Implementação das Políticas de Segurança da Informação

É importante destacar as definições apresentadas por Ferreira e Araújo (2008), as quais definem que as políticas de segurança devem possuir as seguintes características gerais para a qualidade na sua implementação:

- **Simples e compreensíveis**– sem processos exaustivos e desnecessários, fáceis de entender e aplicar;
- **Homologadas e assinadas pela alta administração** – ter a autorização do maior nível hierárquico é fundamental;

[3]*Site:* endereço virtual utilizado pela internet para comunicação comercial ou pessoal.
[4]*E-mail:* é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação.

- **Estruturadas de forma a permitir a sua implantação por fases** – níveis de aplicação devem ser estabelecidos para amenizar e medir o impacto no negócio;
- **Orientadas aos riscos** – a segurança das políticas devem priorizar os riscos existentes;
- **Flexíveis e preventivas** – podem ser moldados de acordo com as novas tecnologias e processos e que protejam e previnam a perda de dados.

Após a implementação é importante o acompanhamento e constante conscientização por parte da equipe de segurança da informação ou o comitê responsável pelo desenvolvimento das políticas. Se houve uma conformidade em relação às políticas definidas e às regras do negócio, Ferreira e Araújo (2008) destacam que se evidenciam os seguintes aspectos:

- Estabelecimento do conceito de que as informações são um ativo extremamente importante para a organização;
- Envolvimento da alta administração com relação á Segurança da Informação para consistência das políticas e responsabilidade formal dos colaboradores sobre a proteção dos recursos da informação, estabelecendo padrões para a segurança da informação.

3 *DATA LOSS PREVENTION* (DLP)

Todos os dias uma grande quantidade de dados é compartilhada e movimentada a partir de transferência de arquivos e mensagens instantâneas, seja através da rede interna da organização (intranet) ou pela internet. As ameaças de vazamento de dados podem estar relacionadas desde o roubo por pessoas da organização, sabotagem e até simplesmente por negligência do usuário, em muitos casos de forma não intencional. Nestes mesmos casos, o motivo para a negligência se deve ao não entendimento das normas ou a falta da definição de políticas específicas para conformidade em relação às informações geradas pela empresa. Desta forma, a utilização de tecnologias e soluções contra o vazamento de dados *DLP*, apresentam recursos importantes para a segurança da informação. DLP é considerado um conjunto de solução em que focalizam a perda de dados intencionais ou acidentais, principalmente por fontes internas, através de definição de políticas dentro do sistema, no intuito de prevenir, detectar e barrar a evasão de dados importantes (ISACA, 2010).

Segundo o ISACA (2010), a tecnologia atual permite o armazenamento e o processamento da maior parte dos dados existentes nas organizações de forma digital. Para proteger informações nesse meio, um conjunto de soluções tem sido destaque e colocado em uma categoria conhecida como prevenção contra vazamento de dados (ou *Data Loss Prevention - DLP*).

3.1 IDENTIFICAÇÃO DA INFORMAÇÃO

As soluções DLP utilizam para o seu funcionamento a varredura e tecnologias de inspeção detalhada de conteúdo para determinar a sensitividade do conteúdo e prevenir ou bloquear a saída de dados confidenciais da rede de uma organização. As tecnologias que estão integradas às soluções DLP suportam criptografia de dados, análise de vírus, monitoramento de acesso a dados confidenciais e classificação dos dados. Sejam estações de trabalho ou servidores de armazenamento, a transferência de dados é monitorada e bloqueada se necessário, de acordo com as políticas definidas em um planejamento que integra o projeto de DLP (ISACA, 2014).

De forma abrangente, segundo o ISACA (2010), as soluções DLP consideram as atividades em três níveis de utilização dos dados:

• **Nível de armazenamento (em descanso)**: as soluções DLP possuem a capacidade de identificar e registrar os locais nos quais tipos específicos de informações estão armazenadas na

empresa. Permite identificar tipos de arquivos específicos, sejam planilhas ou documentos de texto, armazenados em servidores de arquivos ou sistemas remotos. Após essa identificação, as soluções DLP são capazes de analisar os arquivos e verificar através dos dados a criticidade das informações. Utilizam rastreadores para identificação das informações;

• **Nível de rede (em trânsito)**: Os dados transmitidos de um local para outro são constantemente monitorados, e, se necessário, bloqueados pelo sistema DLP nos *gateways*[5] de rede ou de *e-mail*. Os pacotes de dados transmitidos são inspecionados utilizando técnicas de revisão para verificar a natureza do conteúdo em trânsito, além das transferências de dados através de *e-mail* (*SMTP*[6]), *web* (*HTTP*[7]*/HTTPS*[8]) e transferência de arquivos (*FTP*[9]*/FTPS*[10]), comparando-as com as políticas configuradas no sistema DLP, para a prevenção ou detecção de algum vazamento de informação confidencial; e

• **Nível do cliente (em operação)**: aplica-se à movimentação dos dados através das estações de trabalho do cliente ou dos usuários finais, onde são consideradas desde a cópia de dados para uma unidade de *pen drive*, o envio de informações para impressora ou até mesmo o copiar e colar entre aplicativos.

3.2 MUDANÇA CULTURAL NAS ORGANIZAÇÕES

As pessoas certas do negócio devem estar envolvidas no desenvolvimento e na implementação de tecnologias DLP, porque elas serão cruciais ao fazer julgamentos de valor relacionados a violações. O proprietário dos dados comerciais que tem uma ideia do contexto está muito mais capacitado para tomar essas decisões do que um analista de segurança de TI (ISACA, 2010).

De acordo com ISACA (2010), as empresas devem considerar, quando da implementação de tecnologias DLP, primeiramente um modo de monitoramento. É importante que os alertas orientados ao sistema permitam desenvolver a consciência e iniciar mudanças comportamentais, tornando-se uma abordagem melhor do que diretamente bloquear os fluxos de tráfego e sabotar potencialmente os processos comerciais intrínsecos ao negócio.

Jeffrey Brown salienta alguns aspectos fundamentais referente à mudança cultural na organização necessária para implementação de DLP (SCMAGAZINE, 2012):

- **Educação do usuário é a chave -** A educação do usuário é um forte aliado para o sucesso de um programa DLP. Certificar-se de que todos os usuários entendam a política de segurança é o fator essencial para o sucesso na implementação; e
- **Espalhar a palavra –** É necessário trabalhar com os líderes de toda a empresa, bem como os funcionários e ser um exercício constante de educação interna.

De acordo com Darrin Mourer (SCMAGAZINE, 2013), DLP é um agrupamento de pessoas especializadas, a criação de um conjunto de políticas e processos específicos, somado a um conjunto de ferramentas para reduzir o risco de perda de dados. A alta administração deve estar consciente dos riscos de negócios envolvidos na implantação de DLP. Posteriormente atuar na conscientização e divulgação das políticas de segurança para os gestores, pessoas chaves e colaboradores da organização.

---

[5]*Gateway*: máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.
[6]*SMTP*: protocolo padrão para envio de e-mails através da Internet
[7]*HTTP:* protocolo de transferência de hipertexto.
[8]*HTTPS*: protocolo de transferência de hipertexto seguro.
[9]*FTP:* protocolo de transferência de arquivos.
[10]*FTPS:* protocolo de transferência de arquivos seguro.

4 PROTEÇÃO CONTRA O VAZAMENTO DE DADOS: A VISÃO DE PROFISSIONAIS NA ÁREA DE TI EM UMA EMPRESA DE GRANDE PORTE

O procedimento metodológico de levantamento das informações e a revisão bibliográfica realizada ao longo deste permitiram o entendimento sobre a Segurança da Informação, e sobre as ferramentas que são importantes e que contribuem para a prevenção contra o vazamento de dados em uma organização.

A pesquisa e entrevista com os profissionais foi realizada em uma empresa de grande porte que atua no setor alimentício a mais de 50 anos no mercado. Possui mais de 2000 funcionários atuantes e um vasto portfólio de produtos comercializados. Dois profissionais da área de TI da empresa aceitaram responder em comum consenso o questionário baseado nas pesquisas realizadas.

4.1 ENTREVISTA COM DOIS PROFISSIONAIS DA ÁREA DE TI

Foi elaborado um conjunto de questões com o objetivo do entendimento dos fatores que uma empresa deve considerar para a diminuição dos riscos de vazamento de dados. Este estudo considera o entendimento e respostas por parte dos profissionais que atuam diretamente com a segurança da informação de uma empresa de grande porte. Um com cerca de dez anos de atuação e o outro com mais de trinta anos de experiência na gestão de TI, em consenso responderam ao questionário através da uma entrevista informal.

Em relação aos desafios enfrentados em gerenciar e proteger a informação ao longo dos anos, os profissionais da área de segurança apontaram que os principais desafios estão sempre relacionados à cultura das organizações, uma vez que sempre tem o sentimento do "na minha empresa isso nunca irá acontecer". Os profissionais afirmam que esse é o maior erro da maioria dos gestores de segurança, pois nunca se preocupam em elaborar processos, criar armazenamentos específicos e controle de acesso apropriado para cada tipo de informação. E quando estas ações existem, com o passar dos anos não são atualizadas.

Sobre as tecnologias fundamentais que devem ser utilizadas e aplicadas para a segurança das informações, os mesmos responderam e classificaram da seguinte forma:

- *Firewall* – com políticas e regras constantemente revisadas e testadas;
- Filtro *Web* – para controle da navegação *web* dos usuários de tecnologia;
- Autenticação – todos os acessos devem ser gerenciados através de credenciais, como por exemplo, *Active Directory Microsoft;*
- Antivírus – sempre atualizado e com políticas adequadas a cada tipo de acesso/usuário;
- Sistema Operacional – sempre atualizados e seguindo sempre as melhores práticas recomendadas pelo fabricante;
- Controle de acesso às áreas de armazenamento central das informações, como por exemplo, *Datacenters*; e
- DLP – Ferramentas baseadas em *software* que atuam desde a camada de rede, armazenamento até as estações de trabalho.

Questionados sobre a recente utilização do termo *Data Loss Prevention* nas discussões no cenário de líderes em TI e os desafios e dificuldades enfrentadas na utilização e aprovação de investimentos na área, os profissionais apontaram que quando se trata de segurança, as mudanças culturais são, com certeza, o maior desafio enfrentado. As dificuldades são apontadas como

relacionadas à escolha das ferramentas x implantação. No caso de aprovação de investimentos, é salientado que no Brasil, esse tema ainda é um "tabu", onde é cultural esperar acontecer para se proteger. Afirmam que, é necessário por parte dos gestores de segurança, apontar e evidenciar os riscos.

Quando questionados sobre o impacto da mudança cultural em uma organização a partir da definição e aplicação de ações em Segurança da Informação, os mesmos responderam que, como toda mudança, os transtornos são inevitáveis e fazem parte do processo, porém o impacto é grande e evidenciado quando as políticas já começam a fazer parte do cotidiano das empresas, e, ao contrário do que muitos pensam, tudo fica mais simples, rápido e seguro.

Por fim, quando questionados sobre qual a importância da prevenção contra o vazamento de dados, os mesmos responderam que, a todo instante é possível acompanhar na mídia que, as notícias sobre o vazamento de informações, a busca por resultados, a corrupção e a obtenção de vantagens competitivas passam essencialmente pela obtenção de informações estratégicas. Por essas razões, garantir a segurança dos dados trafegados é fundamental para a sobrevivência de qualquer organização, e a prevenção é a melhor opção, pois quando se trata de informação não existe segunda chance.

4.2 ANÁLISE E COMPREENSÃO DAS VISÕES

Fatores que foram destaque nas respostas apresentadas pelos profissionais de Segurança da Informação, e que foram citados ao longo da pesquisa realizada, são que o entendimento a respeito de que a segurança da informação não pode ser alcançada totalmente, mas deve ser considerada como um processo contínuo para a redução dos riscos e vulnerabilidades, para a definição de políticas específicas para os colaboradores, para o negócio e para a comunicação interna e externa da empresa. E principalmente, deve-se considerar fortemente a utilização de tecnologias que auxiliam no processo de segurança da informação, como por exemplo, *Firewall*, filtro *web*, Antivírus e DLP.

Um dos principais desafios gira em torno da mudança cultural nas organizações, conforme descrito pelos profissionais, que podem trazer transtornos que são inevitáveis, mas a partir do momento que essas mudanças começam a fazer parte do cotidiano das pessoas, as ações aplicadas para a segurança das informações evidenciam resultados positivos, e os processos se tornam mais simples, rápidos e seguros. A prevenção é a chave para a sobrevivência das empresas contra o vazamento de informações.

5 CONCLUSÃO

As informações são os ativos mais importantes para as organizações atualmente. Conhecer o valor agregado a elas e classifica-las da forma correta é o primeiro passo para que seja possível aplicar ações em segurança da informação. Crimes digitais com o objetivo do vazamento de informações acontecem de forma cada vez mais frequente; o fator humano externo não pode ser mais considerado como única forma de ataque, mas a ação interna por parte dos próprios colaboradores, seja intencional ou acidental, é apresentado como um grande percentual dos ataques apontados por líderes de TI do mundo todo.

A aplicação de ferramentas DLP pode auxiliar no processo contínuo de segurança da informação, partindo do entendimento que tais tecnologias realizam a proteção de dados que estão em descanso, em trânsito e em operação. No entanto, a mudança cultural provocada pela implantação de DLP ou outra tecnologia com foco em segurança da informação, torna-se um dos fatores mais preocupantes, porque, se não for planejada e organizada em conformidade com os riscos existentes, pode impactar diretamente nos processos de negócios da organização.

Assim, neste trabalho é conclusivo salientar que a segurança da informação deve ser um processo sempre presente, baseado em constantes atualizações, conscientização por parte dos colaboradores, gestores e até mesmo a alta hierarquia da empresa, aplicando sempre ferramentas em tecnologia que estejam em conformidade aos negócios, e permita a diminuição dos riscos e vulnerabilidades, buscando sempre a prevenção, chave para que o vazamento de informações não seja concretizado.

REFERÊNCIAS BIBLIOGRÁFICAS

ERNEST & YOUNG. **Crimes Cibernéticos são a maior ameaça à sobrevivência das empresas, aponta estudo da EY**, 2013. Disponível em: < http://www.ey.com/BR/pt/Services/Release_Pesquisa_Seguranca_Informacao_EY>. Acesso em: 08 jun 2015.

FERREIRA, Fernando Nicolau Freitas; ARAUJO, Marcio Tadeu de. **Política de Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna, 2008.

FONTES, Edison. **Segurança da Informação: O usuário faz toda a diferença**. São Paulo: Saraiva, 2006.

ISACA. **Considerações essenciais para a proteção do vazamento de dados confidenciais através de ferramentas de prevenção de perda de dados**, 2014. Disponível em: <http://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Key-Considerations-in-Protecting-Sensitive-Data-Leakage-Using-Data-Loss-Prevention-Tools-Portuguese.aspx>. Acesso em: 15 jun 2015.

ISACA. **Prevenção contra vazamento de dados**, 2010. Disponível em: <http://www.isaca.org/Knowledge-Center/Research/Documents/DLP_whp_Por_0311.pdf>. Acesso em: 12 nov 2014.

LYRA, Mauricio Rocha. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Editora Ciência Moderna, 2008.

MITNICK, Kevin D.; SIMON, William L. **A ARTE DE ENGANAR**. Pearson Education do Brasil, São Paulo, 2003.

PWC. **Principais resultados da Pesquisa Global de segurança da informação 2014**, 2014. Disponível em: <https://www.pwc.com.br/pt_BR/br/publicacoes/servicos/assets/consultoria-negocios/pesq-seg-info-2014.pdf> Acesso em 15 set 2015.

ROEBUCK, K. **Data loss prevention (DLP) - high-impact strategies. Brisbane:** Emereo Pty Limited, 2011.

SCMAGAZINE. **Defining a DLP strategy**, 2012. Disponível em: <http://www.scmagazine.com/defining-a-dlp-strategy/article/228632> Acesso em 20 jun 2015.

SCMAGAZINE. **DLP Challenging Common Misconceptions**, 2013. Disponível em:http://www.scmagazine.com/dlp-challenging-common-misconceptions/article/293172/> Acesso em 20 jun 2015.

ULBRICH, Henrique Cesar; VALLE, James Della. **Universidade H4ck3r**. São Paulo: Digerati Books, 2007.